

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)"

«БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

ДЕСЯТАЯ
МЕЖДУНАРОДНАЯ
НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

(Москва, 3-4 декабря 2019 года)

СБОРНИК ТРУДОВ КОНФЕРЕНЦИИ

МГТУ им.Н.Э.Баумана
НУК «Информатика и системы управления»
МОСКВА-2019

УДК 003.26.7: 004.05
ББК 32.937.202
Б31

Б31

Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019. 409 с. – илл.

ISBN 978-5-9906630-6-0

Сборник содержит тезисы докладов, представленных на Десятой всероссийской научно-технической конференции "Безопасные информационные технологии" (БИТ-2019), проходившей 3-4 декабря 2019 г. в Москве в МГТУ им. Н.Э. Баумана.

Тезисы публикуются в редакции научных руководителей или в авторской редакции при наличии ученой степени.

Редакционный совет:

Александров А.А., д-р техн. наук, ректор МГТУ им. Н.Э. Баумана
Пролетарский А.В., д-р техн. наук, декан факультета ИУ МГТУ им. Н.Э. Баумана
Басараб М.А., д-р физ.-мат. наук, зав. кафедрой ИУ-8 МГТУ им.Н.Э.Баумана
Марков А.С., д-р техн. наук, профессор кафедры ИУ-8 МГТУ им.Н.Э.Бауман



© Коллектив авторов
© НУК ИУ МГТУ им.Н.Э.Баумана

Программно-аппаратная система аутентификации в пользовательских приложениях

Акулов Е. А.¹

Разработан макет аппаратного хранилища автоматизированного ввода многозначных паролей. Это исследование может быть применено для решения проблемы безопасного хранения паролей на внешнем носителе. Описываются принципы и алгоритмы работы устройства.

Ключевые слова: токен, аппаратное хранилище паролей, двухфакторная аутентификация, криптоконтейнер, микроконтроллер.

Введение

Многофакторная аутентификация все больше выходит на первый план в вопросах защиты аутентификационных данных. В 2016 г. SecureAuth Corporation совместно с Wakefield Research провели исследование, опросив 200 руководителей IT отделов в США. Исследование показало, что 69% организаций, скорее всего, могут отказаться от паролей в течение ближайших пяти лет; 99% респондентов согласились с тем, что двухфакторная аутентификация является лучшим способом защиты. В облачных сервисах Microsoft ежедневно совершается около 300 млн попыток мошеннического входа. Многофакторная аутентификация (МФА) может помочь защитить учетные записи от многих типов атак.

По словам специалистов Microsoft, пользователи, включившие МФА, в итоге блокируют 99,9% автоматических атак. Рекомендация распространяется не только на учетные записи Microsoft, но и на любой другой профиль, web-сайт или online-сервис. Если поставщик услуг поддерживает МФА, Microsoft рекомендует использовать ее, независимо от того, является ли она чем-то простым, как одноразовые SMS-пароли или расширенные биометрические решения. В настоящее время злоумышленники имеют в своем распоряжении различные методы, позволяющие получить учетные данные пользователей, и в большинстве случаев пароль и его сложность не имеют значения. От постоянных попыток мошеннического входа защитит включение МФА. Она не сможет заблокировать только 0,1% атак, в ходе которых злоумышленники используют технические решения для захвата токенов МФА, но они происходят крайне редко. Из всего вышесказанного следует что МФА можно назвать эффективным средством защиты от кражи аутентификационных данных [1-9].

Для защиты своих аутентификационных данных в повседневной жизни, пользователи используют, либо токены, либо парольные менеджеры, либо что чаще всего, вообще никак не защищают свои аутентификационные данные, создавая тем самым угрозу их компрометации. Токены имеют высокую стоимость и весьма ограниченный спектр применения, а парольные менеджеры содержат в себе большое количество уязвимостей. Что в свою очередь оставляет нерешенным вопрос безопасной аутентификации, для пользователей в повседневной жизни. Целью работы является решения проблемы безопасной аутентификации.

Общее описание устройства

Для решения проблемы безопасной аутентификации был разработан парольный аутентификатор, изначально в качестве платформы использовался микроконтроллер Arduino pro micro. Подключение к компьютеру происходит по проводному каналу связи и

¹ Акулов Евгений Алексеевич, студент, Сибирский государственный университет науки и технологии имени академика М. Ф. Решетнева, Красноярск, evgeny.akulov@gmail.com

аутентификатор распознается как hid-устройство. С её помощью был реализован следующий функционал [10]:

- защищенная передача пароля по каналу связи;
- защищенное хранение базы данных паролей;
- программа взаимодействия с устройством;
- устройство хранения паролей;

Устройство может функционировать в 3х режимах:

- Режим «редактирование». Данный режим необходим для настройки устройства с использованием компьютера и специальной программы.
- Режим «настройка устройства». В данном режиме работа по настройке устройства осуществляется с помощью самого устройства и 2-х кнопок, входящих в его состав.
- Режим «основной». В данном режиме устройство осуществляет авторизацию в приложении/сервисе/браузере.

От взлома корпуса, устройство защищено пломбой (термотрансферной этикеткой).

Так как возможности этой аппаратной платформы были исчерпаны, в следствии ограниченности вычислительных ресурсов и отсутствия возможности расширения, путем интеграции дополнительных аппаратных модулей, для дальнейшей модернизации и развития устройства, было принято решение перейти на микроконтроллеры семейства STM32. Их основное преимущество на сегодняшний день — универсальность. В своей основе они могут иметь различные процессорные ядра, наиболее популярные и отвечающие требованиям для реализации механизмов функции обеспечения информационной безопасности. С их помощью, на текущий момент были частично реализованы следующие режимы работы устройства:

- режим работы «ОТР»;
- режим работы «GSM».

Общая блок-схема работы устройства представлена на рис. 1.

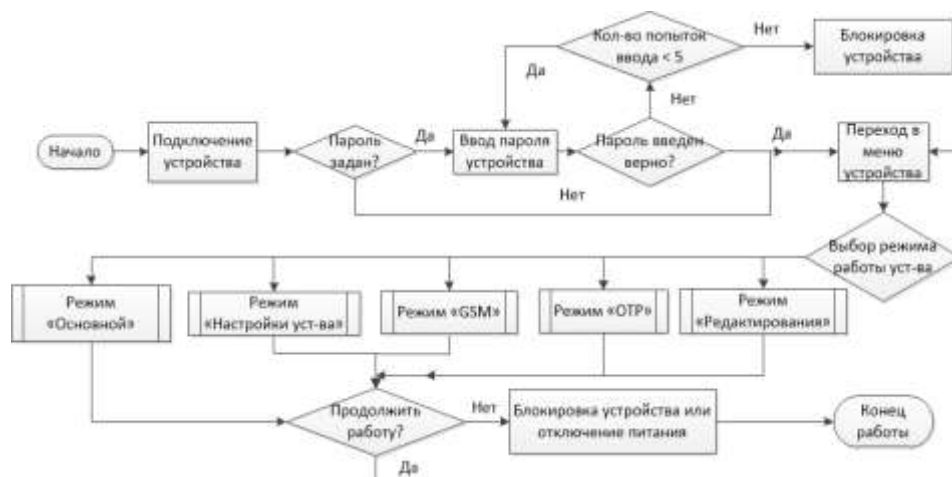


Рис.1. Блок-схема работы устройства

Режим работы «ОТР»

Он заключается в следующем, аутентификация в сервисе/приложении происходит с помощью одноразового пароля. Устройство содержит уникальный секретный ключ, который будет использован для шифрования некоторых данных, используемых для генерации пароля. Тот же самый ключ содержится и на сервере аутентификации. Сервер шифрует их же и сравнивает результат с тем, что получает от клиента. При совпадении значений считается, что процесс аутентификации прошел успешно. В данном устройстве используется синхронный режим, и синхронизация происходит по времени. Сервер

аутентификации и ОТР-устройство генерирует пароль, базируясь на показаниях внутренних часов. При этом возможность применения данного пароля ограничена определенным интервалом времени. Блок-схема данного режима представлена на рис. 2.



Рис.2. Режим работы «ОТР»

Режим работы «GSM»

Он заключается в следующем, при попытке аутентификации на зарегистрированный номер телефона придет СМС с одноразовым паролем для входа в систему. Роль телефона, на который приходит смс с одноразовым паролем, выполняет микроконтроллер с GSM модулем, который принимает смс сообщение с одноразовым паролем и отображает его на экране устройства. Через минуту пришедшее сообщение с паролем стирается. Данный режим может использоваться в различных банковских приложениях. Блок-схема данного режима представлена на рис. 3.

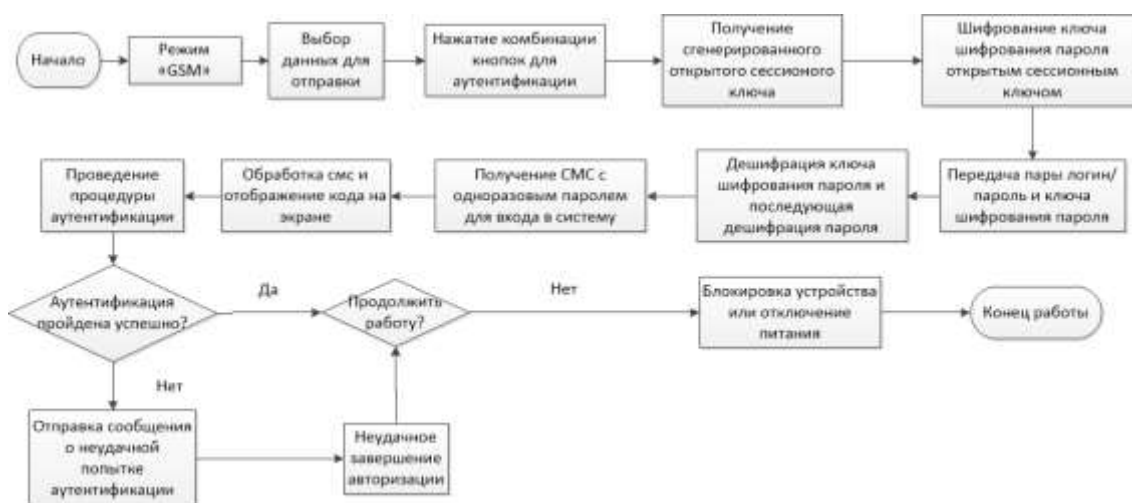


Рис.3. Режим работы «GSM»

Выводы

В ходе работы разработано устройство – парольный аутентификатор осуществляющий безопасное хранение и передачу пароля по открытому каналу. Оно позволяет осуществлять безопасную аутентификацию в различных сервисах и приложениях, используя различные методы многофакторной аутентификации.

Данное устройство решает проблему безопасной аутентификации. Преимуществами данного устройства являются: открытый программный код, что дает возможность проверки на НДВ, широкий спектр применения в различных сервисах, приложениях, а

также сочетание защищенного хранилища паролей и устройства аутентификации в одном устройстве, что нивелирует угрозы присущие программными менеджерами паролей.

Литература

1. Давлетханов М. Концепция одноразовых паролей в системе аутентификации // ВУТЕ/Россия. № 7–8. С. 95.
2. Жаринов А.А. Шмокин М.Н. Факторы уязвимости информационной технической системы // Успехи современного естествознания, 2011 г. № 7. С. 108-109.
3. Титов В.С. Идентификация и аутентификация. Способы и методы аутентификации// Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова. С 4514-4519.
4. Брянцев А. В., Дихнов В. Е., Качурин А. Г., Адодин А. А. Разработка программного модуля аутентификации внешних пользователей компьютерной системы // Молодой ученый, 2018 г. № 23 (209). С.195-197.
5. Ус А.А., Беловодский Е.В. Эффективность средств аутентификации в информационно-вычислительных системах // Вестник современных исследований, 2018 г. № 4.2 (19) С. 313-316.
6. Матевосян С.Л. Полухин С.М. Механизмы аутентификации платежных систем студенческая наука для развития информационного общества Сборник материалов VIII Всероссийской научно-технической конференции. 2018 148-151.
7. Альтерман А.Д., Лушников Н.Д. Аутентификация и идентификация как один из основных элементов безопасности технических средств // Аллея науки, 2018 г. Т. 1 № 6 (22). С. 936-938.
8. Лесников А.В. Анализ методов защиты информации в автоматизированной системе управления от несанкционированного доступа оптимизация и моделирование в автоматизированных системах // Труды международной молодежной научной школы, 2018 г. С. 160-164.
9. Шевченко В.К. Защита информации от несанкционированного доступа закономерности и тенденции инновационного развития общества // сборник статей по итогам «Международной научно-практической конференции», 2019 г. С. 72-75.
10. Акулов Е. А., Пароткин Н. Ю. Анализ возможностей микроконтроллеров для решения задач аутентификации в пользовательских приложениях // Материалы V Международной научно-практической конференции творческой молодежи «Актуальные проблемы авиации и космонавтики», 2019 г. С. 201-204.

Научный руководитель: Пароткин Николай Юрьевич, кандидат технических наук, доцент кафедры безопасности информационных технологий Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнёва (СибГУ), nyparotkin@yandex.ru.

The hardware and software authentication system in custom applications

Akulov E. A.²

Abstract. The model of automated hardware storage was developed, enter reusable passwords. This study can be applied to solve the problem secure password storage on external storage. This article describes the principles and algorithms of the device.

Keywords: token, two-factor authentication, hardware storage of passwords, cryptocontainer, microcontroller.

² Akulov Evgeny Alekseevich, student, Siberian State University of Science and Technology named after academician M.F. Reshetnev, Krasnoyarsk, evgeny.akulov@gmail.com

Методика повышения устойчивости функционирования информационно-управляющих систем при информационно-технических воздействиях

Антонов С.Г.³, Гвоздева Г.А.⁴, Климов С.М.⁵

Разработана методика, позволяющая повысить устойчивость функционирования информационно-управляющих систем при информационно-технических воздействиях на основе многовариантного выбора организационно-технических мер информационной безопасности и устранения уязвимостей. В качестве информационно-управляющих систем исследуются объекты критической информационной инфраструктуры, объединяющие распределенные информационно-телекоммуникационные сети, информационные системы и выполняющие единый технологический цикл управления. Угрозами нарушения устойчивости функционирования информационно-управляющих систем являются целенаправленные информационно-технические воздействия на программное и информационное обеспечение объектов критической информационной инфраструктуры, приводящие к нарушению процессов их функционирования на заданном интервале времени.

Ключевые слова: информационно-технические воздействия, логические правила анализа рисков, организационно-технические мероприятия информационной безопасности, показатели оценки, уязвимости.

Введение

Значимыми объектами критической информационной инфраструктуры (КИИ) являются информационно-телекоммуникационные сети и информационные системы, которые при выполнении взаимосвязанных функций сбора, обработки и передачи информации объединяются в информационно-управляющие системы (ИУС). Программно-техническая основа сложных ИУС формируется на базе информационных и телекоммуникационных технологий с зарубежным участием, что обуславливает использование значительного числа протоколов информационного взаимодействия (известно около 400 протоколов информационного взаимодействия различных приложений) и значительного объема информации в центрах обработки данных.

Значительный объем сетевых протоколов и данных в ИУС на объектах КИИ, стандартные настройки параметров средств защиты информации (СЗИ) объективно приводят к внесению в них множества уязвимостей [1, 2, 7]. Совокупность уязвимостей в ИУС создает предпосылки для реализации потенциальных угроз информационно-технических воздействий (ИТВ) нарушителей, которые снижают устойчивость функционирования ИУС [1, 7, 10]. Информационно-технические воздействия представляют собой целенаправленные программно-аппаратные и программные воздействия, приводящие к нарушению устойчивости функционирования ИУС. Реализация ИТВ нарушителями осуществляется в форме компьютерных атак «отказ в обслуживании» (DDoS-атак) и информационной нагрузки [1, 2, 6].

Таким образом, разработка методики, позволяющей повысить устойчивость функционирования ИУС при ИТВ за счет априорной оценки и многовариантного выбора организационно-технических мер информационной безопасности (ОТМ ИБ), устранения уязвимостей является актуальной.

³Антонов Сергей Григорьевич, 4 ЦНИИ Минобороны России, e-mail: sergey_antonov_1960@mail.ru

⁴Гвоздева Галина Алексеевна, 4 ЦНИИ Минобороны России, e-mail: g_gvozdeva62@mail.ru

⁵Климов Сергей Михайлович, д.т.н., профессор, 4 ЦНИИ Минобороны России, e-mail: klimov.serg2012@yandex.ru

Структура методики повышения устойчивости функционирования ИУС

На основе анализа современных методов устойчивости информационных систем [3-5, 7-11] в методике повышения устойчивости функционирования ИУС при ИТВ (рис.1) определена базовая последовательность:

экспериментальная оценка реальной защищенности ИУС в условиях ИТВ в ходе испытаний на стендовом полигоне и сбор статистики;

выбор ОТМ ИБ;

оценка выполнения требований к устойчивости ИУС в условиях ИТВ.



Рис.1. Схема методики повышения устойчивости функционирования ИУС при ИТВ

Модель реализации угроз ИТВ на ИУС

Модель реализации угроз ИТВ на ИУС, которая включает в свой состав классификацию угроз целенаправленных ИТВ на ИУС и аналитические выражения для оценки характеристик ИТВ.

Классификация угроз целенаправленных ИТВ на ИУС (рис.2) определяет возможные способы реализации и типы ИТВ в соответствии с эталонной моделью взаимодействия открытых систем (ЭМ ВОС) и последствия ИТВ.

Аналитические выражения для оценки характеристик ИТВ позволяют:

а) определить вероятность успешной реализации ИТВ на ИУС:

$$P_{ИТВ} = 1 - \prod_{i=1}^{N_{ИТВ}} [(1 - e^{-\lambda_{ИТВ_i} t_{ИТВ_i}}) \times (1 - e^{-\lambda_{ИН_i} t_{ИТВ_i}}) \times (1 - e^{-\lambda_{СК_i} t_{ИТВ_i}})], \quad (1)$$

где $\lambda_{ИТВ_i} = \sum_{i=1}^{m_{ИТВ}} \frac{n_{ИТВ ИУС_i}}{N_{ИУС_i} t_{ИТВ_i}}$ – среднее число успешных ИТВ типа «отказ в обслуживании» в единицу времени,

$n_{ИТВ ИУС_i}$ – число нарушенных ИУС при реализации ИТВ «отказ в обслуживании»,

$N_{ИУС_i}$ – общее количество ИУС,

$t_{ИТВ_i}$ – время ИТВ,

$N_{ИТВ}$ – общее количество ИТВ на ИУС,

$N_{ИТВ} \in \{m_{ОО}, n_{ИН}, k_{СК}\}$,

где: $m_{ОО}$ – число ИТВ «отказ в обслуживании»,

$n_{ИН}$ – число ИТВ «информационная нагрузка»,

k_{CK} – число сканирований уязвимостей путем направления в сеть стандартных пакетов передачи данных и реализаций фаззинга за счет выдачи в сеть искаженных стеков протоколов передачи данных,

$$\lambda_{ИИi} = \sum_{i=1}^{n_{ИИ}} \frac{m_{ИИ ИУCi}}{N_{ИУCi} t_{ИТВi}} - \text{интенсивность информационной нагрузки},$$

$m_{ИИ ИУCi}$ – число нарушенных ИУС при реализации ИТВ «информационная нагрузка»,

$$\lambda_{CK} = \sum_{i=1}^{k_{CK}} \frac{r_{CK ИУCi}}{N_{ИУCi} t_{ИТВi}} - \text{интенсивность сканирования уязвимостей стандартными}$$

пакетами и методом фаззинга,

$r_{CK ИУCi}$ – число нарушенных ИУС при реализации ИТВ «сканирование уязвимостей и фаззинг»,

б) получить оценки потенциального риска для ИУС при реализации ИТВ

$$R_{ИТВi}^{ИУC}(t_{ИТВi}) = P_{ИТВi} \gamma_i, \quad (2)$$

где: γ_i – величина ущерба от ИТВ, $\gamma = \{1, \dots, 30\}$ – определяется экспертным путем по числу нарушенных элементов ИУС и стоимости ущерба [1, 7-10].

По статистике испытаний элементов ИУС на стендовом полигоне при реализации ИТВ проводится предварительная оценка показателей устойчивости ИУС в условиях ИТВ математическими выражениями для определения:

а) вероятности устойчивого функционирования ИУС в условиях ИТВ:

$$P_{уст}^{ИУC}(t_{\phi}) = \frac{\mu_{Bi}}{\lambda_{ИТВi} + \mu_{Bi}} + \frac{\lambda_{ИТВi}}{\lambda_{ИТВi} + \mu_{Bi}} e^{-(\lambda_{ИТВi} + \mu_{Bi}) t_{\phi}}, \quad (3)$$

где $\mu_{Bi} = 1/\tau_{вос}$ – интенсивность восстановления ИУС после i -го ИТВ,

$\tau_{вос}$ – среднее время восстановления,

б) коэффициента готовности ИУС:

$$K_{\Gamma_i}^{ИУC} = \frac{1}{1 + Z_{отмi} \frac{\lambda_{ИТВi}}{\mu_{Bi}}} P_{адан}, \quad (4)$$

где: $Z_{отм}$ – количество внедренных мер защиты информации в ИУС (технические меры – автоматизированные модули доверенной загрузки (АМДЗ), межсетевые экраны (МЭ), средства антивирусной защиты (САВЗ), виртуальные частные сети (VPN), модули системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) – ИУС),

$P_{адан}$ – вероятность успешной адаптации ИУС к сбоям и отказам после реализации ИТВ; $0,95 \geq P_{адан} \geq 0,85$.

Структура ОТМ ИБ и логические правила для их выбора

Структура ОТМ ИБ для повышения устойчивости ИУС при реализации ИТВ нарушителя формируется исходя из требований регуляторов в области ИБ (рис.3).

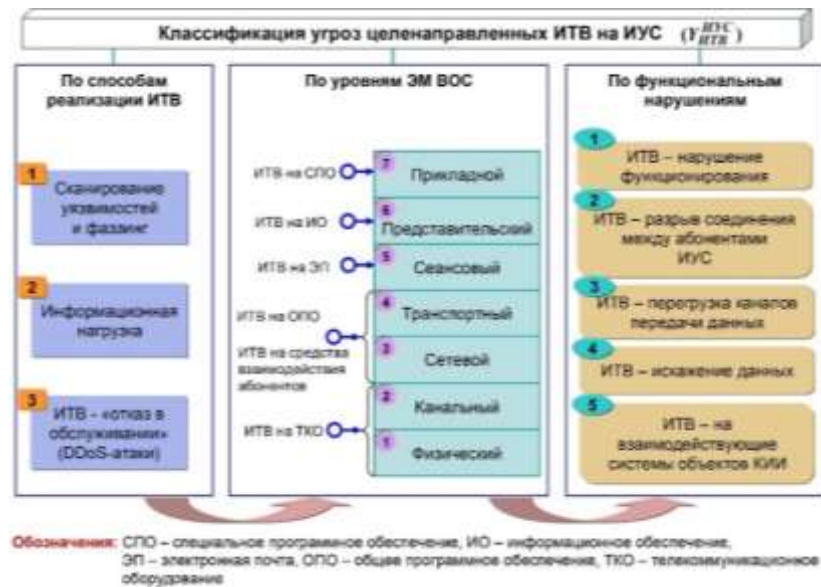


Рис.2. Классификация угроз целенаправленных ИТВ на КСА РКШН



Рис.3. Структура ОТМ ИБ информационно-управляющих систем

Логические правила для многовариантного выбора ОТМ ИБ представим следующим образом:

1) Определение функционала защищенности ИУС в условиях ИТВ:

$$W_{СЗИ}^{ИУС} = [\{\xi_{уяз}^{ИУС}\}, \{Y_{ИТВ}^{ИУС}\}, \{Z_{ОТМ}\}, \xi_{уязj}^{ИУС} \in \xi_{уяз}^{ИУС}, Y_{ИТВj}^{ИУС} \in Y_{ИТВ}^{ИУС}, z_{ОТМj} \in Z_{ОТМ}^{ИУС}]. \quad (5)$$

2) Правило распределения ОТМ ИБ по множествам уязвимостей ИУС и угроз ИТВ, обеспечивающих максимум вероятности устойчивости ИУС:

$$\forall z_{ОТМj} \in Z_{ОТМ} \exists P_{уст}^{ИУС*}(z_{ОТМj}^*, \xi_{уязj}^{ИУС*}, Y_{ИТВj}^{ИУС*}) \rightarrow \max. \quad (6)$$

3) Правила снижения риска нарушения устойчивости ИУС:

а) существует $z_{ОТМj} \in \{0,1\}, \forall j \in R_{ИТВ}^{ИУС} \rightarrow z_{ОТМj} = 1$, если j -я ОТМ ИБ обеспечила устойчивость ИУС, и $z_{ОТМj} = 0$, если j -я ОТМ ИБ не обеспечила устойчивость ИУС, $\bar{z}_{ОТМ}$ – вектор параметров ОТМ ИБ;

б) существует $\xi_{уязj}^{ИУС} \in \{0,1\}, \forall j \in R_{ИТВ}^{ИУС} \rightarrow \xi_{уязj}^{ИУС} = 1$, если j -я уязвимость использована нарушителем, и $\xi_{уязj}^{ИУС} = 0$, если уязвимость устранена, $\vec{\xi}_{уяз}^{ИУС}$ – вектор параметров уязвимостей;

в) существует $y_{ИТВj}^{ИУС} \in \{0,1\}, \forall j \in R_{ИТВ}^{ИУС} \rightarrow y_{ИТВj}^{ИУС} = 1$, если j -е успешное ИТВ, и $y_{ИТВj}^{ИУС} \neq 0$, если ИТВ не реализовано, $\vec{y}_{ИТВ}^{ИУС}$ – вектор параметров ИТВ,

г) тогда интегральный показатель снижения риска нарушения устойчивости ИУС:

$$G_{уст}^{ИУС} = G_{\max}^{ИУС}(\vec{\xi}_{уяз}^{ИУС}, \vec{y}_{ИТВ}^{ИУС}) - G_{ИТВ}^{ИУС}(\vec{\xi}_{уяз}^{ИУС}, \vec{y}_{ИТВ}^{ИУС}, \vec{z}_{ОТМ}) =$$

$$= \sum_{j=1}^N R_{ИТВj}^{ИУС} - \sum_{j=1}^N P_{ИТВj}^{ИТВ} \gamma_j, z_{ОТМj} \xi_{уязj}^{ИУС} y_{ИТВj}^{ИУС}, \quad (7)$$

где $P_{ИТВj}^{ИТВ}$ – вероятность нейтрализации риска нарушения устойчивости ИУС за счёт j -ой ОТМ ИБ.

Условием минимизации остаточного риска выбранного варианта устойчивого ИУС в условиях ИТВ считается устранение уязвимостей, через которые могут быть реализованы ИТВ, взаимосвязанным применением ОТМ ИБ.

Критерий оценки требований к устойчивости ИУС при ИТВ

Дано:

1. Известные параметры уязвимостей элементов ИУС:

$\xi_{ПО}$ – программного обеспечения (ПО),

$\xi_{ИО}$ – информационного обеспечения (ИО),

$\xi_{ТКО}$ – телекоммуникационного оборудования (ТКО),

ξ_{Φ} – функциональные уязвимости ИУС.

Параметры уязвимостей устанавливаются с использованием отечественной (BDU) и зарубежной (CVE) баз данных уязвимостей.

2. Характеристики ИТВ:

$Y_{ИТВ}$ – параметры средств реализации ИТВ.

Параметры ИТВ соответствуют характеристикам имитаторов ИТВ, например средства нагрузочного тестирования Ixia Breaking Point.

3. Параметры ОТМ ИБ:

$Z_{ОТМ}$ – параметры ОТМ ИБ.

Требуется: найти такие значения параметров ОТМ ИБ $Z_{ОТМ}$, при которых значения вероятности устойчивого функционирования максимальны

$$P_{уст}^{ИУС*} = \max_{Z_{ОТМ}^* \in Z_{ОТМ}} P_{уст}^{КСА}[(\xi_{ПО}^*, \xi_{ИО}^*, \xi_{ТКО}^*, \xi_{\Phi}^*) Y_{ИТВ}^*, Z_{ОТМ}^*]. \quad (8)$$

При ограничениях:

- на параметры уязвимостей ИУС

$\xi_{ПО}^* \in \xi_{ПО}, \xi_{ИО}^* \in \xi_{ИО}, \xi_{ТКО}^* \in \xi_{ТКО}, \xi_{\Phi}^* \in \xi_{\Phi},$

- на характеристики средств реализации ИТВ

$T_{ИТВ} \ll T_{\Phi}, Y_{ИТВ}^* \in Y_{ИТВ}.$

Заключение

В методике разработаны показатели оценки потенциального риска для ИУС при реализации ИТВ по результатам стендовых испытаний, экспертные логические правила для выбора ОТМ ИБ и критерий оценки выполнения требований к устойчивости ИУС при ИТВ, которые позволяют априорно устранить уязвимости и выбрать рациональные варианты ОТМ ИБ.

Литература

1. Антонов С.Г., Климов С.М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. 2017. Том 17. №1. С. 32-39.
2. Климов С.М., Сосновский Ю.В. Методика оценки защищенности микропроцессорных систем управления в условиях информационно-технических воздействий. // Надежность. 2018. Том 18. №4. С. 36-44.
3. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. – Ульяновск: Областная типография «Печатный двор», 2012. 216 с.
4. Климов С.М., Половников А.Ю., Сергеев А.П. Модель функциональной отказоустойчивости процессов обеспечения потребителей навигационными сигналами в сложных условиях // Надежность. 2017. Том 17. № 2. С. 41-47.
5. Климов С.М., Поликарпов С.В., Федченко А.В. Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий. // Надежность. 2017. Том 17. №3. С. 32-40.
6. Климов С.М., Купин С.В., Купин Д.С. Модели вредоносных программ и отказоустойчивости информационно-телекоммуникационных сетей // Надежность. 2017. № 4. С. 36-43. DOI: 10.21683/1729-2640-2017-17-4.
7. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. – Ульяновск: Обл. типография «Печатный двор», 2016. 544 с.
8. Гапанович В.А., Шубинский И.Б., Замышляев А.М. Метод оценки рисков системы из разнотипных элементов // Надежность. 2016. Том 16. № 2. С. 49-53.
9. Климов С.М., Котяшев Н.Н. Метод регулирования рисков комплексов средств автоматизации в условиях компьютерных атак // Надежность. 2013. №2. С. 93-107.
10. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. – Ульяновск: Областная типография «Печатный двор», 2012. 296 с., ил.
11. Климов С.М., Поликарпов С.В., Рыжов Б.С., Тихонов Р.И., Шпырня И.В. Методика обеспечения устойчивости функционирования критической информационной инфраструктур в условиях информационных воздействий // Вопросы кибербезопасности. 2019. №6, 2019, С. 37-48.

Method of increase management-information systems operation stability in computer attack conditions

Sergey G. Antonov⁶, Galina A. Gvozdeva⁷, Sergey M. Klimov

This paper presents method, allowing to increase management-information systems operation stability in computer attack conditions on basis of multichoice alternative variants of organization and technical measures information security and vulnerability elimination. By the way of management-information systems investigate critical information infrastructure objects. This object integrated distributed management-communication networks and information systems, which realize common technological management cycle. Purposeful computer attacks against critical information infrastructure objects software and dataware is threats management-information systems operation stability, which bring to system operation process violation on specified time interval.

Keywords: computer attack, logical rules risk analysis, organization and technical measures of information security, evaluation index, information security facilities, vulnerability.

⁶Antonov Sergey G., 4 Central Science Research Defense Institute, e-mail: sergey_antonov_1960@mail.ru

⁷Gvozdeva Galina A., 4 Central Science Research Defense Institute, e-mail: g_gvozdeva62@mail.ru

⁸Klimov Sergey M., Doctor of Science, professor, 4 Central Science Research Defense Institute, e-mail: klimov.serg2012@yandex.ru

Учебный имитатор объединенной отечественной сети ПД специального назначения (структура, функции)

Басараб М.А.⁸, Бельфер Р.А.⁹, Кравцов А.В.¹⁰

На кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана совместно с Научно-исследовательским испытательным центром ЦНИИ МО РФ с 2017 года проводится работа по созданию учебного лабораторного стенда (УЛС) имитатора объединенной сети передачи данных (ПД) специального назначения с обеспечением высоких требований по надежности, информационной безопасности и другим показателям. Разработанный в настоящее время одноуровневый учебный имитатор объединенной сети ПД не позволяет моделировать установление соединений и передачу данных между оконечными пунктами, территориально расположенными в разных регионах страны. Поставлена задача создать такой усовершенствованный учебный имитатор объединенной сети. Предложена иерархическая структура такой сети и основанного на ней учебного имитатора (в качестве примера) с одноуровневым учебным имитатором в качестве одного из блоков. По сравнению с одноуровневым учебным имитатором перед усовершенствованным имитатором поставлены задачи по выполнению дополнительных технологических и эксплуатационных функций.

Ключевые слова: имитатор объединенной сети (united network simulator), иерархическая структура (hierarchical structure), частная сеть (private network), информационная безопасность (information security), сеть передачи данных (data transmission network).

Введение

В резолюции IV конференции «Информационные технологии на службе оборонно-промышленного комплекса России-2015» отмечается, что в качестве одного из основных направлений развития информационно-коммуникационных инфраструктур в интересах ОПК по-прежнему является отечественная разработка сетей передачи данных [1]. Для решения задач в этой области конференция отмечает на необходимость “активизации взаимодействия научно-образовательных, образовательных организаций и предприятий ОПК по вопросам проведения исследовательской деятельности и подготовки ИТ-специалистов в интересах ОПК”. Цель создания УЛС имитатора объединенной сети – получение студентами знаний и опыта для работы по созданию такой отечественной действующей сети.

На кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана совместно с Научно-исследовательским испытательным центром ЦНИИ Войск ВКО МО РФ с 2017 года проводится работа по созданию учебного лабораторного стенда (УЛС) имитатора объединенной сети передачи данных (ПД) специального назначения.

Конференция [1] отмечает, что сегодня на повестке дня остро стоит необходимость создания единой системы объединенных коммуникаций в сфере ОПК, чтобы не создавать отдельную систему ПД под каждую систему вооружения. Это позволит сократить стоимость и сроки создания боевых технических средств. Этому же будет способствовать так же создание единой системы объединенных сетей ПД не только для ОПК. В соответствии с классификацией ФЗ «О связи» (п.16) сети связи специального назначения предназначены «для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка». Об актуальности включения в объединенную

⁸ Басараб Михаил Алексеевич, д.ф.-м.н., заведующий кафедрой «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва bmic@mail.ru

⁹ Бельфер Рувим Абрамович, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, a.belfer@yandex.ru

¹⁰ Кравцов Александр Владимирович, начальник отдела НИИЦ (Москва) ЦНИИ ВВКО, skyak78@gmail.com

сеть частные сети МВД свидетельствует атака злоумышленников на внутренние сети этого ведомства, имевшая место 12 мая 2017 года (газета "Московский Комсомолец", 15 мая, 2017г.).

Итак, под объединенной сетью понимается создание единой сети, включающей несколько изолированных (частных сетей, ЧС) ПД имитатора специального назначения для некоторых ведомств из указанных в категории сетей специального назначения.

Цель создания УЛС имитатора объединенной сети – получение студентами знаний и опыта для работы по созданию такой отечественной действующей сети.

Разработанный в настоящее время одноуровневый учебный имитатор объединенной сети ПД не позволяет моделировать установление соединений между конечными пунктами, территориально расположенными в разных регионах страны. В настоящем докладе предлагается другая структура сети ПД и соответственно структура учебного имитатора этой сети, которые позволяют исправить этот недостаток.

Структура объединенной сети ПД категории специального назначения

Междугородная мультимедийная сеть связи общего пользования ТфОП/ISDN построена на иерархической двухуровневой структуре, что позволяет устанавливать соединения и передавать речь или данные между конечными пунктами, расположенными в разных субъектах РФ [2]. Нижний уровень представляет автоматические междугородные телефонные станции регионов страны АМТС, верхний уровень представляет узлы автоматической коммутации (УАК), выполняющий функции транзитных станций. Все УАК соединяются между собой по принципу “каждый с каждым”. Любая АМТС должна быть связана, как минимум с двумя УАК. На ТфОП/ISDN России установлено 8 коммутаторов, расположенных в Москве, Санкт-Петербурге, Екатеринбурге, Новосибирске, Ростов-на-Дону, Хабаровске и других городах.

На рис. 1 приведен пример структуры объединенной сети ПД специального назначения, построенной по приведенному принципу междугородной сети страны.

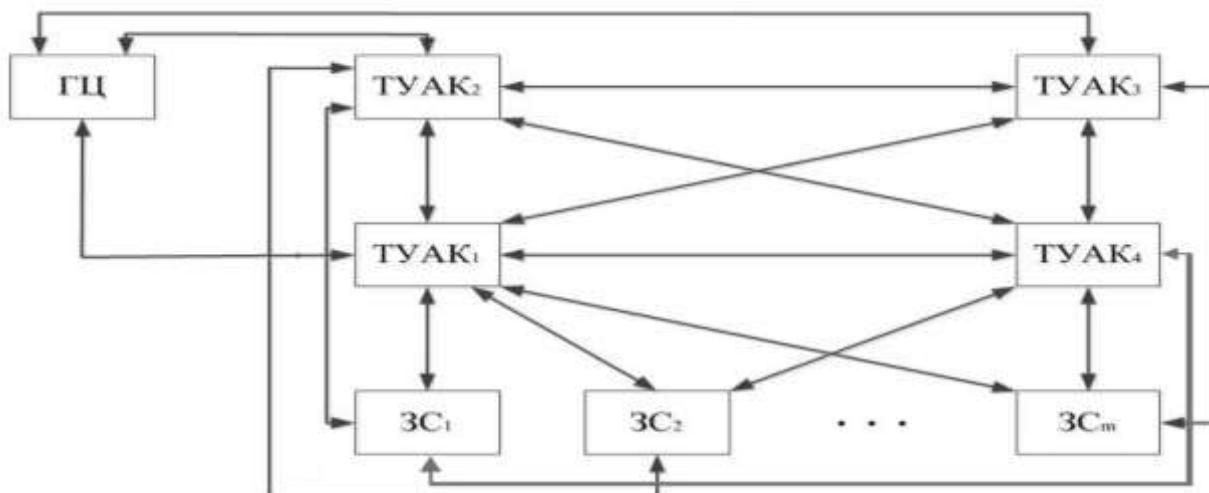


Рис. 1. Пример иерархической структуры сети ПД специального назначения страны

Нижний уровень включает зоновые сети (ЗС), территориально расположенные в разных субъектах федерации страны. Каждая такая ЗС, включает зоновый центр эксплуатации ЦЭС, один или несколько конечных пунктов (ОП), может включать узлы коммутации УК. ОП в зоновой сети могут принадлежать одной или разным частным сетям (ЧС). Число

ЗС, территориальное расположение каждой ЗС, состав устройств и конфигурация взаимодействующих в них устройств определяется в процессе проектирования сети ПД. ЗС соединена с узлами коммутации верхнего уровня (транзитными узлами автоматической коммутации ТУАК). Соединение между устройствами разных ЗС осуществляется через эти транзитные коммутаторы. На рис. 1 в качестве примера показаны четыре ТУАК - ТУАК₁, ТУАК₂, ТУАК₃, ТУАК₄. Коммутация осуществляется по принципу междугородной сети ТфОП/ISDN с помощью нескольких транзитных узлов автоматической коммутации (ТУАК), соединенных «каждый с каждым». По причине высоких требований к надежности объединенных сетей ПД специального назначения каждая ЗС соединена с тремя или четырьмя ЗС. Это позволяет устанавливать каждое транзитное соединение по пучку маршрутов с последующей передачей одного и того же сообщения соответственно по трем или четырем путям маршрутизации. На рис. 1 показано соединение каждого ЗС с тремя ТУАК. В качестве примера покажем один из возможных пучков соединения между оконечными пунктами ЗС₂ и ЗС_м, состоящий из трех путей маршрутизации:

ЗС₂ - ТУАК₁ – ЗС_м; ЗС₂ - ТУАК₂ – ТУАК₃ - ЗС_м; ЗС₂ - ТУАК₄ – ЗС_м.

Число ТУАК и каналов связи между ЗС и ТУАК определяется при разработке имитатора сети ПД.

На верхнем уровне установлены так же головные центры ГЦ, включающие не показанные на рис.1 головные центры каждой частной сети ГЦЧ (ГЦЧ₁, ГЦЧ₂.....ГЦЧ_n) и общий центр ОЦ для всех частных сетей. Эти головные центры соединяются с зонавыми сетями через узлы коммутации ТУАК. ГЦЧ обеспечивает соединение с оконечными пунктами ЗС одной из частных сетей. ОЦ соединяется с оконечными пунктами разных частных сетей (смешанное соединение).

Имитатор объединенной сети ПД специального назначения иерархической структуры

На рис. 2 приведен пример иерархической структуры имитатора объединенной сети ПД специального назначения, в основу которой положена приведенная на рис. 1 структура объединенной сети ПД страны..

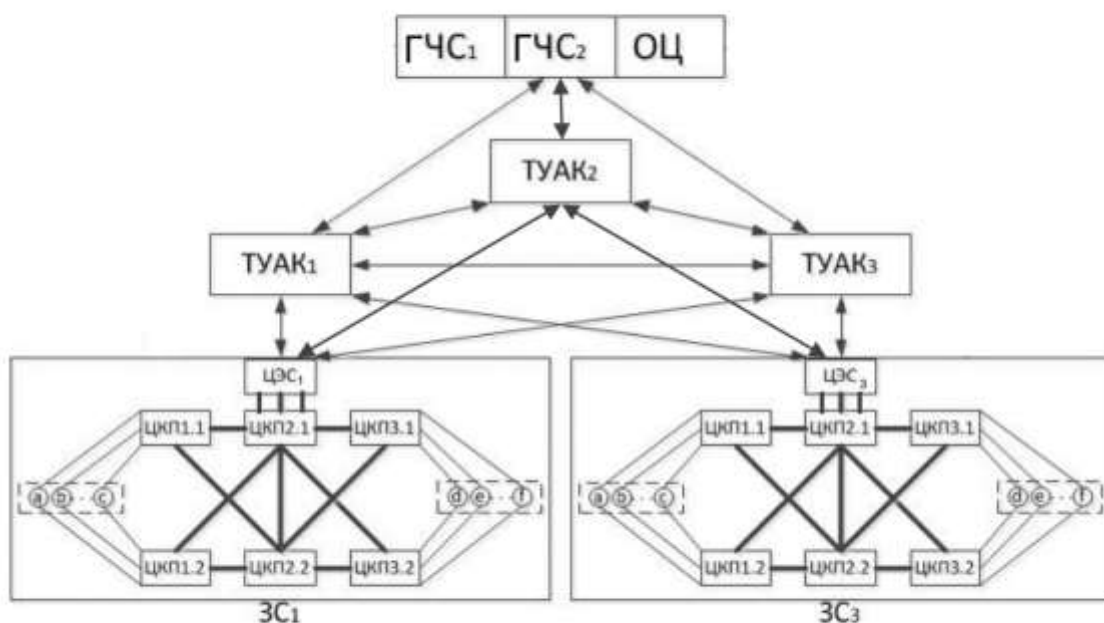


Рис. 2. Пример иерархической структуры имитатора сети ПД специального назначения

Приведенная структура служит для создания усовершенствованного имитатора объединенной сети ПД специального назначения. Иерархическая структура сети позволяет устранить недостаток разработанного одноуровневого учебного имитатора ПД, который состоит в невозможности установления соединений между оконечными пунктами, расположенными в разных регионах страны. Как видно из рис.2, усовершенствованный имитатор включает на верхнем уровне три транзитных узла коммутации (ТУАК₁, ТУАК₂, ТУАК₃), головные центры первой и второй частных сетей (ГЧС₁ и ГЧС₂), общий центр эксплуатации (ОЦ), первую и третью зоновые сети (ЗС₁ и ЗС₃). Конфигурация и состав устройств этих зоновых сетей аналогичны созданному одноуровневному имитатору сети. ЗС этого имитатора и состоит из зонового центра эксплуатации сети, шести центров коммутации пакетов (ЦКП), оконечных пунктов (a,b,...,c и d,e,...,f). В отличие от задачи создания усовершенствованного имитатора одноуровневый имитатор позволяет устанавливать соединения и передавать пакеты данных только между ОП одного ЗС. Некоторые из научно-практических результатов, полученные на одноуровневом имитаторе объединенной сети могут быть использованы при создании учебного имитатора иерархической структуры. Это относится к разработанным алгоритмам с обеспечением высоких требований по надежности и информационной безопасности, к построению программного обеспечения [3-7]:

- по установлению/разъединению коммутируемых виртуальных каналов (КВК) в разных частных сетях между ОП, принадлежащих одной и той же частной сети и между ОП разных частных сетей;
- передача пакета данных по установленным КВК.

Надежность обеспечивается передачей сообщения по пучку маршрутов из четырех некоррелированных к помехам путей маршрутизации. Информационная безопасность обеспечивается имитацией канального, сквозного шифрования и контролем целостности на абонентских доступах и на участках транспортной части сети. Высокие требования

к информационной безопасности сетей ПД категории специального назначения выполняются не стандартизированными механизмами защиты, которые разрабатывают отечественные специализированные научно-практические организации. В рамках УЛС имитатора сети ПД стоит другая задача – провести исследования и предложить в разрабатываемых алгоритмах основные положения ИБ, учитывающие особенности объединенной сети ПД специального назначения. Это относится к использованию ключей и механизмов безопасности для разных частных сетей и на разных участках соединений. При этом используются результаты анализа зарубежных работ сетей с высокими требованиями к безопасности: в сетях связи - интеллектуальной энергосистемы Smart Grid [8], VPN на базе MPLS (VPRN) [9], общеканальной сигнализации ОКС№7 [10, 11] и др. В разработанных алгоритмах одноуровневого имитатора объединенной сети ПД предусмотрена возможность обеспечить дифференцированный подход к требованиям информационной безопасности для разных частных сетей (периодичность смены ключей, создание одноразовых ключей, смена механизмов безопасности).

Предложенные для одноуровневого имитатора централизованный алгоритм принудительной маршрутизации (“от источника”) так же может быть использован в зонной сети усовершенствованного маршрутизатора [12].

Функции имитатора объединенной сети ПД иерархической структуры

По сравнению с одноуровневым учебным имитатором перед усовершенствованным имитатором поставлены задачи по выполнению дополнительных технологических и эксплуатационных функций.

Технологические функции

Перед усовершенствованным имитатором объединенной сети ПД категории специального назначения стоит задача разработать алгоритм и смоделировать установление трех видов соединений оконечных пунктов одной из частных сетей - одноадресных и групповых (многоадресных и широковещательных). Одноадресное соединение устанавливается между головными центрами частных сетей (ГЦЧ) и оконечными пунктами зонных сетей или по команде из ГЦЧ в центр эксплуатации зонной сети ЦЭС между оконечными пунктами в разных или одной ЗС. При установлении групповых соединений ГЦЧ передает групповые адреса только один раз, затем они тиражируются и доставляются только по тем адресам, которые соответствуют оконечным пунктам определенной частной сети. Как было отмечено выше, перед усовершенствованным имитатором стоит задача установления еще одного вида одноадресного соединения – смешанного. При этом по команде из общего центра ОЦ соединение устанавливается между оконечными пунктами разных частных сетей.

Приведем примеры путей маршрутизации двух одноадресных соединений КВК в усовершенствованном имитаторе объединенной сети ПД категории специального назначения (структуры рис.2). Примем, что в ЗС1 входят оконечный пункт a (ОПа) ЧС₁, оконечный пункт b (ОП_b) ЧС₂, а в ЗС₃ - оконечный пункт f (ОП_f) ЧС₂ и оконечный пункт d ЧС₁.

Пример 1. Одноадресное соединение в ЗС1 между ГЧС₁ и оконечным пунктом a (ОПа) ЗС₁.

В сообщении ГЧС₁ указываются адреса ЗС₁ и ОПа. Приведем три пути маршрутизации КВК: 1) ГЧС₁ – ТУАК₁ – ЦЭС₁ – ЦКП 2.1 - ЦКП 1.1 – ОПа; 2) ГЧС₁ – ТУАК₂ - ЦЭС – ЦКП 2.1 - ЦКП 1.2 – ОПа;

3) ГЧС₁ – ТУАК₃ – ЦЭС₁ – ЦКП 2.1 – ЦКП 2.2- ЦКП 1.1 – Опа.

Пример 2. ГЧС₂ направляет в ЗС₁ команду на установление одноадресного соединения ЧС2 между ОП_b, входящим в ЗС₁ и ОП_f, входящим в ЗС₃. В сообщении ГЧС₂ указываются адреса ЗС₁ и ОП_b, ЗС₃ и ОП_f.

Одноадресное соединения: между ОП_b (ЗС₁) и ОП_f (ЗС₃) по команде ГЧС₂ в ОП_b (ЗС₁). В сообщении ГЧС₃ указывается ЗС₁, ОПа.и ОП_f.

Приведем три пути маршрутизации КВК от ГЧС₂ в ОП_b (ЗС₁): 1) ГЧС₂ – ТУАК₁ – ЦЭС₃ – ЦКП 2.1 - ЦКП 1.1 – ОП_b; 2) ГЧС₂ – ТУАК₂ - ЦЭС₃ – ЦКП 2.1 - ЦКП 1.2 – ОП_b;

3) ГЧС₃ – ТУАК₃ – ЦЭС₃ – ЦКП 2.1 – ЦКП 1.2 - ЦКП 1.1 – ОП_b.

Приведем три пути маршрутизации КВК от ОП_b (ЗС₁) в ОП_f (ЗС₃). 1) ОП_b – ЦКП 1.1 – ЦКП 2.1 – ЦЭС₁ - ТУАК₁ - ЦЭС₃ – ЦКП 2.1 - ЦКП 1.1 – ОП_f; 2) ОП_b – ЦКП 1.2 – ЦКП 2.1 – ЦЭС₁ - ТУАК₃ - ЦЭС₃ – ЦКП 2.1 - ЦКП 1.2 – ОП_f; 3) ОП_b – ЦКП 1.2 – ЦКП 2.2 - ЦКП 2.1 – ЦЭС₁ - ТУАК₁ - ТУАК₃ - ЦЭС₃ – ЦКП 2.1 - ЦКП 2.2 - ЦКП 1.1 – ОП_f.

Эксплуатационные функции

- Контроль технического состояния и работоспособности устройств сети.
- Контроль функционирования приведенных выше технологических процедур установления/разъединения соединения и передачи данных.
- Развитие сети ПД введением новых устройств.
- Изменение конфигурации сети.
- Обнаружение отказов устройств сети, вывод их из эксплуатации, ввод в эксплуатацию после восстановления.
- Периодическая смена параметров защиты информационной безопасности (ключей, сертификатов и др.).

Выводы

На кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана совместно с Научно-исследовательским испытательным центром ЦНИИ Войск ВКО МО РФ с 2017 года проводится работа по созданию учебного лабораторного стенда (УЛС) имитатора объединенной сети передачи данных (ПД) категории специального назначения с обеспечением высоких требований по надежности, информационной безопасности и другим показателям. Разработанный в настоящее время одноуровневый учебный имитатор объединенной сети ПД не позволяет моделировать установление соединений и передачу данных между оконечными пунктами, территориально расположенными в разных регионах страны. Поставлена задача создать такой усовершенствованный учебный имитатор объединенной сети. Предложена иерархическая структура построения такой сети ПД с оконечными пунктами на нижнем уровне в зонах сетей страны и транзитными узлами коммутации на верхнем уровне. На основе этой структуры сети страны приведена структура учебного имитатора с двумя зональными сетями, включающими одноуровневый учебный имитатор. По сравнению с одноуровневым учебным имитатором перед усовершенствованным имитатором поставлены задачи по выполнению дополнительных технологических и эксплуатационных функций. По сравнению с одноуровневым учебным имитатором перед усовершенствованным имитатором поставлены дополнительные технологические и эксплуатационные функции.

Литература

1. Резолюция конференции «Информационные технологии на службе оборонно-промышленного комплекса России 2015» // Connect. 2015. № 9. С. 78-88.
2. Гольдштейн Б.С, Соколов Н.А., Яновский Г.Г. Сети связи. «БХВ» Петербург. 2011. 400с.
3. Басараб М.А., Бельфер Р.А., Кравцов А.В., Никулина Т.П. Алгоритм аутентификации и формирования разовых ключей в имитаторе лабораторного стенда объединенной сети ПД специального назначения // Первая миля. 2019. №2. С.62-68.
4. Басараб М.А., Бельфер Р.А., Глинская Е.В., Кравцов А.В. Алгоритм защищенного установления соединения в имитаторе объединенной сети ПД специального назначения // Первая миля, 2019. №8. С.78-82.
5. Басараб М.А., Бельфер Р.А., Глинская Е.В., Кравцов А.В. Алгоритм передачи данных в имитаторе объединенной сети ПД специального назначения //Телекоммуникации и информационные технологии, 2019 . №2. С.32-36.
6. Басараб М.А., Бельфер Р.А., Кравцов А.В. Маршрутизация в объединенном имитаторе сети ПД специального назначения между оконечными пунктами разных частных сетей// Электросвязь . 2019. № 3. С.51-53.
7. Басараб М.А., Бельфер Р.А., Кравцов А.В. Архитектура очередей таблиц маршрутизации объединенной сети ПД категории специального назначения// Электросвязь. 2019. № 2.С.33-37.
8. Lee Sangji, Bong Jinsuk, Shin Sunhee, Shin Yongtae. A security mechanism of Smart Grid AMI network through smart devicemutual authentication. The International Conference on Information Networking 2014 (ICOIN2014). 2014. pp. 592 – 595.
9. Michael H. Behringer, Monique J. Morrow. MPLS VPN Security Cisco Press, 2005, p.312
10. Rufa G. Developments in Telecommunications. With a Focus on SS7 Network Reliability Springer. 2009. 277 p.
11. Sengar H, Wijesekera D. Jajodia S. Authentication and Integrity in telecommunication Signaling Network. Engineering of Computer-Based Systems,12th IEEE International Conference and Workshops. 2005. pp. 163 – 170.
12. Бельфер Р.А., Макаров И.М., Никулина Т.П. Алгоритм формирования маршрутизации от источника в имитаторе сети ПД категории специального назначения. .Сборник трудов Девятой всероссийской конференции, Безопасные Информационные Технологии, 2018, С. 14-19

Training simulator of the united national special-purpose data network (structure, functions)

At the Department of "Information Security" Bauman University Since 2017, Bauman, together with the Scientific Research Testing Center of the Central Research Institute of the Ministry of Defense of the Russian Federation, has been working on the creation of a training laboratory bench for a simulator of a special purpose integrated data network with high requirements for reliability, information security and other indicators. The single-level training simulator of the integrated data network currently developed does not allow simulating the establishment of connections and data transfer between endpoints located in different regions of the country. The task is to create such an advanced training simulator of the integrated network. A hierarchical structure of such a network and an educational simulator based on it is proposed (as an example) with a single-level educational simulator as one of the blocks. Compared with a single-level training simulator, the advanced simulator is tasked with performing additional technological and operational functions.

Использование линейной фильтрации дискретного сигнала в аддитивном шуме по двум каналам передачи информации для улучшения его корреляционного приема

Басараб М. А.¹¹, Троицкий И.И.¹², Якубов Р.Ж.¹³

В статье исследуется возможность улучшения корреляционного приема дискретного сигнала в аддитивном шуме на основе использования его линейной фильтрации по двум каналам передачи информации. Шумы в исследуемых каналах передачи информации статистически связаны между собой. Для улучшения показателей корреляционного приема предлагается использовать механизм линейной фильтрации, рассмотренный в предыдущих работах авторов. Для проведения исследований использовалась модель дискретного коррелятора, который имеет два входа и один выход. Исследования проводились для двух случаев каналов передачи информации. Первый случай - наличие дискретного сигнала только в одном канале передачи информации, второй случай – в обоих каналах. Полученные результаты позволяют сравнить показатели корреляционного приема для различных случаев и убедиться в целесообразности применения линейной фильтрации.

Ключевые слова: корреляционный прием, линейная фильтрация, аддитивный шум, каналы передачи информации, дискретный сигнал.

Введение

В настоящее время корреляционный прием является одним из самых эффективных методов распознавания дискретного сигнала в аддитивном шуме [1-6]. Он широко используется в телемедицине, мобильной связи и т.д. В статье исследуется возможность применения линейной фильтрации к двум статистически зависимым каналам передачи информации [7-10] для улучшения показателей корреляционного приема дискретного сигнала.

Для проведения исследований использовался дискретный коррелятор, имеющий два входа и один выход. На входы коррелятора подаются исследуемые сигналы $\varphi = (\varphi_1, \varphi_2, \dots, \varphi_N)$ и $\omega = (\omega_1, \omega_2, \dots, \omega_N)$. На выходе коррелятора определяется статистика θ :

$$\theta = \frac{1}{N} \sum_{t=1}^N \varphi_t \omega_t, \quad (1)$$

где N – число измерений (объем выборки).

Рассмотрим сначала первый случай передачи информации по двум каналам, предполагающий наличие дискретного сигнала лишь в одном из каналов.

$$y = \frac{a}{2} \eta + \varepsilon, x = \delta, \quad (2)$$

где ε , η , δ – случайные величины, причем случайная величина η не зависит от шумов ε и δ ,

$$\eta = \begin{cases} 1, & \text{с вероятностью } 0,5 \\ -1, & \text{с вероятностью } 0,5 \end{cases}$$

$\varepsilon \sim N(0, \sigma_\varepsilon^2)$ - шум в первом канале,

$\delta \sim N(0, \sigma_\delta^2)$ - шум во втором канале,

¹¹ Басараб Михаил Алексеевич, д.ф.-м.н., профессор каф. ИУ8 МГТУ им. Н.Э. Баумана, Москва bmic@mail.ru

¹² Троицкий Игорь Иванович, к.т.н., доцент каф. ИУ8 МГТУ им. Н.Э. Баумана, Москва, iitroickiy@mail.ru

¹³ Якубов Рустам Жафарович, аспирант каф. ИУ8 МГТУ им. Н.Э. Баумана, Москва, yakubov_rustam@inbox.ru

$a = |m_1^{(1)} - m_{-1}^{(1)}|$ - сигнал в первом канале,

$N(m, \sigma^2)$ - нормальный закон распределения с параметрами (m, σ^2) .

Условные плотности распределения вероятностей $P(y/\eta = 1)$, $P(y/\eta = -1)$ имеют нормальный закон с соответствующими параметрами $N(m_1^{(1)}, \sigma_\varepsilon^2)$ и $N(m_{-1}^{(1)}, \sigma_\varepsilon^2)$.

Для сокращения выкладок перейдем к нормированным случайным величинам:

$$\hat{y} = \frac{a}{2\sigma_\varepsilon} + \frac{\varepsilon}{\sigma_\varepsilon} = \frac{a}{2\sigma_\varepsilon} + \hat{\varepsilon}, \quad \hat{x} = \frac{\delta}{\sigma_\delta} = \hat{\delta} \quad (3)$$

Тогда линейная фильтрация дискретного сигнала будет иметь следующий вид:

$$\hat{z} = \hat{y} + c\hat{x} = \frac{a}{2\sigma_\varepsilon}\eta + \hat{\varepsilon} + c\hat{\delta}, \quad (4)$$

где $\hat{z}$ - результирующий сигнал, c - неизвестный параметр.

Сравним несколько вариантов работы дискретного коррелятора:

а) На один вход коррелятора подадим сигнал $\hat{y}$, на другой - сигнал η . Сигнал выхода коррелятора умножим на 2, в этом случае будет вычислена статистика L_1 :

$$L_1 = \frac{2}{N} \sum_{t=1}^N \eta_t \hat{y}_t = \frac{2}{N} \sum_{t=1}^N \eta_t \left(\frac{a \cdot \eta_t}{2\sigma_\varepsilon} + \hat{\varepsilon}_t \right) \quad (5)$$

Определим математическое ожидание и дисперсию статистики L_1 :

$$M[L_1] = M \left[\frac{2}{N} \sum_{t=1}^N \eta_t \left(\frac{a\eta_t}{2\sigma_\varepsilon} + \hat{\varepsilon}_t \right) \right] = \frac{2}{N} \sum_{t=1}^N M \left[\eta_t \left(\frac{a\eta_t}{2\sigma_\varepsilon} + \hat{\varepsilon}_t \right) \right] \quad (6)$$

Рассмотрим одно слагаемое суммы (6)

$$M \left[\eta_t \left(\frac{a \cdot \eta_t}{2\sigma_\varepsilon} + \hat{\varepsilon}_t \right) \right] = M \left[\frac{a}{2\sigma_\varepsilon} \cdot \eta_t^2 \right] + M[\eta_t \hat{\varepsilon}_t] = \frac{a}{2\sigma_\varepsilon} \quad (7)$$

Тогда $M[L_1] = \frac{a}{\sigma_\varepsilon}$, что является отношением сигнал/шум для канала y .

Дисперсия статистики L_1 :

$$D[L_1] = D \left[\frac{2}{N} \sum_{t=1}^N \left(\frac{a}{2\sigma_\varepsilon} \eta_t^2 + \eta_t \hat{\varepsilon}_t \right) \right] = \frac{4}{N^2} \sum_{t=1}^N D \left[\frac{a\eta_t^2}{2\sigma_\varepsilon} + \eta_t \hat{\varepsilon}_t \right] \quad (8)$$

Также рассмотрим одно слагаемое суммы (8)

$$D \left[\frac{a\eta_t^2}{2\sigma_\varepsilon} + \eta_t \hat{\varepsilon}_t \right] = D[\eta_t \hat{\varepsilon}_t] = M[\eta_t^2 \hat{\varepsilon}_t^2] = 1,$$

поскольку $\frac{a\eta_t^2}{2\sigma_\varepsilon}$ не является случайной величиной. Тогда $D[L_1] = \frac{4}{N}$

б) Теперь на один вход коррелятора подадим результирующий сигнал $\hat{z}$, а на второй сигнал η .

Сигнал выхода коррелятора умножим на 2, в этом случае будет вычислена статистика L_2 :

$$L_2 = \frac{2}{N} \sum_{t=1}^N \eta_t \hat{z}_t = \frac{2}{N} \sum_{t=1}^N \eta_t \left(\frac{a\eta_t}{2\sigma_\varepsilon} + \hat{\varepsilon}_t + c\hat{\delta}_t \right) \quad (9)$$

Найдем математическое ожидание и дисперсию статистики L_2 :

$$M[L_2] = \frac{2}{N} \sum_{t=1}^N \eta_t \hat{z}_t = \frac{2}{N} \sum_{t=1}^N M \left[\eta_t^2 \frac{a}{2\sigma_\varepsilon} + \eta_t \hat{\varepsilon}_t + c\eta_t \hat{\delta}_t \right] = \frac{a}{\sigma_\varepsilon} \quad (10)$$

$$\begin{aligned} D[L_2] &= D \left[\frac{2}{N} \sum_{t=1}^N \left(\eta_t^2 \frac{a}{2\sigma_\varepsilon} + \eta_t \hat{\varepsilon}_t + c\eta_t \hat{\delta}_t \right) \right] = \\ &= \frac{4}{N^2} \sum_{t=1}^N D \left[\eta_t^2 \frac{a}{2\sigma_\varepsilon} + \eta_t \hat{\varepsilon}_t + c\eta_t \hat{\delta}_t \right] = \\ &= \frac{4}{N^2} \sum_{t=1}^N D[\eta_t \hat{\varepsilon}_t + c\eta_t \hat{\delta}_t] \end{aligned} \quad (11)$$

Рассмотрим одно слагаемое суммы (11):

$$D[\eta_t \varepsilon_t + c\eta_t \delta_t] = D[\eta_t \varepsilon_t] + D[c\eta_t \delta_t] + 2cov(\eta_t \varepsilon_t, c\eta_t \delta_t) \quad (12)$$

Определим каждое слагаемое выражения (12) по отдельности:

$$D[\eta_t \varepsilon_t] = M[\eta_t^2 \varepsilon_t^2] - \{M[\eta_t \varepsilon_t]\}^2 = 1 \quad (13)$$

$$D[c\eta_t \delta_t] = M[c^2 \eta_t^2 \delta_t^2] - \{M[c\eta_t \delta_t]\}^2 = c^2 \quad (14)$$

$$2cov(\eta_t \varepsilon_t, c\eta_t \delta_t) = 2M[c\eta_t^2 \varepsilon_t \delta_t] = 2cr_{\varepsilon\delta}, \quad (15)$$

где $r_{\varepsilon\delta}$ – коэффициент корреляции между случайными величинами ε и δ . Тогда

$$D[L_2] = \frac{4}{N} (1 + c^2 + 2cr_{\varepsilon\delta}) \quad (16)$$

Определим значение параметра c , при котором дисперсия $D[L_2]$ принимает наименьшее значение. Нетрудно показать, что дисперсия минимальна при значении $c = -r_{\varepsilon\delta}$. В этом случае она принимает значение:

$$\hat{D}[L_2] = \frac{4}{N} (1 - r_{\varepsilon\delta}^2) \quad (17)$$

Следовательно, $\hat{D}[L_2] \leq D[L_1]$, их равенство достигается при $r_{\varepsilon\delta} = 0$.

Случай равенства $r_{\varepsilon\delta} = \pm 1$ не рассматривается, поскольку в этом случае нет необходимости использовать корреляционный прием (вероятность распознавания дискретного сигнала равна единице).

в) На один вход коррелятора подается сигнал $\hat{y}$, на другой сигнал $\hat{x}$. Тогда на выходе коррелятора:

$$L_3 = \frac{1}{N} \sum_{t=1}^N \delta_t \left(\frac{a \cdot \eta_t}{2\sigma_\varepsilon} + \varepsilon_t \right) \quad (18)$$

Найдем математическое ожидание и дисперсию статистики L_3 :

$$M[L_3] = \frac{1}{N} \sum_{t=1}^N M \left[\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t + \varepsilon_t \delta_t \right] = \frac{1}{N} \sum_{t=1}^N r_{\varepsilon\delta} = r_{\varepsilon\delta} \quad (19)$$

$$\begin{aligned} D[L_3] &= \frac{1}{N^2} \sum_{t=1}^N D \left[\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t + \varepsilon_t \delta_t \right] = \\ &= \frac{1}{N^2} \sum_{t=1}^N \left\{ D \left[\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t \right] + D[\varepsilon_t \delta_t] \right. \\ &\quad \left. + 2cov \left(\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t, \varepsilon_t \delta_t \right) \right\} \end{aligned} \quad (20)$$

Рассмотрим каждое слагаемое суммы (20):

Первое слагаемое (20)

$$\begin{aligned} D \left[\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t \right] &= M \left[\left(\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t \right)^2 \right] - \left\{ M \left[\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t \right] \right\}^2 = \\ &= \frac{a^2}{4\sigma_\varepsilon^2} M[\eta_t^2 \delta_t^2] = \frac{a^2}{4\sigma_\varepsilon^2} \end{aligned} \quad (21)$$

Рассмотрим второе слагаемое (20)

$$D[\varepsilon_t \delta_t] = M[\varepsilon_t^2 \delta_t^2] - \{M[\varepsilon_t \delta_t]\}^2 \quad (22)$$

Пусть $\hat{r}_{\varepsilon\delta}$ – коэффициент корреляции между случайными величинами ε_t^2 и δ_t^2 .

$$\text{Тогда } \hat{r}_{\varepsilon\delta} = \frac{M[(\varepsilon_t^2 - M[\varepsilon_t^2])(\delta_t^2 - M[\delta_t^2])]}{\sqrt{D[\varepsilon_t^2]} \sqrt{D[\delta_t^2]}}$$

Вычислим

$$M[\varepsilon_t^2] = 1, M[\delta_t^2] = 1$$

$$D[\varepsilon_t^2] = M[\varepsilon_t^4] - \{M[\varepsilon_t^2]\}^2 = 2$$

$$D[\delta_t^2] = M[\delta_t^4] - \{M[\delta_t^2]\}^2 = 2$$

Следовательно, $\hat{r}_{\varepsilon\delta} = \frac{M[\varepsilon_t^2 \delta_t^2] - 1}{2}$. Отсюда

$$M[\varepsilon_t^2 \delta_t^2] = 1 + 2\hat{r}_{\varepsilon\delta} \quad (23)$$

Итак, второе слагаемое (22) равно

$$D[\varepsilon_t \delta_t] = 1 + 2\hat{r}_{\varepsilon\delta} - r_{\varepsilon\delta}^2 \quad (24)$$

Третье слагаемое (22)

$$\begin{aligned} 2cov\left(\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t, \varepsilon_t \delta_t\right) &= \\ &= 2M\left[\left(\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t - M\left[\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t\right]\right)(\varepsilon_t \delta_t - M[\varepsilon_t \delta_t])\right] = \\ &= 2M\left[\frac{a}{2\sigma_\varepsilon} \eta_t \varepsilon_t \delta_t^2 - \frac{a}{2\sigma_\varepsilon} \eta_t \delta_t r_{\varepsilon\delta}\right] = 0 \end{aligned} \quad (25)$$

Тогда

$$D\left[\frac{a}{2\sigma_\varepsilon} \eta_t \delta_t + \varepsilon_t \delta_t\right] = \frac{a^2}{4\sigma_\varepsilon^2} + 1 + 2\hat{r}_{\varepsilon\delta} - r_{\varepsilon\delta}^2 \quad (26)$$

Следовательно, дисперсия статистики L_3 равна

$$D[L_3] = \frac{\frac{a^2}{4\sigma_\varepsilon^2} + 1 + 2\hat{r}_{\varepsilon\delta} - r_{\varepsilon\delta}^2}{N} \quad (27)$$

Рассмотрим второй случай, когда в каждом канале есть сигнал и шум:

$$y = \frac{a}{2}\eta + \varepsilon, x = \frac{b}{2}\eta + \delta. \quad (28)$$

Описание случайных величин $\varepsilon, \delta, \eta$ совпадает с их описанием для первого случая, за исключением того, что в канале x будет сигнал. Введем обозначения:

$a = |m_1^{(y)} - m_{-1}^{(y)}|$ - сигнал в первом канале,

$b = |m_1^{(x)} - m_{-1}^{(x)}|$ - сигнал во втором канале.

Пусть условные плотности распределения вероятностей $P(y/\eta = 1), P(y/\eta = -1), P(x/\eta = 1), P(x/\eta = -1)$ будут распределены по нормальным законам распределения $N(m_1^{(y)}, \sigma_\varepsilon^2), N(m_{-1}^{(y)}, \sigma_\varepsilon^2), N(m_1^{(x)}, \sigma_\delta^2)$ и $N(m_{-1}^{(x)}, \sigma_\delta^2)$, соответственно.

Как и в предыдущем случае, введем нормированные случайные величины:

$$\begin{aligned} \hat{y} &= \frac{\frac{a}{2}\eta}{\sigma_\varepsilon} + \frac{\varepsilon}{\sigma_\varepsilon} = \frac{\frac{a}{2}\eta}{\sigma_\varepsilon} + \hat{\varepsilon}, \text{ где } \hat{\varepsilon} = \frac{\varepsilon}{\sigma_\varepsilon} \\ \hat{x} &= \frac{\frac{b}{2}\eta}{\sigma_\delta} + \frac{\delta}{\sigma_\delta} = \frac{\frac{b}{2}\eta}{\sigma_\delta} + \hat{\delta}, \text{ где } \hat{\delta} = \frac{\delta}{\sigma_\delta} \end{aligned}$$

Применив линейную фильтрацию, получим результирующий сигнал $\hat{z}$:

$$\hat{z} = \hat{y} + c\hat{x} = \frac{a}{2\sigma_\varepsilon}\eta + \frac{cb}{2\sigma_\delta}\eta + \hat{\varepsilon} + c\hat{\delta}, \quad (29)$$

где c – неизвестный параметр.

Рассмотрим различные случаи работы дискретного коррелятора.

а) На один вход коррелятора подается сигнал $\hat{y}$, на другой сигнал η . Сигнал выхода коррелятора умножим на 2, в этом случае будет вычислена статистика $\widehat{L}_1$:

$$\widehat{L}_1 = \frac{2}{N} \sum_{t=1}^N \eta_t \hat{y}_t = \frac{2}{N} \sum_{t=1}^N \eta_t \left(\frac{a\eta_t}{2\sigma_\varepsilon} + \hat{\varepsilon}_t \right) \quad (30)$$

Нетрудно показать, что $M[\widehat{L}_1] = \frac{a}{\sigma_\varepsilon}, D[\widehat{L}_1] = \frac{4}{N}$

б) На один вход коррелятора подается сигнал $\hat{x}$, на другой сигнал η . Сигнал выхода коррелятора умножим на 2, в этом случае будет вычислена статистика $\widehat{L}_2$:

$$\widehat{L}_2 = \frac{2}{N} \sum_{t=1}^N \eta_t \hat{x}_t = \frac{2}{N} \sum_{t=1}^N \eta_t \left(\frac{b \cdot \eta_t}{2\sigma_\delta} + \delta_t \right) \quad (31)$$

Нетрудно показать, что $M[\widehat{L}_2] = \frac{b}{\sigma_\delta}$, $D[\widehat{L}_2] = \frac{4}{N}$

Для наилучших показателей корреляционного приема выбираем тот канал передачи информации, у которого большее отношение сигнал/шум $\left(\frac{a}{\sigma_\varepsilon}, \frac{b}{\sigma_\delta} \right)$.

в) На один вход коррелятора подается результирующий сигнал $\hat{z}$, на другой сигнал η . Сигнал выхода коррелятора умножим на 2, в этом случае будет вычислена статистика $\widehat{L}_3$:

$$\widehat{L}_3 = \frac{2}{N} \sum_{t=1}^N \eta_t \hat{z}_t = \frac{2}{N} \sum_{t=1}^N \eta_t \left(\frac{a}{2\sigma_\varepsilon} \eta_t + \varepsilon_t + \frac{cb\eta_t}{2\sigma_\delta} + c\delta_t \right) \quad (32)$$

Найдем математическое ожидание и дисперсию статистики $\widehat{L}_3$:

$$\begin{aligned} M[\widehat{L}_3] &= M \left[\frac{2}{N} \sum_{t=1}^N \eta_t \left(\frac{a}{2\sigma_\varepsilon} \eta_t + \varepsilon_t + \frac{cb\eta_t}{2\sigma_\delta} + c\delta_t \right) \right] = \\ &= \frac{2}{N} \sum_{t=1}^N M \left[\frac{a}{2\sigma_\varepsilon} \eta_t^2 + \varepsilon_t \eta_t + \frac{cb}{2\sigma_\delta} \eta_t^2 + c\delta_t \eta_t \right] \end{aligned} \quad (33)$$

Рассмотрим одно слагаемое выражения (33)

$$M \left[\frac{a}{2\sigma_\varepsilon} \eta_t^2 + \varepsilon_t \eta_t + \frac{cb}{2\sigma_\delta} \eta_t^2 + c\delta_t \eta_t \right] = \frac{a}{2\sigma_\varepsilon} + \frac{cb}{2\sigma_\delta} \quad (34)$$

Тогда $M[\widehat{L}_3] = \frac{a}{\sigma_\varepsilon} + \frac{cb}{\sigma_\delta}$. Теперь вычислим дисперсию статистики $\widehat{L}_3$

$$\begin{aligned} D[\widehat{L}_3] &= D \left[\frac{2}{N} \sum_{t=1}^N \left(\frac{a}{2\sigma_\varepsilon} \eta_t^2 + \varepsilon_t \eta_t + \frac{cb}{2\sigma_\delta} \eta_t^2 + c\delta_t \eta_t \right) \right] = \\ &= \frac{4}{N^2} \sum_{t=1}^N D \left[\frac{a}{2\sigma_\varepsilon} \eta_t^2 + \varepsilon_t \eta_t + \frac{cb}{2\sigma_\delta} \eta_t^2 + c\delta_t \eta_t \right] = \\ &= \frac{4}{N^2} \sum_{t=1}^N D[\varepsilon_t \eta_t + c\delta_t \eta_t] = \frac{4}{N} (1 + c^2 + 2cr_{\varepsilon\delta}) \end{aligned} \quad (35)$$

Для определения значения параметра c вычислим аналог отношения сигнал/шум

$$R_z = \frac{\left| \frac{a}{\sigma_\varepsilon} + c \frac{b}{\sigma_\delta} \right|}{\frac{2}{\sqrt{N}} \sqrt{1 + c^2 + 2cr_{\varepsilon\delta}}} \quad (36)$$

В [8] показано, что максимум выражения (36) достигается при $c = \frac{r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} \frac{b}{\sigma_\delta}}{r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon}}$ и равен

$$\begin{aligned} \widehat{R}_z &= \\ &= \frac{\left| \frac{a}{\sigma_\varepsilon} \left(r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right) + \frac{b}{\sigma_\delta} \left(r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} - \frac{b}{\sigma_\delta} \right) \right|}{\frac{2}{\sqrt{N}} \sqrt{\left(r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right)^2 + \left(r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} - \frac{b}{\sigma_\delta} \right)^2 + 2r_{\varepsilon\delta} \left(r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right) \left(r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} - \frac{b}{\sigma_\delta} \right)}} \end{aligned} \quad (37)$$

Рассмотрим частный случай: пусть $r_{\varepsilon\delta} = 0$. Следовательно, из уравнения (37) имеем

$$\begin{aligned}\widehat{R_z} &= \frac{a}{\sigma_\varepsilon \frac{2}{\sqrt{N}}} \sqrt{1 + \left(\frac{\sigma_\varepsilon b}{a \sigma_\delta} \right)^2} = \\ &= \frac{b}{\sigma_\delta \frac{2}{\sqrt{N}}} \sqrt{1 + \left(\frac{b \sigma_\delta}{a \sigma_\varepsilon} \right)^2} > \max \left(\frac{a}{\sigma_\varepsilon \frac{2}{\sqrt{N}}}, \frac{b}{\sigma_\delta \frac{2}{\sqrt{N}}} \right)\end{aligned}\quad (38)$$

Из последней формулы следует, что даже в случае, когда $r_{\varepsilon\delta} = 0$, есть выигрыш в соотношении сигнал/шум.

Теперь докажем, что если использовать два канала, то отношение сигнал/шум в любом случае будет выше, чем в одном канале:

$$\text{Пусть } \frac{a}{\sigma_\varepsilon} \left(r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right) + \frac{b}{\sigma_\delta} \left(r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} - \frac{b}{\sigma_\delta} \right) > 0 \text{ и } \frac{b}{\sigma_\delta} > \frac{a}{\sigma_\varepsilon}$$

Необходимо доказать неравенство:

$$\begin{aligned}& \frac{a}{\sigma_\varepsilon} \left(r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right) + \frac{b}{\sigma_\delta} \left(r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} - \frac{b}{\sigma_\delta} \right) \\ & \sqrt{\left(r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right)^2 + \left(r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} - \frac{b}{\sigma_\delta} \right)^2 + 2r_{\varepsilon\delta} \left(r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right) \left(r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} - \frac{b}{\sigma_\delta} \right)} \\ & \geq \frac{b}{\sigma_\delta}\end{aligned}\quad (39)$$

После несложных вычислений получаем, что неравенство (39) принимает следующий вид:

$$\left(\frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right)^2 + \frac{2ab(1 - r_{\varepsilon\delta})}{\sigma_\varepsilon \sigma_\delta} \geq 0 \quad (40)$$

Аналогично доказывается неравенство для случая, когда

$$\frac{a}{\sigma_\varepsilon} \left(r_{\varepsilon\delta} \frac{b}{\sigma_\delta} - \frac{a}{\sigma_\varepsilon} \right) + \frac{b}{\sigma_\delta} \left(r_{\varepsilon\delta} \frac{a}{\sigma_\varepsilon} - \frac{b}{\sigma_\delta} \right) < 0 \quad (41)$$

г) Теперь на один вход коррелятора подается сигнал $\hat{y}$, на другой сигнал $\hat{x}$.

Тогда на выходе коррелятора

$$\widehat{L_4} = \frac{1}{N} \sum_{t=1}^N \left(\frac{a \cdot \eta_t}{2\sigma_\varepsilon} + \xi_t \right) \left(\frac{b \cdot \eta_t}{2\sigma_\delta} + \delta_t \right) \quad (42)$$

Найдем математическое ожидание статистики $\widehat{L_4}$:

$$\begin{aligned}M[\widehat{L_4}] &= \frac{1}{N} \sum_{t=1}^N M \left[\frac{ab}{2\sigma_\varepsilon 2\sigma_\delta} \eta_t^2 + \frac{a}{2\sigma_\varepsilon} \delta_t \eta_t + \frac{b}{2\sigma_\delta} \xi_t \eta_t + \xi_t \delta_t \right] = \\ &= \frac{1}{N} \sum_{t=1}^N \left(\frac{ab}{4\sigma_\varepsilon \sigma_\delta} + r_{\varepsilon\delta} \right) = \frac{ab}{4\sigma_\varepsilon \sigma_\delta} + r_{\varepsilon\delta}\end{aligned}\quad (43)$$

Статистика $\widehat{L_4}$ является смещенной оценкой, поэтому рассмотрим статистику

$$\widehat{L_5} = \widehat{L_4} - \frac{ab}{4\sigma_\varepsilon \sigma_\delta} \quad (44)$$

Тогда $M[\widehat{L_5}] = r_{\varepsilon\delta}$. Теперь вычислим дисперсию статистики $\widehat{L_5}$

$$\begin{aligned}D[\widehat{L_5}] &= \frac{1}{N^2} \sum_{t=1}^N D \left[\frac{a}{2\sigma_\varepsilon} \delta_t \eta_t + \frac{b}{2\sigma_\delta} \xi_t \eta_t + \xi_t \delta_t \right] = \frac{1}{N^2} \sum_{t=1}^N \left\{ D \left[\frac{a}{2\sigma_\varepsilon} \delta_t \eta_t \right] + \right. \\ & D \left[\frac{b}{2\sigma_\delta} \xi_t \eta_t \right] + D[\xi_t \delta_t] + 2cov \left(\frac{a}{2\sigma_\varepsilon} \delta_t \eta_t, \frac{b}{2\sigma_\delta} \xi_t \eta_t \right) + \\ & \left. 2cov \left(\frac{a}{2\sigma_\varepsilon} \delta_t \eta_t, \xi_t \delta_t \right) + 2cov \left(\frac{b}{2\sigma_\delta} \xi_t \eta_t, \xi_t \delta_t \right) \right\}\end{aligned}\quad (45)$$

Рассмотрим каждое слагаемое выражения (45)

$$\begin{aligned}
D\left[\frac{a}{2\sigma_\varepsilon}\delta_t\eta_t\right] &= \frac{a^2}{4\sigma_\varepsilon^2}; D\left[\frac{b}{2\sigma_\delta}\xi_t\eta_t\right] = \frac{b^2}{4\sigma_\delta^2}; D[\xi_t\delta_t] = 1 + 2\hat{r}_{\varepsilon\delta} - r_{\varepsilon\delta}^2; \\
2cov\left(\frac{a}{2\sigma_\varepsilon}\delta_t\eta_t, \frac{b}{2\sigma_\delta}\xi_t\eta_t\right) &= 2M\left[\frac{a}{2\sigma_\varepsilon}\frac{b}{2\sigma_\delta}\eta_t^2\xi_t\delta_t\right] = \frac{ab}{2\sigma_\varepsilon\sigma_\delta}r_{\varepsilon\delta}; \\
2cov\left(\frac{a}{2\sigma_\varepsilon}\delta_t\eta_t, \xi_t\delta_t\right) &= 0; \\
2cov\left(\frac{b}{2\sigma_\delta}\xi_t\eta_t, \xi_t\delta_t\right) &= 0.
\end{aligned}$$

Тогда

$$D[\widehat{L}_5] = \frac{\frac{a^2}{4\sigma_\varepsilon^2} + \frac{b^2}{4\sigma_\delta^2} + \frac{ab}{2\sigma_\varepsilon\sigma_\delta}r_{\varepsilon\delta} + 1 + 2\widehat{r}_{\varepsilon\delta} - r_{\varepsilon\delta}^2}{N} \quad (46)$$

Выводы

Для обоих случаев доказано улучшение показателей корреляционного приема дискретного сигнала при применении линейной фильтрации. При этом выигрыш достигается даже в случае, если между шумами в каналах связи нет корреляционной связи (второй случай).

Литература

1. Hamed Kiani Galoogahi, Terence Sim, Simon Lucey. Correlation Filters With Limited Boundaries.// The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 4630-4638
2. Wei Liu. Optimal Estimation for Discrete-Time Linear Systems in the Presence of Multiplicative and Time-Correlated Additive Measurement Noises.// IEEE Transactions on Signal Processing, 2015, vol. 63, Issue. 17, pp. 4583-4593, DOI: 10.1109/TSP.2015.2447491
3. А.В. Акимов, А.А. Сирота. Синтез и анализ алгоритмов распознавания цифровых сигналов в условиях деформирующихся искажений и аддитивных помех// Известия высших учебных заведений. Радиоэлектроника. 2017, т.60, №10, с. 592-604. DOI: 10.20535/S0021347017100041
4. A.V. Akimov, A.A. Sirota. Synthesis and analysis of algorithms for digital signal recognition in conditions of deforming distortions and additive noise// Radioelectronics and Communications Systems. 2017. T. 60. № 10. С. 458-468. DOI: 10.3103/S0735272717100041
5. Ю.Ф. Стругов, А.М. Семенов, С.М. Добровольский, И.А. Батырев. Стохастическое моделирование каналов с аддитивными и мультипликативными помехами. Схема реализации.//Математические структуры и моделирование. 2015 № 2(34) С. 48-63
6. В. М. Артющенко, В. И. Воловач. Оценка погрешности измерения векторного информационного параметра сигнала на фоне аддитивных некоррелированных негауссовских помех // Журнал радиоэлектроники: электронный журнал. 2016. № 1. URL: <http://jre.cplire.ru/jre/jan16/6/text.pdf>
7. Троицкий И. И., Басараб М. А., Матвеев В. А. Использование двух каналов передачи информации для решения задачи распознавания дискретного сигнала в аддитивном шуме // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение, 2015. № 4. с. 106-112. DOI: 10.18698/0236-3933-2015-4-106-112
8. Троицкий И.И., Басараб М.А., Матвеев В.А. Определение вероятности распознавания дискретного сигнала в аддитивном шуме для двух каналов передачи информации // Электромагнитные волны и электронные системы. 2014. №11, т.19. С. 40-44.
9. Троицкий И.И., Якубов Р.Ж. Распознавание дискретного сигнала в аддитивном шуме для двух каналов передачи информации. // Вопросы кибербезопасности. 2017. № 1, с. 57-62. DOI: 10.21581/2311-3456-2017-1-57-62.
10. Троицкий И.И., Якубов Р.Ж. Сравнительный анализ линейной фильтрации дискретного сигнала в аддитивном шуме для двух каналов передачи информации с методом к ближайших соседей // Вопросы кибербезопасности. 2018. № 2, с. 59-69. DOI: 10.21681/2311-3456-2018-2-59-69.

Басараб Михаил Алексеевич (г.р. 1970), окончил в 1993 г. Харьковский авиационный институт им. Н.Е. Жуковского. Доктор физико-математических наук, профессор кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор 5 монографий и более 100 научных работ в области прикладной математики, информатики, цифровой обработки сигналов, радиофизики.

Троицкий Игорь Иванович родился в 1955 г., окончил в 1978 г. Московский инженерно-физический институт. Кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор около 40 работ в области информационной безопасности и исследования систем обработки информации и управления.

Якубов Рустам Жафарович, родился в 1992 г., окончил МГТУ им. Баумана в 2015 г. Аспирант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Имеет 8 публикаций, посвященным различным аспектам обеспечения информационной безопасности.

Using the linear filtration of the discrete signal in additive noise by means of two information transmission channels to improve its correlation reception

Basarab M. A.¹⁴, Troitskij I. I.¹⁵, Yakubov R. Zh.¹⁶

The ability to improve the correlation reception of a discrete signal in additive noise, based on the use of its linear filtering over two information transmission channels, is proposed. Noises in the studied information transmission channels are statistically related. To improve the correlation reception indicators, it is proposed to use the linear filtering mechanism, considered in the previous works of the authors. For the research, we used the model of a discrete correlator, which has two inputs and one output. Studies were conducted for two cases of information transmission channels. The first case is the presence of a discrete signal in only one information transmission channel, and the second case is the presence of a discrete signal in both channels. The results obtained make it possible to compare the correlation reception indices for various cases and to verify the feasibility of using linear filtering.

Keywords: correlation reception, linear filtering, additive noise, information transmission channels, discrete signal.

Information about the authors

Basarab M.A. (born 1970) graduated from the Kharkov Aviation Institute in 1993. Dr. Sci. (Phys.-Math.), professor of «Information Security» department of the Bauman Moscow State Technical University. Author of more than 100 publications in the fields of applied mathematics, informatics, digital signal processing, and radiophysics.

Troickiy Igor Ivanovich (born 1955), in 1978 graduated from Moscow Engineering Physics Institute. Candidate of Technical Sciences, Associated Professor at Information Security department in Bauman Moscow State Technical University. Author of more than 40 publication in information security field and researching of information processing systems.

Yakubov Rustam Zhafarovich (born 1992) in 1992 graduated from Bauman Moscow State Technical University. Graduate student of Information security department of BMSTU. He has 8 publications, the devoted various aspect of ensuring information security.

¹⁴ Basarab Mikhail Alekseevich, Dr.Sc. (Phys.-Math.), Head of the Information Security Dept., Bauman MSTU, Moscow, bmic@mail.ru

¹⁵ Troitskij, Cand. Sc. (Eng.), Associate Professor, Information Security Dept., Bauman MSTU, Moscow, iitroickiy@mail.ru

¹⁶ Yakubov Rustam Zhafarovich, Post-graduate student, Information Security Dept., Bauman MSTU, Moscow, yakubov_rustam@inbox.ru

Предложения по учету основных свойств систем аутентификации при поименованном взаимодействии субъектов (объектов) в компьютерных системах и сетях

Бегаев А.Н.¹⁷, Юркин А.А.¹⁸, Шугуров Д.Е.¹⁹, Бегаев С.Н.²⁰

Проведен анализ различных методов аутентификации с учетом локального и удаленного взаимодействия субъектов и объектов в компьютерных системах и сетях. Определены основные ситуации взаимодействия поименованных субъектов и объектов участвующих в аутентификации. Разработаны и представлены свойства системы аутентификации и произведена оценка типовых протоколов безопасности, использующих механизмы аутентификации. Сделан вывод о необходимости учета основных свойств системы аутентификации в условиях возможного несанкционированного воздействия.

Ключевые слова: поименованные субъекты и объекты, система аутентификации, протоколы безопасного взаимодействия, свойства и характеристики аутентификации.

Введение

Несмотря на интенсивное развитие информационных технологий в области аутентификации, а также средств и способов их защиты, уязвимость современных протоколов аутентификации информационно-телекоммуникационных систем и управляющих процессов, функционирующих в них, не уменьшается. Основной причиной данного факта является то, что в настоящее время на всех поименованных уровнях аутентификации информационно-телекоммуникационных систем вопросам безопасности уделяется недостаточное внимание. Как правило, эти вопросы ставятся в конце цикла разработки, а зачастую уже в процессе функционирования системы. Таким образом, безопасность удаленного и локального взаимодействий на сети приходится обеспечивать за счет внесения дополнительных подсистем и модулей аутентификации, которые должны учитывать характеристики сети, особенности протоколов аутентификации в вопросах их устойчивости к различным внешним воздействиям [1-3].

Учитывая данный факт, а также наличие уязвимостей в программном обеспечении средств аутентификации, ошибки пользователей, несовершенство протоколов аутентификации, задержки на сети, а также возможность НСД со стороны нарушителя, следует отметить, что ни один из одиночных компонентов не способен должным образом комплексно обеспечить многоуровневость аутентификации на всех поименованных объектах.

Анализ ситуаций поименованного взаимодействия субъектов (объектов)

Рассмотрим существующие средства аутентификации для разных поименованных субъектов и объектов на примере различных ситуаций взаимодействия на компьютерной сети, в результате которых субъект убеждается в легитимности другого субъекта или в легитимности предоставляемого ресурса как в одностороннем порядке, так и во взаимной аутентификации, а также методы и средства их реализации, которые представлены в таблице 1.

¹⁷ Бегаев А.Н. канд. техн. наук, доцент ИТМО, Санкт-Петербург, a.begaev@nwechelon.ru

¹⁸ Юркин А.А., канд. техн. наук, доцент Академия ФСО России, г. Орёл

¹⁹ Шугуров Д.Е., канд. техн. наук Академия ФСО России, г. Орёл

²⁰ Бегаев С.Н., эксперт АО «Эшелон-СЗ», г. Санкт-Петербург

Таблица 1.

Ситуации взаимодействия поименованных субъектов и объектов и средства их реализации

№ ситуации	Поименованные субъекты и объекты взаимодействия	Метод	Средство аутентификации
1.	Человек (субъект) – человек (субъект)	По голосу	Позывной
		По изображению	Видеотерминал
2.	Программа (объект) – программа (объект)	Совместимость с ОС. Идентификатор (правильность выполнения протокола)	Совместимость работы и подписанный электронный код (протоколы аутентификации)
3.	Человек – ЭВМ (устройство) (первым указан тот, кто распознает)	Внешние признаки (физические: местонахождение, опечатывание внешних USB входов и т.д.)	Механическая (физическая) защита доступа в помещение местонахождения ПЭВМ
4.	Человек – программа (первым указан тот, кто распознает)	Опосредованно через доверие программа-программа	Организационно, регламентировано
5.	Программа – человек (первым указан тот, кто распознает)	Биометрический код	Биометрические сканеры (протоколы аутентификации)
6.	ЭВМ (устройство) – ЭВМ (устройство)	Опосредованно через программу – программа	Протоколы аутентификации

Таким образом, анализируя ситуации взаимодействия и методы можно сделать вывод, что каждый поименованный уровень легитимности в отдельности проверяет сам себя, но при этом не учитывает в полной мере доверенность предыдущего, а это значит, что решение задачи многоуровневой аутентификации приходится усложнением передачи доверия от самого нижнего – 6 к самому верхнему – 1, а ввиду того, что аутентификация является первичной и ключевой в процессе обмена данными, то и она определяет защищенность всего процесса взаимодействия, иными словами насколько достоверна аутентификация, настолько достоверны взаимодействие субъектов и процессов и их защищенность, но не ниже ее.

Учитывая различные ситуации взаимодействия на компьютерных сетях, методы аутентификации могут быть использованы на различных ее элементах. При этом, важное значение использования существующих методов аутентификации имеет их характеристика по удаленности объектов взаимодействия по отношению друг другу. Для выделения особенностей использования локальной и удаленной систем аутентификации проведена их сравнительная характеристика в таблице 2. [4, 5].

Сравнительная характеристика систем аутентификации

Методы аутентификации	Локальная	Удаленная
Характеристика	Для аутентификации может использоваться меньшее количество аутентифицирующих признаков. Используемые при локальной аутентификации признаки обладают большей полнотой, чем в случае удаленной аутентификации (могут передаваться уникальные (внутренние) признаки, присущие только определенному пользователю, такие как биометрические данные). Передача аутентификационных признаков более защищена ввиду допуска к работе квалифицированного персонала и защищенности объекта, на котором обрабатывается информация. Съём данных может осуществляться только вне охраняемой зоны на общедоступных каналах связи. Более высокая степень скрытности передачи данных. Требования к непрерывности у локальной аутентификации ниже, чем у удаленных ввиду их защищенности (аутентификация может осуществляться только один раз и повторяться только при необходимости)	Удаленная аутентификация подвержена большим количествам ошибок в случае внешних воздействий. Нарушитель может осуществлять съём информации на различных участках сети. Полнота передаваемых признаков меньше, чем в случае локальной аутентификации (для полного подтверждения легитимности объекта желательна передача как можно большего количества признаков). Ввиду открытости процесса передачи данных по совокупности признаков легко определяется факт прохождения процесса аутентификации. Малая степень скрытности процесса передачи данных. Для постоянного подтверждения легитимности пользователя необходимо непрерывно проверять его аутентификационные данные (непрерывность проверки будет подтверждать, что на пользователя или канал связи не была осуществлена атака)

На основе вышеприведенных характеристик, можно сделать вывод о сложности реализации аутентификации, соответственно, ее выполнение является сложной и ключевой задачей во взаимодействии субъектов и объектов в компьютерных системах и сетях.

Рассмотрим современные методы защиты на всех уровнях легитимности и выполним оценку защиты от существующих угроз.

В таблице 3 приведены основные подсистемы защиты и средства для обеспечения комплексной безопасности, более детально приведены средства, реализующие аутентификацию при удаленном взаимодействии. Штатные средства ОС Windows, Linux могут быть со слабыми паролями или вообще их не использовать, при этом возможен обход аутентификации средствами реализации активных атак [3].

Таблица 3.

Подсистема аутентификации объектов компьютерной сети

Наименование подсистемы	Используемые средства защиты
Подсистема аутентификации	Штатные механизмы аутентификации операционной системы семейства Windows, Linux (на ПЭВМ и серверах); Протоколы аутентификации: (NTLM, RADIUS, KERBEROS, PAP, CHAP, IPSEC, SSL/TLS); механизмы биометрической аутентификации (сканеры, видеофиксаторы); электронные генераторы паролей; электронные сертификаты; электронные замки; RU-токены

Протоколы аутентификации NTLM, RADIUS, KERBEROS, PAP, CHAP, IPSEC, SSL/TLS²¹ подвержены перехвату – sniffерами (анализаторами) и модификации – манипуляторами пакетов [5].

Анализ таблицы 3 позволяет сделать вывод, что механизмы биометрической аутентификации [6], показывают в достаточной степени хорошие результаты. Однако стоит отметить, что они дороги и не получили широкое распространение при удаленной аутентификации. [7-9]

Электронные генераторы паролей удобны и используются [10], но при этом также подвержены кражам через уязвимости ОС посредством сканеров, средств SQL-инъекций и атакам с помощью переборщиков паролей.

Электронные сертификаты достаточно часто используются в качестве основного аутентифицируемого элемента в клиент-серверных технологиях при удаленном администрировании телекоммуникационного оборудования (ТКО). Также степень доверия к сертификатам будет снижена в условиях реального времени без доступа к удостоверяющему центру [11].

Электронные замки достаточно распространены при доступе к ТКО, при этом возникает вопрос об их доверенном производителе, а также о возможности дублировать данные с них и использовать клоны для нелегитимной аутентификации; отсутствует однозначность владельца ключа, может передаваться от одного лица к другому и, как, правило не используются для удаленного доступа.

Токены применяются локально, как правило, при осуществлении доступа к ОС, обновлении ПО, это наиболее защищенный элемент, но при этом не распознает личность применяющего его, только PIN-код, возможны физическая кража и подсматривание вводимого PIN-кода [12].

Таким образом, большинство средств защиты декларируются, но при этом не могут в полной мере выполнять функции по аутентификации. Они подвержены различным типам угроз, особенно в случае угрозы подмены в ходе сеанса связи/администрирования. В свою очередь, угроза перехвата сеанса и ведение диалога от имени легитимного пользователя не предусматривают использование биометрических методов проверки подлинности, что может являться поводом для проведения исследования в области периодической биометрической аутентификации [13].

Оценка протоколов безопасности по используемым в них механизмам аутентификации

Также следует оценить механизмы аутентификации, реализованные протоколами в компьютерных сетях для осуществления взаимодействий на уровне машина–машина

²¹ RFC 4120, 1994, 2401, 4303, 6101, 5246.

(таблица 4). Приведен перечень способов и протоколов, обладающих механизмами аутентификации с учетом международных стандартов Request for Comments (RFC).

Формат протоколов аутентификации проанализирован как в теоретическом, так и в практическом аспектах и выявлены следующие свойства, которыми должны характеризоваться системы аутентификации с позиции защиты от НСД:

Свойства и характеристики способов и протоколов аутентификации:

- 1) защита информации о связи аутентификационных данных с личностью;
- 2) защищенность аутентификации от DDOS-атак;
- 3) защищенность от повтора;
- 4) уровень предварительной информированности об объекте аутентификации;
- 5) целостность аутентификационных данных;
- 6) неизменность участников в процессе сеанса;
- 7) неотказуемость в проведении аутентификации;
- 8) устойчивость к атакам по словарю;
- 9) однозначность реакции на запросы аутентификации;
- 10) однозначность получателя аутентификационных данных;
- 11) конфиденциальность аутентификационных данных;
- 12) непрерывность процесса аутентификации (за сеанс);
- 13) многоуровневость проверки;
- 14) частота переаутентификации (за сеанс);
- 15) достоверность аутентификации;
- 16) своевременность;
- 17) скрытность процесса аутентификации;
- 18) многофакторность;
- 19) количество этапов аутентификации;
- 20) объем (полнота) признака.

Таблица 4.

Механизмы и протоколы аутентификации																				
Протокол	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
PAP	-	-	-	+	+	-	-	-	-	-	-	-	1	-	-	-	-	1	3	L-пар
CHAP	-	-	+	+	+	-	-	-	-	-	-	-	1	-	-	-	-	1	5	128 бит
S/KEY	-	-	+	+	+	-	-	-	-	-	-	-	1	-	-	-	-	1	4	128 бит
HOTP	-	-	-	+	+	-	-	-	-	-	-	-	1	-	-	-	-	1	5	400 бит
RADIUS	-	-	+	+	+	+	-	+	-	-	+	+	1	-	-	-	-	1	5	176 бит
TACACS+	-	-	+	+	+	+	-	+	-	-	+	+	1	-	-	-	-	1	6	128 бит
DIAMETR	-	-	+	+	+	+	-	+	-	-	+	+	1	-	-	-	-	1	4	128 бит
EAP	-	-	+	+	+	+	-	+	-	-	+	-	1	-	-	-	-	1	5	128 бит
SSL/TLS	-	-	+	+	+	+	+	+	-	-	+	-	2	-	-	-	-	1	6	1450 байт
IPSec	-	-	+	+	+	+	+	+	-	+	+	-	2	-	-	-	-	1	6	1450 байт
Kerberos	-	+	+	+	+	+	+	+	-	+	+	-	2	-	-	-	-	1	8	128 бит

Выводы

В результате проведенного исследования были выявлены следующие особенности механизмов и протоколов аутентификации в компьютерных системах и сетях, которые

необходимо учитывать при проектировании реализации системы аутентификации в условиях НСД:

- число признаков для аутентификации не определено;
- количество аутентификационной информации может быть избыточно при низкой пропускной способности;
- не учитывается, насколько может быть занят канал аутентификационной информацией;
- не регламентируется период смены эталона аутентификационных данных, должна быть осуществлена регламентация соответствующими документами;
- время, затрачиваемое на аутентификацию, не нормировано (формирование, проверка), и нет возможности его корректировки;
- не все протоколы осуществляют периодичность проверки аутентичности при удаленном взаимодействии, используется однократная проверка;
- количество этапов (шагов) аутентификации различно, и никак не документировано;
- учет уровней легитимности, подлежащих проверке при удаленном взаимодействии объектов, для обмена данными не определен;
- статистика достоверности аутентификации протоколов отсутствует.

Литература

1. Сабанов, А. Г. О применимости методов управления рисками к процессам аутентификации при удаленном электронном взаимодействии // *Электросвязь*. 2014. № 6. С. 39–42.
2. Сабанов, А. Г. Некоторые проблемы идентификации при удаленном электронном взаимодействии // *Первая миля (Last Mile)*. – февраль 2014. – № 41. – С. 94–97.
3. Аутентификация при удаленном взаимодействии пользователей в компьютерных сетях / Д. Е. Шугуров, П. Ю. Стародубцев // *Информационная безопасность и защита персональных данных. Проблемы и пути их решения : материалы VII Межрегиональной науч.-практ. конференции / под ред. О. М. Голембиовской*. – Брянск : БГТУ, 2015. – С. 174–178
4. Методы и протоколы аутентификации : Учеб. пособие / Д. Е. Шугуров, А. И. Козачок [и др.]. – Орёл : Академия ФСО России, 2013. – 219 с.
5. Системы анализа защищенности : практическое пособие / Д. Е. Шугуров, А. А. Юркин [и др.] ; под общ. ред. А. А. Юркина. – Орёл : Академия ФСО России, 2017. – 140 с.
6. Бардаев, С. Э. Многофакторная биометрическая пороговая криптосистема / С.Э. Бардаев, – *Известия ЮФУ. Технические науки*, 2015.
7. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
8. Ложников П.С., Сулавко А.Е., Бурая Е.В., Писаренко В.Ю. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица // *Вопросы кибербезопасности*. 2017. № 3 (21). С. 24-34.
9. Крутохвостов Д.С., Хиценко В.Е. Парольная и непрерывная аутентификация по клавиатурному почерку средствами математической статистики // *Вопросы кибербезопасности*. 2017. № 5 (24). С. 91-99.
10. Карачанская Е.В., Костров М.А. Многофункциональный генератор паролей // *Вопросы защиты информации*. 2019. № 3 (126). С. 43-48.
11. Баранов Н. Удостоверяющие центры в России и мире // *Защита информации. Инсайд*. 2012. № 5 (47). С. 76-77.
12. Щербakov А.Ю., Булыгин А.Н., Рябков В.Е., Елизарова А.С. Исследование вопросов применения технологии цифровизации на примере цифрового рейтинга студента // *Вопросы кибербезопасности*. 2019. № 3 (31). С. 33-38.
13. Методика удаленной аутентификации личности [Электронный ресурс] / Д. Е. Шугуров, Ю. И. Стародубцев // *Интернет-журнал «Технологии техносферной безопасности»*. – 2015. – Вып. 5 (63). – С. 265–273. – Режим доступа к ресурсу: <http://ipb.mos.ru/ttb>.

Влияние экранирования на энергию сигнала, излучаемого интерфейсом LVDS**Белова Е.А.²², Кузнецов А.М.²³, Нестерова М.А.²⁴, Погорелко Е.А.²⁵**

Аннотация. В ходе исследования была выполнена серия измерений напряженности побочных электромагнитных излучений от персонального компьютера в форм-факторе моноблока с интерфейсом LVDS без экранирования и с использованием двухмиллиметровой металлической экранирующей пластины, герметично закрывающей заднюю поверхность устройства. Произведен расчет энергии этого излучения, который показал, что наличие металлической пластины оказывает существенное экранирующее действие, уменьшая энергию излучения в сорок два раза. Данное исследование произведено с целью апробации пассивных методов защиты средств вычислительной техники от утечки за счет побочных электромагнитных излучений.

Ключевые слова: побочные электромагнитные излучения, анализ спектра, пассивные меры защиты.

Введение

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал [1].

Канал утечки через побочные электромагнитные излучения (ПЭМИ) в настоящее время закрепляется в качестве одного из самых значимых каналов утечки информации [2-4], т.к. в связи с постоянным развитием аппаратуры для регистрации данных излучений всё более и более слабые излучения могут быть зафиксированы и декодированы.

Для предотвращения утечки информации за счет ПЭМИ используют следующие методы защиты [1]:

- электромагнитное экранирование помещений;
- доработка средств электронной техники с целью уменьшения уровня ПЭМИ;
- криптографическое закрытие информации;
- активная радиотехническая маскировка;

Доработка средств электронной техники с целью уменьшения уровня ПЭМИ должна включать комплекс работ, позволяющий снизить уровень излучения. Однако при разработке интерфейсов передачи данных, уменьшение данных излучений не является первостепенной задачей. Таким образом, возникает потребность в разработке пассивных методов уменьшения излучения отдельных интерфейсов, которые позволят использовать современную технику в защищенном варианте. Далее рассмотрим практическое применение такого пассивного метода уменьшения излучения [5], как экранирование [6], для интерфейса LVDS, используя опыт аналогичных исследований экранирования как концепции [7] и экранирования USB-flash-накопителей [8].

LVDS (Low Voltage Differential Signaling) - метод передачи цифровых данных дифференциальными сигналами с малыми перепадами уровня напряжения (до 350 мВ) на двух физических линиях печатной платы или сбалансированного кабеля со скоростью до сотен и даже нескольких тысяч мегабит в секунду. Малые перепады уровня и токовый режим выхода передатчика обеспечивают малый уровень шума и очень малую потребляемую мощность во всём диапазоне скоростей передачи [9].

²² Белова Екатерина Александровна, МГТУ им. Н.Э. Баумана, Москва, balehok.kat@yandex.ru

²³ Кузнецов Александр Максимович, МГТУ им. Н.Э. Баумана, Москва, almkuznetsov@mail.ru

²⁴ Нестерова Марина Александровна, МГТУ им. Н.Э. Баумана, Москва, marishkan13@inbox.ru

²⁵ Погорелко Егор Алексеевич, МГТУ им. Н.Э. Баумана, Москва, pogorelko.egor@yandex.ru

Практическая часть

При практических измерениях использовалось оборудование, указанное в табл.1.

Таблица 1.

Измерительное оборудование		
№ п/п	Тип	Модель
1	Анализатор спектра	Rohde & Schwarz FSV13
2	Измерительная антенна	АИ5-0

Схема размещения оборудования при проведении измерений представлена на рис. 1.



Рис. 1. Схема размещения оборудования при проведении измерений

С целью обеспечения наиболее корректных и точных измерений напряженности излучения необходимо сгенерировать в канале передаче видеоинформации сигнал с одной гармоникой в интервале, т.е. со скважностью равной двум (тест-сигнал) [10]. Для его формирования используется специальное тестовое программное обеспечение. Во время проведения измерений тест-сигнал был сформирован с помощью следующих настроек:

- разрешение: 1920x1080 пикселей
- частота обновления: 60 Гц
- вид заполнения: пиксель через пиксель, RGB – R:55H, G:55H, B:55H
- ориентировочная частота тона «подкраски»: 128 Гц
- количество полос – 4

Была проведена серия измерений напряженности излучения интерфейса LVDS. В первой серии проводились измерения персонального компьютера в форм-факторе моноблока, задняя поверхность которого была герметично закрыта металлической пластиной толщиной два миллиметра. Измерительная антенна АИ5-0 находилась на расстоянии одного метра от объекта измерений [11]. Результаты измерений представлены в табл.2.

Таблица 2.

Результаты измерений моноблока с крышкой

№ п/п	F, [МГц]	E _{с+ш} , [дБ]	E _ш , [дБ]
1	243.6990	41.94	39.69
2	725.8865	43.85	38.82
3	970.1390	37.22	33.39
4	1214.9990	31.18	29.63

где: F – частота, $E_{с+ш}$ – энергия, полученная при измерении тест-сигнала, $E_{ш}$ – энергия, полученная при измерении шума.

Во второй серии проводились измерения в зависимых условиях, при этом металлическая пластина была демонтирована, таким образом обеспечивалось отсутствие экранирующего материала между непосредственно выходом интерфейса LVDS и измерительной антенной. Результаты измерений представлены в табл.3 и на рис.2.

Таблица 3.

Результаты измерений моноблока без крышки

№ п/п	F, [МГц]	E _{с+ш} , [дБ]	E _ш , [дБ]
1	243.6990	64.82	56.13
2	725.8865	57.44	45.95
3	970.1390	52.39	48.15
4	1214.9990	62.38	51.67

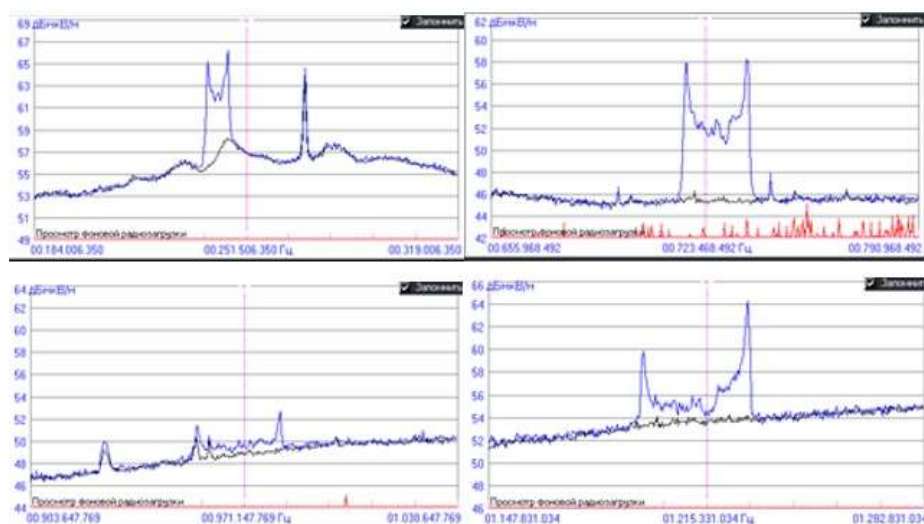


Рис. 2. Спектрограммы измеренных ПЭМИ

С помощью формулы для расчёта энергии сигнала (1) вычислен уровень сигнала ПЭМИ от моноблока с установленной металлической пластиной и без нее [12]. Результаты приведены в табл.4.

$$E_c = \sqrt{E_{c+ш}^2 - E_{ш}^2} \quad (1)$$

Где: E_c – энергия сигнала.

Таблица 4.

Результаты расчёта энергии сигнала

№ п/п	С пластиной			Без пластины		
	F, [МГц]	E_c , [дБ]	E_c , [мкВт]	F, [МГц]	E_c , [дБ]	E_c , [мкВт]
1	243.6990	13.55	22.64644	243.6990	32.42	1745.822
2	725.8865	20.39	109.3956	725.8865	34.47	2798.981
3	970.1390	16.44	44.05549	970.1390	20.65	116.1449
4	1214.9990	9.71	8.260379	1214.9990	34.95	3126.079

Выводы

Среднее значение энергии сигнала для измерений с установленной металлической пластиной составляет 16.64 дБ, а без установленной металлической пластины – 32.89 дБ, что эквивалентно увеличению уровня сигнала в 42 раза. Таким образом, очевидно, что металлическая пластина моноблока выполняет существенное экранирующее действие, многократно снижая уровень сигнала.

Достоверность данного заключения подтверждается приведенными спектрограммами измеренных излучений (рис.2), а также численными значениями (табл.2,3,4), полученными с помощью высокоточных измерительных приборов (табл.1).

Литература

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. 436 с.
2. Ярочкин В.А. Технические каналы утечки информации. - М.: Ось-89, 1994.
3. Петраков А.В. Основы практической защиты информации. - М.: Радио и связь, 2000.
4. Меньшаков Ю.К. Теоретические основы технических разведок. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. - 536 с.: ил.
5. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия-Телеком, 2005. - 416 с.: ил
6. Физический энциклопедический словарь. - М.: Сов. энциклопедия, 1983.
7. М.Р. Курачинова. Средства и способы защиты информации от перехвата за счет побочных электромагнитных излучений и наводок, аттестация объектов, помещений и информационных систем. // Студенческая наука для развития информационного общества. - Ставрополь: Северо-Кавказский федеральный университет, 2017. - с. 200-202
8. Д.А. Паршин Д.А., Ярьско А.П., Остапенко Н.А. Защита USB-flash-носителей от утечек информации по каналу побочных электромагнитных излучений. - Екатеринбург: Изд-во Урал. Ун-та, 2018. - с. 113-116
9. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки. М.: Горячая линия Телеком, 2016. с. 161-165.
10. Харкевич А.А. Спектры и анализ. Изд 5-е. М.: Книжный дом «ЛИБРИКОМ», 2009. 240 с.
11. Хорев А.А. Способы и средства защиты информации. - М.: МО РФ, 1998. - 316 с.
12. Кондратьев А.В. Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки. М.: МАСКОМ, 2011. 256 с.

Научный руководитель — Вайц Екатерина Викторовна, кандидат технических наук, доцент кафедры «Защита информации» МГТУ им. Н.Э. Баумана, vaitcev@yandex.ru.

The effect of shielding on the energy of the signal emitted by the LVDS interface

Belova E.A.²⁶, Kuznetsov A.M.²⁷, Nesterova M.A.²⁸, Pogorelko E.A.²⁹

Abstract: During the research, a series of tension measurements of compromising emanation by PC, that uses LVDS interface are made. Measuring included series with and without two-millimeter metal shielding plate hermetically closing the rear surface of the device. Calculation of received emanation energy are made. As a result, shielding plate reduced emanation energy by 42 times.

Keywords: compromising emanation, spectrum analysis, passive information protection.

²⁶ Belova Ekaterina Aleksandrovna, Bauman Moscow State Technical University, Moscow, balehok.kat@yandex.ru

²⁷ Kuznetsov Aleksandr Maksimovich, Bauman Moscow State Technical University, Moscow, almkuznetsov@mail.ru

²⁸ Nesterova Marina Aleksandrovna, Bauman Moscow State Technical University, Moscow, marishkan13@inbox.ru

²⁹ Pogorelko Egor Alekseevich, Bauman Moscow State Technical University, Moscow, pogorelko.egor@yandex.ru

Возможный подход к оценке средств защиты информации

Бондарев В.В.³⁰

Рассматриваются вопросы сравнительной оценки средств защиты информации с использованием подхода, основанного на понятии меры - единства качественной и количественной определенности объекта.

Ключевые слова: защита информации, средство защиты информации, мера, оценка, эталон, показатель, критерий, качество, количество, свойство, количество свойства.

Введение

При проектировании и построении комплексной системы защиты информации одной из самых сложных проблем является выбор конкретного средства защиты информации из возможных, представленных на рынке [3-7].

Оценка систем сводится к измерению – оценке соответствия меры системы некоторым эталонам, критериям. В отдельных случаях может производиться сравнительная оценка объектов, в данном случае – средств защиты информации.

Обычно свойство выражают или количественно, или качественно: каждое свойство описывают количественно с помощью некоторой переменной – показателя свойства, значение которого характеризует уровень качества относительно этого свойства.

Уровень качества объекта характеризуется совокупностью показателей свойств, необходимых для соответствия объекта его назначению.

Эта совокупность называется **показателем качества** объекта.

Требуемые качества задаются условиями, которым должны удовлетворять возможные значения показателя качества.

Эти условия называются **критериями оценивания**, а проверка их выполнения – **оцениванием** качества объекта.

А сейчас все введенные понятия попытаемся облечь в виде математического аппарата, может быть, к сожалению, и не совсем совершенного.

Описание средства защиты информации в виде меры

Представим меру в виде

$$M = \begin{vmatrix} C_1, C_2, C_3 \dots, & C_n \\ v_{C_1} v_{C_2} v_{C_3} & v_{C_n} \end{vmatrix}, \quad (1)$$

³⁰ Бондарев Валерий Васильевич, кандидат военных наук, доцент, bondarevvv@mail.ru
Московский государственный технический университет имени Н. Э. Баумана, Москва, Российская Федерация, Учебный центр «Информзащита», Москва, Российская Федерация.

где C_i – свойства объекта; v_{c_i} – величина (количество) свойства.

Например, описывая межсетевой экран, можно предложить следующие группы свойств и количеств этих свойств:

физические параметры (WAN, LAN, DMZ, консоль, размер....);

производительность (производительность межсетевого экрана, кол-во пользователей, параллельные сессии, 3DES, политики, работа по расписанию....);

работа в режиме межсетевого экрана (NAT, PAT, прозрачный режим, режим маршрутизации, статическая, динамическая, Virtual IP, NAT на основе политик, фильтрация пакетов в туннелях VPN.....) и т.д.

Требуемая мера (стандарт, критерий)

$$M_K = \begin{bmatrix} C_1, C_2, \dots, C_n \\ v_{c_1}^K, v_{c_2}^K, \dots, v_{c_n}^K \end{bmatrix}. \quad (2)$$

Мера предмета деятельности

$$M_\Pi = \begin{bmatrix} C_1, C_2, \dots, C_n \\ v_{c_1}^\Pi, v_{c_2}^\Pi, \dots, v_{c_n}^\Pi \end{bmatrix}. \quad (3)$$

Близость мер определяется одним из возможных показателей:

$$K_N = \frac{N_{M_K \cap M_\Pi}}{N_{M_K \cup M_\Pi}}; \quad (4)$$

$$K_N = \frac{\sum_{N_{M \cap}} \left[\frac{v_{c_i} \min}{v_{c_i} \max} \right]}{N_{M \max}}, \quad (5)$$

где N_{M_K} , N_{M_Π} – мощности M_K , M_Π ; $N_{M \cap}$ – мощность пересечения множеств C^Π , C^K ; $N_{M \max}$ – мощность объединения множеств C^Π , C^K .

Качество объекта характеризуется декартовым произведением свойств, а величина этого качества – произведением величин этих свойств.

$$M_K = \begin{bmatrix} C_1, C_2, \dots, C_n \\ \prod_i v_{c_i} \end{bmatrix} \quad (6)$$

Методика оценки близости мер

1. Объединяем мощности множеств C в M_0 , $M_\exists$: N_{C^0} , $N_{C^\exists}$.
2. Представляем $M_0 \cap M_\exists$ в виде

$$M = \begin{bmatrix} C_m, & C_{m+1}, \dots, & C_n \\ v_{C_m^0} & v_{C_{m+1}^0} & v_{C_n^0} \\ v_{C_m^3} & v_{C_{m+1}^3} & v_{C_n^3} \end{bmatrix} \quad (7)$$

3. В каждой паре определяем min- и max- величины.
4. Подставляем значения $v_{C_i} min, v_{C_i} max, max(N_{C^3}, N_{C^0})$ в K_N .

Пример.

M

C
 M
 3

C
 K

C

Необходимо упомянуть о слабых местах данного подхода. Во-первых, мы исходим из того, что свойства оцениваемого объекта независимы, что на практике встречается крайне редко. Во-вторых, открытым остаётся вопрос, сколько нужно учитывать этих свойств для получения максимально объективной оценки. И, наконец, по умолчанию считается, что рассматриваемые и учитываемые свойства обладают одинаковым весом для оценки, что также встречается нечасто. Однако эти недостатки не носят принципиального характера и могут быть устранены в процессе дальнейших исследований [1, 2].

$N_{M_0} = 3$.

Литература

1. Бондарев В.В. Функционально-системный подход к управлению информационной безопасностью // Информационно-методический журнал INSIDE. Защита информации. № 2'2018. С. 2-6.
2. Бондарев В.В. Функционально-системный подход в подготовке специалиста в области информационной безопасности. В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 63-67.
3. Иванов В.П., Иванов А.В. К вопросу о выборе технических средств защиты информации от НСД // Защита информации. Инсайд. 2006. № 2 (8). С. 62-67.
4. Кондаков С.Е. Анализ и синтез комплекса средств защиты информации // Вопросы кибербезопасности. 2013. № 2 (2). С. 20-24.
5. Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции // Вопросы кибербезопасности. 2016. № 1 (14). С. 17-23.
6. Петренко С.А., Цирлов В.Л. Импортзамещение решений IDS и SIEM. В сборнике: The 2018 Symposium on Cybersecurity of the Digital Economy (CDE'18) Вторая международная научно-техническая конференция. Санкт-Петербург, 2018. С. 382-387.

$N_{M_3} = 3$.

7. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1(1). С. 17-27.

A Possible Approach to the Assessment of Information Security **Bondarev V.V.³¹**

Discusses the issues of comparative evaluation of information security tools using the campaign based on the concept of action - unity of qualitative and of quantitative determinacy of the object.

Keywords: *information security, information security measure, measure, evaluate, benchmark, measure, criterion, quality, quantity, property, number of properties.*

³¹ Bondarev V.V., Ph.D. (Mil), Associated Professor, BMSTU, Moscow; Training center "Informzaschita", Moscow, Russian Federation, bondarevvv@mail.ru, 964-707-72-28

Учебно – материальная база подготовки специалиста в области информационной безопасности

Бондарев В.В.³²

Рассматриваются вопросы создания и развития учебно-материальной базы подготовки специалиста в области информационной безопасности на основе использования функционального - системного подхода.

Ключевые слова: информационная безопасность, специалист, знания, навыки умения, защита информации, мастерство, подготовка учебно-материальная база, стенд, тренажёр, метод.

Введение

В настоящее время слабо проработаны вопросы создания и развития учебно-материальной базы (УМБ) в области информационной безопасности (ИБ) [5-7].

К вариантам технических средств подготовки специалиста в области ИБ относятся:

- **статический стенд** для формирования знаний о структуре ситуации, связанной с ИБ, и её компонентах;
- **динамический стенд** для формирования знаний о функционировании компонентов ситуации ИБ;
- **тренажёр** - техническое средство подготовки, обеспечивающее постоянный контроль качества деятельности обучаемого и предназначенное для формирования и совершенствования у него навыков и умений, необходимых для эксплуатации, обслуживания и управления ИБ;
- **специализированный тренажёр** для формирования ограниченного круга навыков и умений в области защиты информации [8];

комплексный тренажёр для формирования навыков и умений в полном объёме функциональных обязанностей специалиста, группы специалистов отдела ИБ.

Важным, но практически слабо исследованным вопросом является характер (индивидуальный или коллективный) работы обучаемого с автоматизированной обучающей системой (АОС).

Действительно, работа сотрудников подразделений защиты по форме носит сугубо индивидуальный характер. Но с содержательной стороны эта работа является коллективным трудом, так как труд одного сотрудника основан на результатах деятельности других сотрудников. Другими словами, работа сотрудников служб ИБ есть работа коллективная, основанная на доверии друг другу всех ее участников. Видимо и в процессе обучения необходимо формировать подобное отношение к будущей деятельности

³² Бондарев В.В., к.в.н., доцент, Московский государственный технический университет имени Н. Э. Баумана, Москва, Российская Федерация, bondarevvv@mail.ru

у обучаемых. Однако существующие АОС не рассчитаны на реализацию этого. Нужны новые подходы к созданию АОС, учитывающие эту специфику работы. Одним из подходов может служить реализация идеи сетевой АОС, причём, алгоритм функционирования этой АОС должен базироваться на принципах функционально-системного подхода.

Основной функцией компьютерных сетей в обучении является создание условий для повышения эффективности обучения, то есть их реализация как средства обучения. Однако следует иметь в виду, что можно говорить, по крайней мере, о двух основных направлениях применения сетей в обучении. Глобальные (территориальные) сети могут применяться для реализации т.н. дистанционного обучения, когда обучаемый и АОС связаны между собой по каналу связи.

По назначению следует различать:

специализированную САОС;

сетевую автоматизированную обучающую оболочку.

В зависимости от вида учебной задачи, которая решается на специализированной САОС, следует различать системы, предназначенные для решения специально разработанных учебных задач и системы, представляющие собой учебный аналог (имитатор) реальной задачи.

Сетевая автоматизированная обучающая оболочка (САОО) – это локальная сеть ПК, предназначенная для обеспечения взаимодействия обучаемого и преподавателя в процессе групповых учебных занятий. Принципиальным отличием САОО от САОС является то, что в ней в АРМ слушателей выступает не АОС, а реальные рабочие программы. Обучающую же функцию реализует преподаватель с помощью программной надстройки, которая резидентно находится в оперативной памяти каждого АРМ и обеспечивает осуществление контроля и диалога с обучаемым

Исходя из этого, **целью создания УМБ подготовки специалистов по ИБ** является формирование модели профессиональной среды, в рамках которой выпускник будет выполнять должностные обязанности в течение ближайших 2-3 лет после окончания вуза. **Развитие УМБ** предполагает систему постоянно действующих организационно-технических мероприятий, обеспечивающих адекватность элементов УМБ различного уровня (вузовского, факультетского, кафедрального) объектам будущей деятельности выпускников с учетом изменений, происходящих в области технических средств разведки и методов и способов противодействия им. Кроме того **УМБ должна также обеспечивать** проведение научных исследований и подготовку научно - педагогических и научных кадров.

Современные условия подготовки специалистов в области защиты информации характеризуются недостаточным финансированием системы образования, расширением объёма решаемых задач, повышением требований к качеству результатов. Особенно это актуально для подготовки специалистов в области ИБ.

В этих условиях неприменимы традиционные пути подготовки специалистов с заблаговременной разработкой УМБ и средств подготовки (например, тренажёры), поскольку эти средства сложные, дорогие в изготовлении и эксплуатации, морально устаревающие за очень короткое время, не способные прививать требуемый объём знаний, навыков и умений в динамичных реальных условиях деятельности.

Учитывая значимость УМБ в решении задач подготовки специалистов в области ИБ и необходимость вложения значительных материальных средств в ее развитие и поддержание, необходим системный подход в определении замысла и формировании решения на ее развитие.

При этом УМБ должна рассматриваться не как самостоятельная система, а как материальная основа учебно-методической среды, в рамках которой осуществляется формирование профессионального облика выпускника вуза, удовлетворяющего квалификационным требованиям.

Особенностью функциональной системы в приложении к системам «человек - техника», к которым с полным основанием можно отнести УМБ системы подготовки специалиста в области ИБ, является доминирующая роль человека как целеполагающего фактора (формирование цели деятельности системы) и как системообразующего фактора (в соответствии с целью подбор наиболее целенаправленных компонентов из имеющихся в наличии и соединение их в систему).

Таким образом, УМБ подготовки специалиста в области ИБ можно определить **как комплекс взаимодействующих материальных и технических средств, составляющих основу профессиональной среды будущей служебной деятельности выпускников ВУЗа, и предназначенных для обеспечения подготовки слушателей по специальности (специализации) ИБ в соответствии с государственным образовательным стандартом, квалификационными требованиями, учебными планами и программами, а также для выполнения научных исследований и подготовки научных и научно – педагогических кадров.**

В основу формирования УМБ вуза предлагается положить принцип функционально - системного подхода. Суть его состоит в следующем:

- Исходя из специализаций, по которым в вузе осуществляется подготовка специалистов по ИБ и, исходя из количества выпускаемых ежегодно специалистов, формируется учебный полигон вуза (кафедры), на элементах которого осуществляется заключительный этап подготовки выпускников по должностному предназначению;
- Для эффективного использования УМБ разрабатывается система обобщённых, комплексных и частных задач, отражающих квалификационные требования к выпускникам и обеспечивающих корреляцию общепрофессиональных дисциплин.

Основу УМБ, её сердцевину должны составлять объекты, на которых выпускники выполняют свои функциональные задачи [1-4].

Литература

1. Бондарев В.В. Проблемы подготовки специалистов в области информационной безопасности// доклад на 9-й международной научно-технической конференции «Приборостроение – 2016», 23–24 ноября 2016 г. Минск/
2. Бондарев В.В. Психологические аспекты информационной безопасности. В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 28-32.
3. Бондарев В.В. Создание и развитие учебно-материальной базы подготовки специалиста в области информационной безопасности. В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 68-73.
4. Бондарев В.В. Функционально-системный подход к управлению информационной безопасностью//Информационно-методический журнал INSIDE. Защита информации. № 2'2018. С. 2-6.
5. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 2-14.
6. Салтанов К.С., Петренко С.А. Современные подходы к обучению специалистов в области ИБ // Защита информации. Инсайд. 2018. № 5 (83). С. 80-85.
7. Шеремет И. А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере. 2016. № 5 (18). С. 3-7.
8. Басараб М.А., Бельфер Р.А., Кравцов А.В. Учебный имитатор объединенной отечественной сети ПД специального назначения (структура, функции). В сборнике: Безопасные информационные технологии. Сборник трудов Десятой всероссийской научно-технической конференции. НУК «Информатика и системы управления». 2019.

Educational - material basis of training specialist in the field of information security **Bondarev V.V.³³**

The issues of creation and development of the educational and material base for training a specialist in the field of information security are considered on the basis of the use of the system-functional approach.

Keywords: *information security, specialist, knowledge, skills of skills, information protection, skill, training material and educational base, stand, simulator, method.*

³³ Bondarev V.V., Ph.D., Associated Professor, BMSTU, Moscow.

Игровая постановка задачи выбора дополнительного фактора аутентификации для рабочих мест на примере клавиатурного почерка Быков А.Ю.³⁴, Акулова Н.О.³⁵

Представлена игровая постановка задачи двух игроков: защитника и нападающего. Защитник выбирает рабочие места, на которых целесообразно, кроме основного фактора аутентификации, использовать дополнительный фактор в виде клавиатурного почерка с учетом ограничений на ресурсы. Нападающий выбирает рабочие места, на которые он будет проводить атаку с целью получения доступа за счет преодоления используемых механизмов аутентификации. Постановка задачи является игрой с нулевой суммой, показателем качества является оценка ущерба защитника с учетом важности информации, обрабатываемой на рабочих местах. В поставленной задаче каждый из игроков должен решить свою задачу булевого программирования при фиксированном решении другого игрока. Игра может быть сведена к матричной игре большой размерности. Представлены ссылки на источники литературы, в которых описаны алгоритмы решения подобных задач на основе критерия гарантированного результата и на основе поиска седловой точки игры в смешанных стратегиях.

Ключевые слова: информационная безопасность, аутентификация и идентификация, клавиатурный почерк, теория игр, матричная игра, дискретная оптимизация

Введение

В различных задачах защиты информации часто используются модели теории игр. Учитывая, что при защите информации присутствуют две стороны: сторона защиты и сторона нападения, в подобных задачах рассматривают два игрока – игрок нападения и игрок защиты. В [1-10] приведены примеры задач двух игроков, применяемые для решения различных вопросов, связанных с защитой информации. Рассмотрим постановку задачи двух игроков, возникающую при выборе дополнительного фактора аутентификации для нескольких рабочих мест.

Содержательную постановку задачи сформулируем следующим образом. В защищаемой системе существует заданное число рабочих мест (РМ), для доступа на эти РМ пользователей используются средства идентификации и аутентификации. Предполагается, что существует основное средство (алгоритм, фактор) идентификации и аутентификации (ИА), которое достаточно надежно, но которое, тем не менее, может быть преодолено нападающим, задана вероятность преодоления основного средства ИА при атаке на рабочее место (основное средство может быть основано на использовании паролей, биометрии, USB-ключей, смарткарт и т.п.). В случае доступа нападающего на заданное РМ известен ущерб защитника, который зависит от важности информации, хранимой или обрабатываемой на РМ. Требуется, определить целесообразность использования для рабочих мест дополнительного фактора аутентификации на основе клавиатурного почерка (КП). Известно, что отдельно КП как фактор аутентификации использовать не эффективно из-за относительно высокого значения вероятностей ошибок первого и второго родов, поэтому предлагается использовать клавиатурный почерк в виде дополнительного фактора. Основные достоинства КП: не требуется дополнительных устройств, идентификацию и аутентификацию можно проводить без ведома пользователя, получившего доступ к РМ по основному фактору аутентификации. Для КП как фактора аутентификации известны оценки вероятностей ошибок первого и второго родов. Применение дополнительного

³⁴ Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru

³⁵ Акулова Надежда Олеговна, МГТУ им. Н.Э. Баумана, Москва, akel17.95@yandex.ru

фактора аутентификации для защитника требует дополнительных ресурсов (это могут быть деньги, время, затрачиваемое на использование дополнительного фактора и др.). Предполагается, что со стороны нападения попытка получения доступа к РМ, также требует ресурсов (денежных, вычислительных и других), которые ограничены.

Предлагается следующая игровая задача: решение нападающего — это выбор РМ для атаки с целью получения доступа в условиях ограниченных ресурсов, а решение защитника — это выбор РМ, на которых будет использован дополнительный фактор ИА для повышения защищенности. В качестве показателя качества будем использовать суммарную оценку ущерба защитника, т.е. игра будет с нулевой суммой.

1. Математическая постановка задачи

1.1. Исходные данные

Базисные множества

$R = \{r_1, r_2, \dots, r_n\}$ – множество РМ, на которых используется механизм аутентификации, $N = \{1, 2, \dots, n\}$ – множество индексов РМ.

$G = \{g_1, g_2, \dots, g_m\}$ – множество ограниченных ресурсов стороны защиты, $M = \{1, 2, \dots, m\}$ – множество индексов этих ресурсов.

$Q = \{q_1, q_2, \dots, q_k\}$ – множество ограниченных ресурсов стороны нападения, $K = \{1, 2, \dots, k\}$ – множество индексов этих ресурсов.

Параметры элементов множеств и отношений между ними

$w_i^{(1)}, \forall i \in N$ – ущерб в случае ошибки 1-го рода при аутентификации по КП (не допуске к РМ законного пользователя) на i -ом РМ.

$w_i^{(2)}, \forall i \in N$ – ущерб в случае ошибки 2-го рода при аутентификации по КП (ущерб при обходе механизмов аутентификации незаконным пользователем, считается, что основное средство аутентификации преодолено нападающим) на i -ом РМ.

$p_i, \forall i \in N$ – вероятность преодоления основного средства аутентификации при атаке на i -ое РМ нападающего.

$p^{(1)}$ – вероятность ошибки 1-го рода при аутентификации по КП.

$p^{(2)}$ – вероятность ошибки 2-го рода при аутентификации по КП.

$a_{ji}, \forall j \in M, i \in N$ – значение j -го ограниченного ресурса защитника, используемого для проведения аутентификации по КП на i -ом РМ.

$b_j, \forall j \in M$ – максимальное значение j -го ограниченного ресурса, выделенное для проведения аутентификации по КП на всех РМ.

$c_{ji}, \forall j \in K, i \in N$ – значение j -го ограниченного ресурса стороны нападения, используемого для атаки на i -ое РМ.

$d_j, \forall j \in K$ – максимальное значение j -го ограниченного ресурса стороны нападения, выделенного на проведение атак на все РМ.

1.2 Искомые данные

Для защитника введем булеву переменную $x_i \in \{0, 1\}, \forall i \in N$, $x_i = 1$, если на i -ом РМ будем использовать аутентификацию по КП, $x_i = 0$ – в противном случае, переменные образуют вектор X .

Аналогично для нападающего введем булеву переменную $y_i \in \{0, 1\}, \forall i \in N$, $y_i = 1$, если на i -ое РМ нападающий будет осуществлять атаку, $y_i = 0$ – в противном случае, переменные образуют вектор Y .

1.3. Показатель качества

В качестве показателя качества будет использовать оценку суммарного ущерба стороны защиты при доступе стороны нападения к РМ. Для расчета ущерба используются следующие параметры:

- $w_i^{(2)}p_i$ – оценка ущерба при атаке на i -ое РМ нападающего в случае использования только основного фактора аутентификации;
- $w_i^{(2)}p_ip^{(2)}$ – оценка ущерба при атаке на i -ое РМ нападающего при использовании дополнительного фактора аутентификации по КП;
- $w_i^{(1)}p^{(1)}$ – оценка ущерба при использовании на i -ом РМ аутентификации по КП в случае ошибки 1-го рода (не допуск законного пользователя).

Ущерб защитника для множества РМ при использовании дополнительного фактора аутентификации будем считать так: $U = U_{max} - U_{пред} + U_{ош1}$, где U_{max} – максимальный ущерб, если не использовать аутентификацию по КП, $U_{пред}$ – предотвращенный ущерб при использовании аутентификации по КП, $U_{ош1}$ – ущерб из-за ошибок 1-го рода при использовании аутентификации по КП.

Перечисленные ущербы можно записать как функции от векторов X и Y : $U_{max}(Y) = \sum_{i \in N} w_i^{(2)}p_i y_i$, $U_{пред}(X, Y) = \sum_{i \in N} w_i^{(2)}p_i(1 - p^{(2)})x_i y_i$, $U_{ош1}(X) = \sum_{i \in N} w_i^{(1)}p^{(1)}x_i$.

Тогда показатель ущерба:

$$U(X, Y) = \sum_{i \in N} w_i^{(2)}p_i y_i - \sum_{i \in N} w_i^{(2)}p_i(1 - p^{(2)})x_i y_i + \sum_{i \in N} w_i^{(1)}p^{(1)}x_i. \quad (1)$$

Защитник желает этот показатель минимизировать, а нападающий максимизировать.

1.4. Ограничения

Система ограничений на использование ограниченных ресурсов стороной защиты, задающая множество допустимых альтернатив $\Delta_{доп}^{(X)}$, имеет вид:

$$\Delta_{доп}^{(X)}: \{\sum_{i \in N} a_{ji}x_i \leq b_j, \forall j \in M. \quad (2)$$

Система ограничений на использование ограниченных ресурсов стороной нападения, задающая множество допустимых альтернатив $\Delta_{доп}^{(Y)}$, имеет вид:

$$\Delta_{доп}^{(Y)}: \{\sum_{i \in N} c_{ji}y_i \leq d_j, \forall j \in K. \quad (3)$$

Таким образом, задача выбора дополнительного фактора аутентификации для заданного числа РМ стороной защиты и задача выбора рабочих мест для проведения атак для стороны нападения сводится к решению каждым из игроков своей задачи булевого программирования при фиксированной решении другого игрока. Сторона защиты минимизирует показатель (1) при ограничениях (2), а сторона нападения максимизирует показатель (1) при ограничениях (3).

2. Об алгоритмах для решения задачи поставленной задачи

Подобную задачу можно свести к матричной игре большой размерности, примеры этого представлены в [9, 10]

При решении подобных задач можно использовать разные критерии принятия решений. Рассмотрим два критерия: критерий гарантированного результата и критерий, основанный на поиске седловой точки.

Если использовать критерий гарантированного результата для защитника, то в поставленной задаче этот критерий превращается в критерий минимакса, возможный алгоритм решения в этом случае представлен в [8].

При поиске седловой точка игры, которая в чистых стратегиях может не существовать, но в смешанных стратегиях существует всегда, можно использовать алгоритм, описанный в [9, 10]. Этот алгоритм основан на идеях алгоритма Брауна-Робинсона, но без явного построения матрицы игры. Для сокращения вычислительной

сложности предложено не решать на каждом шаге задачу булевого программирования, а начиная с определенного шага алгоритма, использовать решения, полученные на предыдущих шагах.

Выводы

В работе представлены содержательная и математическая постановки задачи выбора рабочих мест, на которых необходимо использовать дополнительный фактор аутентификации в виде клавиатурного почерка, для стороны защиты и выбора рабочих мест для получения доступа к ним за счет преодоления основного фактора идентификации и аутентификации для стороны нападения. Постановка задачи является игрой с нулевой суммой, каждый из игроков должен решать свою задачу булевого программирования при фиксированном решении другого игрока. Для решения задачи представлены ссылки на алгоритм, реализующий критерий гарантированного результата для защитника, и алгоритм поиска седловой точки в смешанных стратегиях.

Подобная постановка задачи позволяет количественно обосновать выбор тех рабочих мест, на которых целесообразно использовать дополнительный фактор аутентификации в виде клавиатурного почерка с учетом возможного ущерба, ограничений на ресурсы защитника и нападающего, и возможных действий нападающего.

Достоверность представленных решений подтверждается корректностью постановки задачи, явной содержательной интерпретацией математической постановки задачи, а также ссылкой на источники, в которых описаны исследования алгоритмов, предложенных для решения похожих задач.

Литература

1. Liang Xiao, Dongjin Xu, Narayan B. Mandayam, H. Vincent. Poor Attacker-Centric View of a Detection Game against Advanced Persistent Threats // IEEE Transactions on Mobile Computing. 2018. Vol. 17. Iss. 11. P. 2512-2523. DOI: 10.1109/TMC.2018.2814052
2. Shirui Huang, Hengwei Zhang, Jindong Wang, Jianming Huang. Markov Differential Game for Network Defense Decision-Making Method // IEEE Access. 2018. Vol. 6. P. 39621-39634. DOI: 10.1109/ACCESS.2018.2848242
3. Mauro Barni, Benedetta Tondi. Adversarial Source Identification Game with Corrupted Training // IEEE Transactions on Information Theory. 2018. Vol. 64. Iss. 5. P. 3894-3915. DOI: 10.1109/TIT.2018.2806742
4. Hengwei Zhang, Lv Jiang, Shirui Huang, Jindong Wang, Yuchen Zhang. Attack-Defense Differential Game Model for Network Defense Strategy Selection // IEEE Access. 2019. Vol. 7. P. 50618-50629. DOI: 10.1109/ACCESS.2018.2880214
5. Hao Wu, Wei Wang. A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems // IEEE Transactions on Information Forensics and Security. 2018. Vol. 13. Iss. 6. P. 1432-1445. DOI: 10.1109/TIFS.2018.2790382
6. Lu-Xing Yang, Pengdeng Li, Yushu Zhang, Xiaofan Yang, Yong Xiang, Wanlei Zhou. Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach // IEEE Transactions on Information Forensics and Security. 2019. Vol. 14. Iss. 7. P. 1713-1728. DOI: 10.1109/TIFS.2018.2885251
7. Быков А.Ю., Крыгин И.А., Муллин А.Р. Алгоритм распределения ресурсов системы защиты между активами мобильного устройства на основе игры с нулевой суммой и принципа равной защищенности. Вестник МГТУ им. Н.Э. Баумана. Приборостроение. 2018. № 2. С. 48- 68. DOI: 10.18698/0236-3933-2018-2-48-68
8. Быков А. Ю., Алтухов Н. О., Сосенко А. С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры. Инженерный вестник МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 4. Режим доступа: <http://engbul.bmstu.ru/doc/708106.html>
9. Быков А.Ю., Крыгин И.А., Гришунин М.В. Алгоритм поиска седловой точки в смешанных стратегиях на основе модификации метода Брауна-Робинсона для решения задачи выбора защищаемых объектов. В сборнике: Безопасные информационные технологии Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 33-38.

10. Быков А.Ю., Гришунин М.В., Крыгин И.А. Игровая задача выбора защищаемых объектов и исследование алгоритма поиска седловой точки на основе модификации метода Брауна-Робинсона // Вопросы кибербезопасности. 2019. № 2 (30). С. 2-12. DOI: 10.21681/2311-3456-2019-2-2-12

The technique of choosing keyboard handwriting as an additional authentication factor for workplaces in game theory

Bykov A.Yu.³⁶, Akulova N.O.³⁷

Abstract. *A game formulation of the problem of two players, a defender and an attacker, is analyzed. A defender selects workplaces where it is necessary, in addition to the main authentication factor, to use the additional authentication factor in the form of keyboard handwriting, taking into account resource restrictions. An attacker chooses the workplaces that he will attack in order to gain access by overcoming the authentication mechanisms used. The problem formulation is a zero-sum game, a quality indicator is the assessment of the defender's damage, taking into account the importance of information processed at the workplace. In the task at hand, each of the players must solve their own Boolean programming problem with a fixed solution for the other player. The game can be reduced to a matrix game of large dimension. Links are provided to literature sources that describe algorithms for solving such problems: based on the principle of a guaranteed result and the search for the saddle point of the game in mixed strategies.*

Keywords: *information security, authentication and identification, keyboard handwriting, games theory, matrix game, discrete optimization.*

³⁶Aleksandr Bykov, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, abykov@bmstu.ru

³⁷Nadezhda Akulova, Bauman Moscow State Technical University, Moscow, akel17.95@yandex.ru

Постановка задачи выбора средств защиты на основе модели дискретно-непрерывной игры с противоположными интересами при ограничениях на ресурсы и подходы к ее решению

Быков А.Ю.³⁸, Крыгин И.А.³⁹

Для выбора средств защиты информации в системе обработки информации предложена игровая постановка задач двух игроков: защитника и нападающего. Защитник выбирает средства защиты из заданного множества при ограничениях на ресурсы, нападающий выбирает типы проводимых атак при ограничениях на свои ресурсы. У каждого игрока отдельный показатель качества выбора: для защитника – оценка возможного ущерба, для нападающего – оценка его выигрыша. Множество элементов выбора защитника является дискретным, множество элементов выбора нападающего – непрерывно, что связано с неопределенностью его действий. Защитник должен решать задачу нелинейного булевого программирования, а нападающий задачу линейного программирования при фиксированном решении другого игрока. Представлены подходы к решению подобных задач. Решение задачи позволит количественно обосновать выбор средств защиты для заданной системы с учетом ограничений и действий противоположной стороны.

Ключевые слова: защита информации, теория игр, равновесие по Нэшу, булево программирование, линейное программирование

Введение

Рассмотрим математическую постановку задачи выбора средств защиты информации (СЗИ) для некоторой системы обработки информации (программно-аппаратной основой подобных систем могут быть: локальная вычислительная сеть некоторого предприятия с возможным выходом в интернет, сервер или система серверов различного назначения и т.п.). Оптимизационные постановки задачи выбора СЗИ приведены в [1-3], в них угроз безопасности информации оценивались вероятностью их появления. При защите информации кроме стороны защиты, как правило, присутствует вторая сторона – сторона нападения, поэтому во многих случаях более адекватные модели выбора это модели теории игр (в случае непреднамеренных угроз могут рассматриваться игры с «природой»). В [4-13] приведены примеры использования теории игр при решении задач, связанных с различными аспектами защиты информации. В [8] представлена постановка задачи выбора СЗИ, в которой защитник выбирает средства защиты, а нападающий выбирает возможные типы атак (реализации угроз безопасности), постановка является дискретной. Ниже рассмотрим дискретно-непрерывную игру, в которой защитник выбирает средства защиты, множество элементов выбора защитника дискретно. Нападающий выбирает типы атак (средства реализации угроз), причем поведение нападающего описывается в виде вероятностей проведения атак (или возможностей их проведения в терминах нечетких множеств), множество элементов выбора нападающего непрерывно. Подобный подход применим при неполных данных о поведении нападающего.

1. Постановка задачи

Базисные множества

1. $Z = \{z_1, z_2, \dots, z_m\}$ – множество типов атак (реализаций угроз безопасности) в защищаемой системе, $M = \{1, 2, \dots, m\}$ – множество индексов этих атак.

³⁸ Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru

³⁹ Крыгин Иван Александрович, МГТУ им. Н.Э. Баумана, Москва, krygin.ia@gmail.com

2. $S = \{s_1, s_2, \dots, s_n\}$ – множество средств защиты (методов или способов), которые могут быть использованы для защиты системы, $N = \{1, 2, \dots, n\}$ – множество индексов этих средств.
3. $R^{(3)} = \{r_1^{(3)}, r_2^{(3)}, \dots, r_{l^{(3)}}^{(3)}\}$ – множество ограниченных ресурсов стороны защиты, $L^{(3)} = \{1, 2, \dots, l^{(3)}\}$ – множество индексов этих ресурсов. Примеры таких ресурсов: денежные средства, а также ресурсы вычислительных средств, каналов связи и т.п., требуемых для работы СЗИ.
4. $R^{(H)} = \{r_1^{(H)}, r_2^{(H)}, \dots, r_{l^{(H)}}^{(H)}\}$ – множество ограниченных ресурсов стороны нападения, $L^{(H)} = \{1, 2, \dots, l^{(H)}\}$ – множество индексов этих ресурсов. Примеры таких ресурсов аналогично как для стороны защиты.

Параметры элементов множеств и отношений между ними

1. $w_i^{(3)} \geq 0, \forall i \in M$ – оценка ущерба защитника при успешной для нападающего реализации i -го типа атаки.
2. $w_i^{(H)} \geq 0, \forall i \in M$ – оценка выигрыша нападающего при успешной для нападающего реализации i -го типа атаки.
3. $p_{ij} \in [0, 1], \forall i \in M, j \in N$ – вероятность (или возможность) предотвращения i -ой атаки (реализации угрозы) при использовании j -го средства защиты (одно средство защиты может защищать от нескольких типов атак с разной эффективностью).
4. $a_{kj}^{(3)} \geq 0, \forall k \in L^{(3)}, j \in N$ – значение k -го ограниченного ресурса защитника, необходимого для функционирования j -го средства защиты.
5. $b_k^{(3)} \geq 0, \forall k \in L^{(3)}$ – максимальное значение объема k -го ограниченного ресурса защитника, который он может использовать на все СЗИ.
6. $a_{ki}^{(H)} \geq 0, \forall k \in L^{(H)}, i \in M$ – значение k -го ограниченного ресурса нападающего, необходимого для проведения i -го типа атаки.
7. $b_k^{(H)} \geq 0, \forall k \in L^{(H)}$ – максимальное значение объема k -го ограниченного ресурса нападающего, который он может использовать для проведения всех типов атак.

Искомые переменные

Для стороны защиты введем булеву переменную $x_j \in \{0, 1\}, \forall j \in N$, $x_j = 1$, если используется j -ое средство защиты, $x_j = 0$ – в противном случае, переменные образуют вектор $\vec{X}$.

Для стороны защиты введем переменную $y_i \in [0, 1], \forall i \in M$, значение y_i , можно интерпретировать как вероятность или возможность (в терминах нечетких множеств) проведения i -го типа атаки, переменные образуют вектор $\vec{Y}$.

Показатели игроков

При расчете ущерба защитника будем полагать, что вероятность (степень защищенности при нечетком описании) защиты от i -го типа атаки при использовании нескольких средств защиты определяется средством защиты с максимальной

вероятностью: $P_i = \max_{j \in N} \{p_{ij}x_j\}, \forall i \in M$. Тогда оценка предотвращенного ущерба $U_{\text{пр}}(\vec{X}, \vec{Y}) = \sum_{i \in M} P_i w_i^{(3)} y_i = \sum_{i \in M} \max_{j \in N} \{p_{ij}x_j\} w_i^{(3)} y_i$.

Оценка полного ущерба стороны защиты это есть оценка максимального ущерба (если не использовать защиту) минус оценка предотвращенного ущерба:

$$U(\vec{X}, \vec{Y}) = \sum_{i \in M} w_i^{(3)} y_i - \sum_{i \in M} \max_{j \in N} \{p_{ij}x_j\} w_i^{(3)} y_i. \quad (1)$$

Защитник хочет этот показатель минимизировать.

Оценка выигрыша стороны нападения вычисляется по аналогичным принципам:

$$V(\vec{X}, \vec{Y}) = \sum_{i \in M} w_i^{(H)} y_i - \sum_{i \in M} \max_{j \in N} \{p_{ij}x_j\} w_i^{(H)} y_i. \quad (2)$$

Первое слагаемое определяет выигрыш нападающего при отсутствии защиты, слагаемое со знаком минус это упущенный выигрыш нападающего из-за применения защиты. Нападающий хочет этот показатель максимизировать.

Ограничения

Ограничения на использование ограниченных ресурсов стороны защиты, требуемых на функционирование СЗИ:

$$\sum_{j \in N} a_{kj}^{(3)} x_j \leq b_k^{(3)}, \forall k \in L^{(3)}. \quad (3)$$

Ограничения на использование ограниченных ресурсов стороны нападения, требуемых на проведение атак:

$$\sum_{i \in M} a_{ki}^{(H)} y_i \leq b_k^{(H)}, \forall k \in L^{(H)}. \quad (4)$$

Представленная поставка задачи с показателями игроков (1), (2) и ограничениями для игроков (3) и (4) является смешанной дискретно-непрерывной игрой. Сторона защиты должна решать задачу булевого программирования с нелинейным по $\vec{X}$ показателем (1) и ограничениями (3) при фиксированном решении стороны нападения $\vec{Y}$, а сторона нападения решает задачу линейного программирования с показателем (2) (показатель линейный относительно $\vec{Y}$) и ограничениями (4) при фиксированном $\vec{X}$.

2. Подходы к решению задачи

Рассмотрим два основных подхода принятия решения для стороны защиты:

- подход, основанный на обеспечении гарантированного результата;
- подход, основанный на поиске равновесного состояния, в данном случае, состояния, удовлетворяющего критерию равновесия по Нэшу.

При использовании подхода на основе гарантированного результата со стороны защиты защитник использует принцип минимакса. Для неполного перебора возможных решений защитника можно использовать алгоритм, подобный, рассмотренному в [8]. При неполном переборе исключаются из рассмотрения недопустимые решения защитника и решения защитника, которые доминируются другими решениями (например, при исключении из допустимого решения некоторых средств защиты значение показателя качества для защитника не улучшится в рамках рассмотренной модели). При этом для каждого рассматриваемого решения защитника при неполном переборе решаем задачу для нападающего – максимизация показателя (2) при ограничениях (4), получаем решение нападающего. Для полученной пары решений защитника и нападающего вычисляем значение показателя (1). При переборе таких пар находим пару с минимальным значением показателя (1). Это и будет гарантированное значение показателя защитника.

При подходе, основанном на поиске равновесного состояния, удовлетворяющего критерию Нэша, для получения точного решения можно модифицировать алгоритм,

описанный в [12], а для получения приближенного решения можно использовать модифицированный метод, использующий идеи метода Брауна-Робинсона. Для дискретного выбора пример подобного метода представлен в [10, 11]. В случае поиска решений, когда решения одной стороны непрерывно, необходимо в качестве фиксированного решения стороны нападения, используемого для поиска $\vec{X}$ на каждом шаге алгоритма, применять среднюю точку в пространстве векторов $\vec{Y}$, как среднее среди решений, получаемых для стороны нападения при фиксированном $\vec{X}$ на каждом шаге алгоритма.

Выводы

В работе представлена математическая постановка задачи выбора средств защиты в системе обработки информации для стороны защиты и выбора типов атак для стороны нападения. Постановка задачи является дискретно-непрерывной игрой с разными показателями качества игроков, защитник должен решать задачу нелинейного булевого программирования, а нападающий задачу линейного программирования при фиксированном решении другого игрока. Непрерывность решения со стороны нападения позволяет учесть неопределенность поведения нападающего. Для решения задачи предложены два подхода: на основе гарантированного результата для стороны защиты и на основе поиска равновесной ситуации по Нэшу, приведены ссылки на алгоритмы решения похожих задач.

Постановка задачи позволяет количественно обосновать выбор средств защиты с учетом возможного ущерба, ограничений на ресурсы защитника и возможных действий стороны нападения.

Достоверность представленных решений подтверждается корректностью постановки задачи, ее очевидной содержательной интерпретацией, а также ссылкой на источники, в которых описаны исследования алгоритмов, предложенных для решения частично похожих задач.

Литература

1. Овчинников А.И., Журавлев А.М., Медведев Н.В., Быков А.Ю. Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2007. № 3. С. 115-121
2. Овчинников А.И., Медведев Н.В., Быков А.Ю. Применение метода вектора спада для решения задачи поиска вариантов защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2008. № 2. С. 73-82
3. Быков А. Ю., Панфилов Ф.А., Шмырев Д.В. Задача выбора средств защиты в автоматизированных системах с учетом классов защищенности от несанкционированного доступа к информации // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 1. С. 193-199. DOI: 10.18698/2308-6033-2012-1-85
4. Richeng Jin, Xiaofan He, Huaiyu Dai. On the Security-Privacy Tradeoff in Collaborative Security: A Quantitative Information Flow Game Perspective. IEEE Transactions on Information Forensics and Security. 2019. Vol. 14. Iss. 12. P. 3273-3286. DOI: 10.1109/TIFS.2019.2914358
5. Zhen Ni, Shuva Paul. A Multistage Game in Smart Grid Security: A Reinforcement Learning Solution. IEEE Transactions on Neural Networks and Learning Systems. 2019. Vol. 19. Iss. 9. P. 2684-2695. DOI: 10.1109/TNNLS.2018.2885530
6. Zemin Sun, Yanheng Liu, Jian Wang, Fang Mei, Weiwen Deng, Yuming Ge. Non-Cooperative Game of Throughput and Hash Length for Adaptive Merkle Tree in Mobile Wireless Networks. IEEE Transactions on Vehicular Technology. 2019. Vol. 68. Iss. 5. P. 4625-4650. DOI: 10.1109/TVT.2019.2899647
7. Fanyu Kong, Yufeng Zhou, Bin Xia, Li Pan, Limin Zhu. A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment. IEEE Access. 2019. Vol. 7. P. 161822-161830. DOI: 10.1109/ACCESS.2019.2950731

8. Быков А. Ю., Алтухов Н. О., Сосенко А. С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры // Инженерный вестник МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 4. С. 525-542. Режим доступа: <http://engbul.bmstu.ru/doc/708106.html> (дата обращения 20.11.2019)

9. Быков А.Ю., Крыгин И.А., Муллин А.Р. Алгоритм распределения ресурсов системы защиты между активами мобильного устройства на основе игры с нулевой суммой и принципа равной защищенности // Вестник МГТУ им. Н.Э. Баумана. Приборостроение. 2018. № 2. С. 48- 68. DOI: 10.18698/0236-3933-2018-2-48-68

10. Быков А.Ю., Крыгин И.А., Гришунин М.В. Алгоритм поиска седловой точки в смешанных стратегиях на основе модификации метода Брауна-Робинсона для решения задачи выбора защищаемых объектов // В сборнике: Безопасные информационные технологии Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 33-38.

11. Быков А.Ю., Гришунин М.В., Крыгин И.А. Игровая задача выбора защищаемых объектов и исследование алгоритма поиска седловой точки на основе модификации метода Брауна-Робинсона // Вопросы кибербезопасности. 2019. № 2 (30). С. 2-12. DOI: 10.21681/2311-3456-2019-2-2-12

12. Bykov A.Yu., Grishunin M.V., Krygin I.A. Saddle point search algorithm for the problem of site protection level assignment based on search of simplices // Вестник Московского государственного технического университета им. Н.Э. Баумана. Сер. Приборостроение, 2019, № 2 (125), с. 22-39. DOI: 10.18698/0236-3933-2019-2-22-39

13. Крыгин И.А. Математическая постановка задачи распределения вычислительных ресурсов между средствами защиты информации на основе дискретно-непрерывной игры // В сборнике: Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С 107-111

The statement of security tools selection problem based on non-zero-sum discrete-continuous game with resources limitations and approaches for its solving

Bykov A.Yu.⁴⁰, Krygin I.A.⁴¹

Abstract. *It is suggested the game problem statement of two players, defender and attacker, to select information security tools in information processing system. Defender selects information security tools from given set considering his resources limitations, attacker selects attacks considering his resources limitations. Each player has his own selection quality parameter: for defender – possible damage estimation, for attacker – his benefit estimation. The set of defender selection items is discrete, the set of attacker selection items is continuous. It's related to with attacker's actions unpredictability. Defender solves nonlinear boolean programming problem, and attacker solves linear programming problem with fixed opponent solution. Approaches for solving such problems are presented. The solution of this problem allows to substantiate quantitatively security tools selection for given system with limitations and attacker actions.*

Keywords: *information security, game theory, Nash equilibrium, boolean programming, linear programming*

⁴⁰Aleksandr Bykov, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, abykov@bmstu.ru

⁴¹Ivan Krygin, Bauman Moscow State Technical University, Moscow, krygin.ia@gmail.com

Методы аутентификации с использованием носимых устройств

Ванин А.В.⁴²

Аннотация. Обоснована актуальность изучения методов аутентификации с использованием носимых устройств на основе результатов осуществленного патентного поиска в отечественном и зарубежном сегментах. Предложена классификация методов аутентификации с использованием носимых устройств на основе факторов владения (токен), знания (пароль) и сущности (биометрия). Приведены примеры наиболее современных методов аутентификации с использованием таких носимых устройств как умные часы, очки, кольца. Сделан вывод относительно перспектив дальнейшего развития области изучения и разработки схем и методов аутентификации с использованием носимых устройств.

Ключевые слова. Схемы и методы аутентификации, патентный поиск, умные часы, умные очки, умное кольцо, смартфон.

Введение

Процедура аутентификации может представлять определенные трудности для пользователя становясь чрезмерно отягощенной [1]. В этом случае своеобразным компенсирующим средством выступают методы аутентификации с использованием носимых устройств (умные часы, очки, браслеты, кольца, одежда), гарантирование безопасности которых также является актуальной задачей [2].

Патентный поиск и классификация

Актуальность и перспективность изучения подтверждается проведенным в соответствии с ГОСТ Р. 15.011-96 патентным поиском (цифры актуальны на ноябрь 2019 года). По данной тематике и схожей с ней в отечественном патентном сегменте подано 56 заявок (на основе данных ФИПС), несоизмеримо большее количество в зарубежном – 43241 (на основе данных Google Patents).

Основой классификации методов аутентификации с использованием носимых устройств может выступать схема, разделяющая техники аутентификации на те, которые подчинены факторам: собственности («то, чем владеешь» / токен), знания («то, что знаешь» / пароль) и сущности («то, чем являешься» / биометрия).

Токен

Система аутентификации концептуально схожая использованию физических ключа и замка предложена в работе [3]. В ней обладатель умных часов, содержащих доверенный сертификат, аутентифицируется через мобильный терминал путем прикладывания к нему часов. Сертификат исследуется терминалом на предмет в предоставлении/отказе авторизованного уровня доступа.

С целью оптимизации данной схемы Corner и Noble [4] предложена парадигма аутентификации нулевого взаимодействия, в которой используется активный токен, автономно собирающий доверительные сертификаты и связывающийся с устройством пользователя через беспроводную связь малой дальности. Южнокорейские коллеги [5] предлагают схожую схему, использующую при этом комбинацию смарт-часов и мобильного телефона. В ней пользователь получает авторизацию для совершения защищенных онлайн-транзакций до тех пор, пока оснащенные NFC смарт-часы связаны с мобильным устройством [6].

⁴² Ванин Александр Владимирович, магистрант МГТУ им. Н.Э. Баумана, г. Москва, эл. почта: vaninav@student.bmstu.ru

В работе [7] предлагается носимый ключ, базирующийся на передаче сигналов через тело пользователя, аутентифицирующее его в случае прикосновения к устройству. Похожее решение, основанное на инфракрасном излучении предложено немецкими исследователями [8]. Пользователь – обладатель кольца осуществляет прикосновение к настольному экрану, в результате чего передаются псевдослучайные битовые последовательности, декодируемые дисплеем для осуществления аутентификации.

Пароль

Личные дисплеи при использовании умных очков исследуются в работе D. Yadav [9], сопоставляя проверки подлинности через прикосновение или голос с выводом изображения на экран устройства.

Аналогично, P. Chan [10] представил схему аутентификации для разблокировки умных очков, когда QR-код продублирован на смартфон пользователя и его сканирование осуществляется с использованием встроенной камеры.

J. Thorpe [11] изучает, каким образом могут существовать технологии интерфейсов объединяющих мозг человека и его персональное устройство, используя ввод пароля как основной механизм аутентификации.

Биометрия

Классифицируется на методы: 1) явные, направленные на измерение врожденных характеристик пользователя; 2) имплицитные, осуществляющие сбор данных с устройства пользователя в «скрытом» режиме; 3) носимые системы аутентификации, соединяющие в себе явные и имплицитные составляющие.

Современные разработки с применением устройств типа умных очков обращаются к распознаванию радужной оболочки глаз [12].

J. Yang [13] предлагает приложение, собирающее данные относительно движений от надетого на запястье устройства в процессе воспроизведения жестов с целью идентификации. В пространстве мобильных приложений также разрабатываются имплицитные методы аутентификации пользователя [14]. Данная череда исследований базируется на парадигме непрекращающейся аутентификации, основанной на поведенческой биометрии, получившая название сенсорно-обусловленной аутентификации [15]. Источником для нее служат: данные, извлекаемые с датчиков, прикрепленных к телу пользователя (например, с сенсоров движения); данные, собираемые в процессе активного взаимодействия пользователя с персональным устройством (например, с экраном смартфона).

Исследуются также возможности аутентификации, основанной на параметрах температуры тела пользователя с использованием умных часов и аппарата нейронных сетей [16].

Предлагаются методы реализации процесса аутентификации посредством анализа частоты сердечных сокращений с использованием датчика ЭКГ при использовании комбинации смартфона и умных часов [17].

Наконец, разработка «BreathPrint» [18], представляет схему, основанную на акустических особенностях дыхания человека [19, 20], снимаемых обычным микрофоном смартфона.

Выводы

Несмотря на то, что аутентификация с использованием носимых устройств представляет только зарождающийся исследовательский интерес, комбинация носимых технологий с мобильными платформами уже сегодня предоставляет новые возможности по причине увеличивающихся вычислительной мощности и интерактивных возможностей. Скорее, чем служить в качестве обычных токенов, носимые устройства, несомненно, будут играть в ближайшем будущем значительную роль в реализации эффективных многофакторных схем аутентификации.

Литература

1. Барабанов А.В. и др. Семь безопасных информационных технологий - М.: ДМК Пресс, 2017. 224 с.
2. Das, Ashok Kumar (2017). Lightweight authentication protocols for wearable devices / Ashok Kumar Das, Sherali Zeadally, Mohammad Wazid // Computers & Electrical Engineering. Volume 63 (pp. 196-208).
3. Al-Muhtadi, J., Mickunas, M. D., & Campbell, R. H. (2001). Wearable security services. In Proceedings 21st International Conference on Distributed Computing Systems Workshops (pp. 266–271).
4. Corner, M. D., & Noble, B. D. (2002). Zero-interaction authentication. In Proceedings of the 8th annual international conference on Mobile computing and networking (pp. 1–11).
5. Cha, B.-R., Lee, S.-H., Park, S.-B., Lee, G.-K., & Ji, Y.-K. (2015). Design of Micro-payment to Strengthen Security by 2 Factor Authentication with Mobile & Wearable Devices. In Security, Reliability, and Safety 2015 (pp. 28–32).
6. Рабинович А.С., Казарин О.В. Методика аутентификации пользователя в информационной системе с использованием технологии NFC // Вопросы кибербезопасности. 2013. № 2 (2). С. 59-62.
7. Matsushita, N., Tajima, S., Ayatsuka, Y., & Rekimoto, J. (2000). Wearable key: device for personalizing nearby environment. In Digest of Papers. Fourth International Symposium on Wearable Computers (pp. 119–126).
8. Roth, V., Schmidt, P., & Güldenring, B. (2010). The IR ring: authenticating users' touches on a multi-touch display. In Proceedings of the 23rd annual ACM symposium on User interface software and technology (pp. 259–262).
9. Yadav, D. K., Ionascu, B., Ongole, S. V. K., Roy, A., & Memon, N. D. (2015). Design and Analysis of Shoulder Surfing Resistant PIN based Authentication Mechanisms on Google Glass. In International Conference on Financial Cryptography and Data Security (pp. 281–297).
10. Chan, P., Halevi, T., & Memon, N. D. (2015). Glass OTP: Secure and Convenient User Authentication on Google Glass. In International Conference on Financial Cryptography and Data Security (pp. 298–308).
11. Thorpe, J., Oorschot, P. C. van, & Somayaji, A. (2005). Pass-thoughts: authenticating with our minds. In Proceedings of the 2005 workshop on New security paradigms Vol. 2005 (pp. 45–56).
12. Li, Y.-H., & Huang, P.-J. (2017). An Accurate and Efficient User Authentication Mechanism on Smart Glasses Based on Iris Recognition. Mobile Information Systems (pp. 1–14).
13. Yang, J., Li, Y., & Xie, M. (2015). MotionAuth: Motion-based authentication for wrist worn smart devices. In 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) (pp. 550–555).
14. Luca, A. D., Hang, A., Brudy, F., Lindner, C., & Hussmann, H. (2012). Touch me once and I know it's you!: implicit authentication based on touch screen patterns. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 987–996).
15. Shen, C., Chen, Y., & Guan, X. (2018). Performance evaluation of implicit smartphones authentication via sensor-behavior analysis. Information Sciences, 430, (pp. 538–553).
16. Enamamu, T. S., Clarke, N., Haskell-Dowland, P., & Li, F. (2017). Smart watch based body-temperature authentication. In 2017 International Conference on Computing Networking and Informatics (ICCNI) (pp. 1–7).
17. Kang, S. J., Lee, S. Y., Cho, H. I., & Park, H. (2016). ECG Authentication System Design Based on Signal Analysis in Mobile and Wearable Devices. IEEE Signal Processing Letters, 23(6) (pp. 805–808).
18. Chauhan, J., Hu, Y., Seneviratne, S., Misra, A., Seneviratne, A., & Lee, Y. (2017). BreathPrint: Breathing Acoustics-based User Authentication. In Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (pp. 278–291).
19. Горшков Ю.Г. Акустографическое исследование звуков сердца и легких с оценкой эмоциональной напряженности пациента по голосу. В сборнике: Биотехнические, медицинские, экологические системы и робототехнические комплексы - Биомедсистемы-2017 сборник трудов

XXX Всероссийской научно-технической конференции студентов, молодых ученых и специалистов. Рязанский государственный радиотехнический университет. 2017. С. 163-166.

20. Устройство оценки эмоциональной напряженности человека по голосу / Горшков Ю.Г. и др. - Патент на полезную модель RUS 165114 14.09.2015. 2016.

Научный руководитель. Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, v.tsirlov@bmstu.ru

Authentication methods using wearable devices

Vanin A.V.⁴³

Abstract. *The relevance of the study of authentication methods using wearable devices based on the results of the patent search in the domestic and foreign segments is substantiated. The classification of authentication methods using wearable devices based on the factors of ownership (token), knowledge (password) and entity (biometrics) is proposed. Examples of the most modern authentication methods using such wearable devices as smartwatches, glasses, rings are given. The conclusion is made regarding the prospects for further development of the field of study and development of methods of authentication using wearable devices.*

Keywords. *Authentication schemes and methods, patent search, smartwatch, smart ring, smart glasses, smartphone.*

⁴³ Vanin Alexander Vladimirovich, graduate student, Bauman Moscow State Technical University, Moscow, e-mail: vaninav@student.bmstu.ru

Усиление стойкости протокола обмена ключами с аутентификацией Белловина и Меррита за счет использования асимметричного выполнения криптосистем

Варфоломеев А. А.⁴⁴

Аннотация. Протоколы выработки высокоэнтروпийных криптографических сеансовых ключей из долговременных низкоэнтропийных ключей или паролей (PAKE - Password Authenticated Key Exchange) служат для повышения стойкости защиты информации в информационных системах. В работе показывается, как повысить еще и стойкость самих протоколов PAKE на примере классического протокола EKE (Encrypted Key Exchange) Белловина и Меррита за счет использования предложенной ранее автором концепции асимметричного выполнения криптосистем (см., например, SIBCON 2016, РусКрипто 2018).

Асимметричное выполнение операций в криптосистемах предполагает умышленное существенное увеличение трудоемкости выполнения операций для одного из законных пользователей (например, для сервера, за счет дополнительных преобразований открытого текста, увеличения пароля на случайную величину, выбора режима работы шифров, сокрытия части необходимой для операции информации), приводящее к существенному увеличению трудоемкости нахождения секретных ключей и для злоумышленника.

Ключевые слова: криптография, криптографические протоколы, ключи, трудоемкость, стойкость, протокол EKE.

Введение

Данная работа, помимо самостоятельного значения, является продолжением ряда работ автора в области усиления стойкости криптосистем с короткими ключами. Под короткими ключами понимаются ключи симметричных и асимметричных криптосистем, заданных ограничением для безлицензионного использования, введенным известным Постановлением Правительства РФ от 16.04.2012 № 313. Согласно Постановлению, без лицензии можно применять «симметричный криптографический алгоритм, использующий криптографический ключ длиной, не превышающей 56 бит, либо асимметричный криптографический алгоритм, основанный либо на методе разложения на множители целых чисел, размер которых не превышает 512 бит, либо на методе вычисления дискретных логарифмов в мультипликативной группе конечного поля размера, не превышающего 512 бит, либо на методе вычисления дискретных логарифмов в иной группе размера, не превышающего 112 бит».

В литературе часто используется понятие низкоэнтропийных ключей, по сравнению с высокоэнтропийными ключами в 256 бит, характерными для современных стандартных алгоритмов шифрования. Короткие ключи можно отнести к низкоэнтропийным, но ряд авторов относят к низкоэнтропийным ключам парольные слова и даже PIN – коды, энтропия которых меньше 56 бит.

В работе [1] для симметричных шифров предлагалось внести асимметрию в трудоемкость работы при зашифровании открытого текста и при расшифровании шифртекста законными пользователями. В связи с этим такие шифры и криптосистемы были названы асимметрично выполняемыми. Законный получатель шифртекста в этом

⁴⁴ Варфоломеев Александр Алексеевич, кандидат физико-математических наук, доцент, Московский государственный технический университет имени Н.Э. Баумана, г. Москва, Российская Федерация, a.varfolomeev@mail.ru

случае тратил существенно больше времени на расшифрование, так как ему приходилось опробовать случайный двоичный вектор, на который был увеличен использованный при зашифровании короткий ключ, известный отправителю и получателю сообщения. Злоумышленник для нахождения открытого текста должен был опробовать и короткий ключ и добавленный отправителем к ключу случайный вектор. Конечно, при этом предполагается наличие у отправителя качественного генератора случайных двоичных последовательностей, а для модели злоумышленника – возможность использования для дешифрования только метод полного опробования.

Для усиления стойкости в работе [2] предлагались и другие способы, включая предварительное преобразование открытого текста типа AON- преобразования. Существенным для эффективности реализации оказалось использования новых (по сравнению с ГОСТ 28147-89) режимов работы блочных шифров по стандарту ГОСТ 34.13.

Далее на конференции РусКрипто 2018 [3] автором для усиления стойкости шифров с короткими ключами было предложено использовать протоколы РАКЕ, где в качестве парольного слова использовать короткий ключ. Например, при совместном использовании симметричного и асимметричного шифров с короткими ключами в протоколе ЕКЕ [4] трудоемкость дешифрования не является суммой трудоемкостей дешифрования каждого из шифров, а является их произведением.

В данной работе показывается, как внесение асимметрии в трудоемкость выполнения операций законными пользователями самих протоколов РАКЕ приводит к увеличению трудоемкости решения задач криптоанализа для злоумышленника на примере известных широко известных протоколов.

В ряде работ ранее рассматривалось понятие «асимметричного РАКЕ» (см., например, [5], [6]), но причина использования слова «асимметрия» отличается от изложенного в данной работе. Асимметричный РАКЕ – это тот же РАКЕ в клиент-серверной архитектуре, где сервер хранит не само парольное слово, а значение однонаправленной функции от него. В случае компрометации сервера, злоумышленнику придется выполнить еще дополнительную офф - лайн атаку для нахождения парольного слова.

Криптографический протокол ЕКЕ Белловина - Меррита и предложения по усилению его стойкости.

Протокол ЕКЕ [4] является одним из первых протоколов обмена ключами с аутентификацией на основе парольного слова. Целью протокола является безопасная транспортировка высокоэнтропийного ключа от одного пользователя другому при наличии у них общего низкоэнтропийного секрета (пароля). Протокол ЕКЕ имеет запатентован.

Для замкнутости изложения напомним этапы и шаги протокола ЕКЕ. Обозначим через PW – парольное слово, известное пользователям А и В.

Этап транспортировки ключа.

- 1. А: посылает сообщение $[A, E(PW; PK_A)] \rightarrow B$,

где $E(PW; PK_A)$ – преобразование зашифрования симметричным шифром на ключе PW, PK_A – открытый ключ пользователя А для асимметричного шифра.

- 2. В: вырабатывает высокоэнтропийный ключ k и посылает $E(PW; E_{PK_A}(k)) \rightarrow A$.

Этап подтверждения получения ключа k – «Запрос-ответ».

- 3. А: Из $E(PW; E_{PK_A}(k))$ получает k , посылает $E(k; R_a) \rightarrow B$.
- 4. В: Из $E(k; R_a)$ получает R_a , посылает $E(k; h(R_a) \parallel R_b) \rightarrow A$, здесь h – некоторая хэш-функция.
- 5. А: Из $E(k; h(R_a) \parallel R_b)$ получает $h(R_a) \parallel R_b$ и проверяет $h(R_a)=?$, далее посылает $E(k; h(R_b)) \rightarrow B$.

- 6. В: Из $E(k; h(R_b))$ получает и проверяет $h(R_b)=?$

Согласно модели Долева - Яо, злоумышленник на шаге 1 получает для off-line атаки шифртекст $E(PW; PKa)$. Ввиду сравнительно малого числа вариантов для выбора PW , он может их все перебрать и получить варианты для открытого ключа PKa . Но этот ключ, являющийся открытым текстом для $E(PW; PKa)$, не имеет структурности и похож на случайную последовательность бит. Поэтому выделить истинное парольное слово на этом шаге он не может.

На шаге 2 каждый выбранный вариант PW приводит к задаче нахождения ключа k по соответствующему открытому ключу PKa с 1 шага и по шифртексту $E_{PKa}(k)$, полученному при расшифровании $E(PW; E_{PKa}(k))$ на PW . Даже при возможности опробования всех секретных ключей асимметричного алгоритма зашифрования невозможно определить истинный ключ k , так как он тоже не имеет структурности. При коротких открытых и секретных ключах асимметричного алгоритма (например, в 512 бит) возможно более быстрое нахождение k , но все равно в числе вариантов для PW .

Отсюда следует, что, для увеличения трудоемкости нахождения ключа k злоумышленником, необходимо увеличить число вариантов для PW .

Приведем варианты усиления стойкости протокола ЕКЕ только для этапа транспортировки ключа, опустив второй этап для краткости изложения.

1 вариант усиления протокола.

- 1. А: $[A, E(PW-Ra; PKa \parallel h(PKa))]$ → В, где Ra – случайный вектор, выбранный пользователем А и не известный пользователю В.
- 2. В перебирает Ra и ищет Pka по критерию на открытый текст. Далее посылает $E(PW; E_{PKa}(k))$ → А.

На шаге 1 в открытый текст PKa добавлен хэш-код от него, чтобы придать структурность этому открытому тексту для того, чтобы пользователь В мог найти истинный открытый ключ PKa пользователя А. Трудоемкость расшифрования для В увеличена в $2^{|Ra|}$, где $|Ra|$ – размер вектора Ra .

Но критерий на открытый текст получает и злоумышленник. Таким образом, этот случай подобен случаю передачи шифрованного текста, полученного зашифрованием структурного открытого текста на ключе PW (структурность текста вида $PKa \parallel h(PKa)$ выбрана для наглядности). Для усиления стойкости шифрования в этом случае могут быть применены рекомендации предыдущих работ [1-2].

2 вариант усиления протокола.

На первом шаге шифруется некоторое множество открытых ключей пользователя А: $PKa1, PKa2, \dots, PKaN$.

- 1. А: $[A, E(PW; PKa1, PKa2, \dots, PKaN)]$ → В.
- 2. В: После расшифрования шифртекста $E(PW; PKa1, PKa2, \dots, PKaN)$ и получения множества открытых ключей $\{PKa1, PKa2, \dots, PKaN\}$, пользователь В случайно выбирает один из них - ключ $PKaJ$.
- Далее В вырабатывает высокоэнтропийный ключ k и посылает пользователю А сообщение $E(PW; E_{PKaJ}(k \parallel h(k)))$ → А.
- 3. А, зная парольное слово PW , расшифровывает $E(PW; E_{PKaJ}(k \parallel h(k)))$ и восстанавливает $E_{PKaJ}(k \parallel h(k))$, перебирает свои открытые ключи $PKa1, PKa2, \dots, PKaN$, ищет $PKaJ$ и ключ k . Критерий нахождения истинного ключа k – нахождение ключа k с правильным прикрепленным значением $h(k)$.

Пользователь А в этом варианте работает больше В. Он должен на шаге 3 перебрать все N посланные пользователю В открытые ключи $PKa1, PKa2, \dots, PKaN$.

На шаге 1 как и раньше последовательность $PKa_1, PKa_2, \dots, PKa_N$ не обладает структурностью, что не дает возможности злоумышленнику восстановить парольное слово PW из шифртекста $E(PW; PKa_1, PKa_2, \dots, PKa_N)$ даже полным опробованием.

На шаге 2 имеем $E\_PKaJ(k \amalg h(k))$ – шифртекст, полученный зашифрованием текста $(k \amalg h(k))$ на открытом ключе $PKaJ$ пользователя A . Он не имеет структурности, что не позволяет злоумышленнику найти PW из шифртекста $E(PW; E\_PKaJ(k \amalg h(k)))$ даже полным опробованием.

После 1 шага злоумышленник может иметь $IPWI$ вариантов множества открытых ключей $\{PKa_1, PKa_2, \dots, PKa_N\}$, где $IPWI$ – число возможных вариантов слова PW .

После 2 шага злоумышленник имеет $IPWI * N$ задач дешифрования шифртекста $E\_PKaJ(k \amalg h(k))$. Для оценки сложности дешифрования нужно исходить из стойкости используемого асимметричного алгоритма.

3 вариант усиления протокола.

- 1. $A: [A, E(PW - Ra; PKa_1, PKa_2, \dots, PKa_N, h(*)))] \rightarrow B$.
- 2. B : Перебирает Ra и ищет истинный набор открытых ключей. Критерий – структурность текста $[PKa_1, PKa_2, \dots, PKa_N, h(*)]$. Выбирает один ключ $PKaJ$ пользователя A .
- $E(PW - Ra; E\_PKaJ(k \amalg h(k))) \rightarrow A$, k – высокоэнтропийный ключ.
- 3. A : перебирает свои открытые ключи $PKa_1, PKa_2, \dots, PKa_N$ (Ra – знает), ищет $PKaJ$ и ключ k . Критерий – нахождение ключа k с правильным прикрепленным значением $h(k)$.

4 вариант усиления протокола.

- 1. $A: [A, E(PW - Ra; PKa_1, PKa_2, \dots, PKa_N, h(*)))] \rightarrow B$.
- 2. B : Перебирает Ra и ищет истинный набор открытых ключей. Критерий – структурность текста $[PKa_1, PKa_2, \dots, PKa_N, h(*)]$. Выбирает один ключ $PKaJ$ пользователя A .
- $E(PW - Rb; E\_PKaJ(k \amalg h(k))) \rightarrow A$, k – высокоэнтропийный ключ.
- 3. A : перебирает свои открытые ключи $PKa_1, PKa_2, \dots, PKa_N$ и Rb , ищет $PKaJ$ и ключ k . Критерий – нахождение ключа k с правильным прикрепленным значением $h(k)$.

В четвертом варианте трудоемкость работы пользователя A возрастает за счет неизвестности вектора Rb и выбора пользователем B одного из N открытых ключей, а трудоемкость работы пользователя B возрастает за счет неизвестности вектора Ra .

В 3 варианте вектор $Rb = Ra$ и известен пользователю A .

Но во всех этих вариантах соответственно возрастает и сложность задачи дешифрования для злоумышленника.

В данной работе не приводятся конкретные параметры усиления стойкости, так как во многом они зависят от вычислительной мощности злоумышленника и вычислительной мощности законных участников взаимодействия, а также от требования оперативности получения информации, которое может в свою очередь диктоваться необходимым уровнем безопасности в каждом конкретном случае.

Вывод

Технология асимметричного выполнения пользователями – участниками протокола РАКЕ - криптографических преобразований может увеличить стойкость этих протоколов. В данной работе это продемонстрировано на примере протокола Белловина и Меррита. Для других протоколов РАКЕ необходимо предложить свои конкретные способы асимметричного выполнения.

Литература

1. Варфоломеев А.А. Некоторые рекомендации по повышению стойкости шифра с малым размером ключа к методу полного опробования. // Вопросы кибербезопасности. 2015. № 5(13). С. 60-62.
2. Варфоломеев А.А. О некоторых предварительных преобразованиях открытого текста типа «All-Or-Nothing» для усиления стойкости шифра к методу полного опробования. SIBCON 2016. <http://ni.spbstu.ru/wp-content/uploads/2016/05/SibCon-2016-programa.pdf>.
3. Варфоломеев А.А. Об асимметрично выполнимых симметричных криптосистемах (шифрах). РусКрипто 2018.
4. Bellare, S. M.; M. Merritt (May 1992). Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks. Proceedings of the I.E.E.E. Symposium on Research in Security and Privacy. Oakland. p. 72. doi:10.1109/RISP.1992.213269. ISBN 978-0-8186-2825-2.
5. Jareck, S., Krawczyk H., Xu J. (2018). OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks. *Advances in Cryptology. Lecture Notes in Computer Science*. 10822. pp. 456–486. doi:10.1007/978-3-319-78372-7_15. ISBN 978-3-319-78371-0.
6. RFC 8133. The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol. <https://tools.ietf.org/html/rfc8133>
7. Словарь криптографических терминов. / Под ред. Б. А. Погорелова и В. Н. Сачкова. - М.: МЦНМО, 2006. - 94 с.
8. Menezes A., van Oorschot P., Vanstone S., (1997). Handbook of Applied Cryptography, Boca Raton, CRC Press. ISBN 0-8493-8523-7. (Available online)

Strengthening the password authenticated key exchange protocol of bellare and merritt due to the use of asymmetric execution of cryptosystems

Varfolomeev A.A.

Abstract.

Protocols for generating high-entropy cryptographic session keys from long-term low-entropy keys or passwords (PAKE - Password Authenticated Key Exchange) are used to increase the security of information protection in information systems. The paper shows how to increase the security of the PAKE protocols themselves by using the concept of asymmetric execution of cryptosystems proposed by the author (see, for example, at SIBCON 2016, RusCrypto 2018) on the example of the classical protocol of Bellare and Merritt.

Asymmetric execution of cryptosystems implies a deliberate significant increase in the complexity of performing operations for one of the legitimate users (for example, for the server, due to additional transformations of the plaintext, increasing the password by a random value, choosing the mode of the cipher, hiding part of the information necessary for the operation), resulting in significant increasing the complexity of finding the secret keys and for the attacker.

The proposed strengthening of cryptographic protocols is especially relevant in the context of restrictions on the parameters used in the primitives of cryptographic protocol.

Keywords: cryptography, cryptographic protocols, keys, complexity, resilience, EKE protocol, Diffie-Hellman key agreement protocol, SESPake protocol.

Исследование криптовалюты Monero с точки зрения информационной безопасности **Величко И.К.⁴⁵**

В статье приведены результаты исследования криптовалюты Monero, проведён анализ особенностей её работы и транзакций, включая алгоритм, на которых базируется работа криптовалюты, а также угроз, связанных с его применением.

Ключевые слова: Monero, конфиденциальность, пользователь, транзакция.

Введение

В современном мире все большее развитие получают компьютерные и сетевые технологии. Вместе с этим возникает потребность в современных электронных платежных системах. В большинстве случаев интернет-коммерция опирается на доверенных посредников для проведения электронных платежей. В свою очередь необходимость посредничества доверенных финансовых институтов увеличивает стоимость транзакций, что ограничивает их использование. Возникающая потребность в платежной системе, основанной на криптографических алгоритмах, а не на доверии, привела к созданию криптовалют.

Появление криптовалют безусловно носит благоприятный характер, т.к. их использование предоставляет некие преимущества относительно альтернативных средств оплаты, однако вместе с появлением криптовалют также встает вопрос безопасности их использования [1].

Знакомство с криптовалютой Monero и её свойствами

Monero является ведущей криптовалютой с акцентом на частные и устойчивые к цензуре транзакции. Большинство криптовалют, открыто поддающиеся проверке (таких как Bitcoin и Ethereum), позволяют любому человеку в мире отслеживать деньги любого пользователя. Кроме того, связи между финансовыми записями пользователя и его персональными данными может поставить под угрозу его безопасность.

Чтобы избежать этих опасностей, Monero использует мощные криптографические методы, чтобы создать сеть, которая позволяет сторонам взаимодействовать, не раскрывая отправителя, получателя, или суммы транзакций. Как и другие криптовалюты, Monero имеет децентрализованную бухгалтерскую книгу, которую все участники могут скачать и проверить для себя.

Тем не менее, ряд математических трюков используются, чтобы скрыть все щепетильные детали и методы любого отслеживания блокчейна. Пользователи Monero получают все преимущества децентрализованной безотказной финансовой системы без риска для безопасности и конфиденциальности недостаточно понятного блокчейна.

Одной из важнейших определяющих особенностей Monero является принудительная конфиденциальность по умолчанию. Пользователям специально предотвращают инициализации транзакций, которые случайно или намеренно небезопасны. Это обеспечивает пользователям Monero спокойствие, так как сеть не будет принимать раскрывающую сделку [2].

Принципы работы криптовалюты Monero

Monero была создана по следующим принципам работы:

- Децентрализация сети: сеть Monero и её виртуальная бухгалтерская книга являются глобально распределёнными. Это означает, что нет ни одного сервера или базы данных, которые могут быть злонамеренно контролироваться или подвергаться цензуре. Если одно из государств изолировало Monero узлы в своей стране или

⁴⁵ Величко Иван, студент, МГТУ им. Баумана, Москва, ivan_konstantinovich96@mail.ru

попыталось ограничить тех, кто может отправлять или получать Monero, усилия будут напрасны. Остальная часть мира продолжит работать в сети и обрабатывать все достоверные транзакции.

- **Финансовая безопасность:** у глобально распределенной Monero нет центрального слабого места, которое можно взломать, чтобы украсть ваши средства. Moneroj пользователя (расчётная единица криптовалюты Monero) защищены неизменяемыми криптографическими методами, поэтому нет необходимости доверять третьей стороне ответственность за свои средства. Каждый участник Monero может проверить достоверность самой бухгалтерской книги, поэтому пользователю даже не придется доверять оператору узла.
- **Финансовая конфиденциальность:** большинство блокчейн проектов повышают безопасность ценой конфиденциальности, однако Monero уделяет приоритетное внимание именно конфиденциальности пользователя. Суммы транзакций и личности отправителя и получателя обфусцированы на блокчейне, поэтому деятельность пользователя, связанная с хранением и расходованием денежных средств, не отслеживается.
- **Взаимозаменяемость:** термин "взаимозаменяемость" означает, что некоторый тип актива считается заменяемым. В случае Monero, взаимозаменяемость является особенностью её сложной политики конфиденциальности, и относится к тому, чем обфусцированной записи транзакции, тем трудней выяснить историю какого-либо конкретного Moneroj.

Модель транзакций в Monero

Криптовалюта Monero, первоначально известная как BitMonero, была создана в качестве производной от доказательства концепции криптовалюты CryptoNote. В октябре 2013 года под псевдонимом Nicolas van Saberhagen был опубликован знаковый технический документ, описывающий CryptoNote. Он предлагал анонимность получателя за счет использования одноразовых адресов, а неопределенность отправителя – за счет кольцевых подписей [3]. От неё Monero унаследовала много полезных особенностей, самая важная из которых – модель транзакций.

Классические Bitcoin адреса, будучи опубликованными, становятся однозначным идентификатором для входящих платежей, связывая их между собой и привязывая к псевдонимам получателя. Если кто-то хочет получить "развязанную" транзакцию, он должен передать свой адрес отправителю по частному каналу. Если он хочет получать различные транзакции, которые не могут быть доказаны, как принадлежащие одному и тому же владельцу, он должен генерировать все разные адреса и никогда не публиковать их под своим псевдонимом.

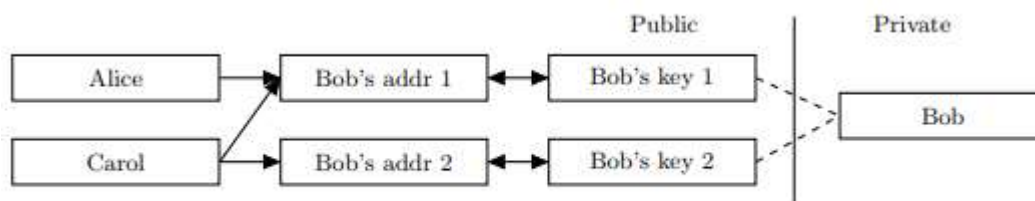


Fig. 2. Traditional Bitcoin keys/transactions model.

Рисунок 1 - Модель ключей/транзакций в Bitcoin

Создатели CryptoNote предложили решение, позволяющее пользователю публиковать один адрес и получать безусловные несвязанные платежи. Назначение каждого вывода CryptoNote (по умолчанию) является открытым ключом, полученным из адреса получателя и случайных данных отправителя. Главное преимущество перед биткойном заключается в том, что каждый ключ назначения уникален по умолчанию (если только

отправитель не использует одни и те же данные для каждой из своих транзакций одному и тому же получателю). Следовательно, нет такой проблемы, как “повторное использование адреса”, и ни один наблюдатель не может определить, были ли какие-либо транзакции отправлены на определенный адрес или связать два адреса вместе.

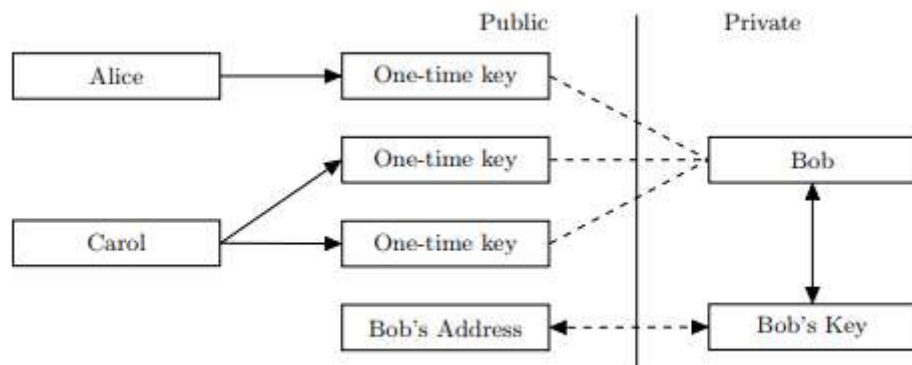


Fig. 3. CryptoNote keys/transactions model.

Рисунок 2 - Модель ключей/транзакций в CryptoNote

Во-первых, отправитель выполняет обмен Диффи-Хеллмана, чтобы получить общий секрет из его данных и половины адреса получателя. Затем он вычисляет одноразовый ключ назначения, используя общий секрет и вторую половину адреса. Для этих двух шагов от получателя требуются два разных ес-ключа (случайно сгенерированный ключ), поэтому стандартный адрес CryptoNote почти в два раза больше, чем адрес биткойн-кошелька. Получатель также выполняет обмен Диффи-Хеллмана для восстановления соответствующего секретного ключа [4].

Стандартный алгоритм транзакции выглядит следующим образом:

1. Алиса хочет отправить платеж Бобу, который опубликовал свой стандартный адрес. Она распаковывает адрес и получает открытый ключ Боба (A, B).
2. Алиса генерирует случайный $r \in [1, l-1]$ и вычисляет одноразовый открытый ключ по следующей формуле:

$$P = H_s(rA)G + B \quad (1)$$

3. Алиса использует P в качестве ключа назначения для вывода, а также упаковывает значение $R = rG$ (как часть обмена Диффи-Хеллмана) где-то в транзакцию. Обратите внимание, что она может создавать другие выходные данные с уникальными открытыми ключами: ключи разных получателей (A_i, B_i) подразумевают разные P_i даже с одним и тем же r .

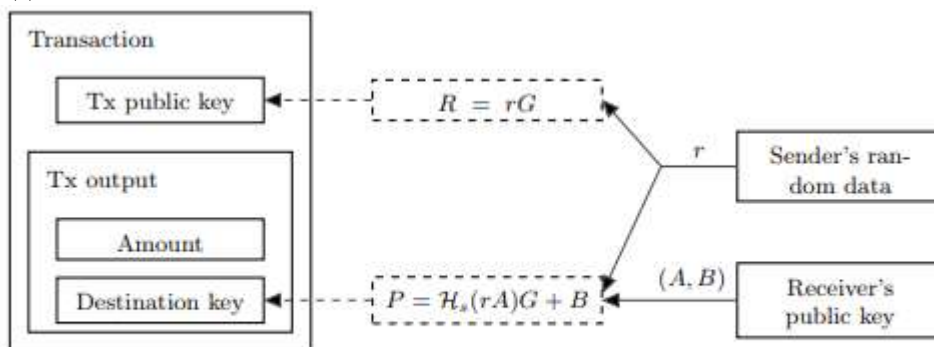


Fig. 4. Standard transaction structure.

Рисунок 3 - Стандартное устройство транзакции

4. Алиса отправляет транзакцию.
5. Боб проверяет каждую проходящую транзакцию с помощью своего закрытого ключа (a, b) и вычисляет одноразовый открытый ключ по следующей формуле:

$$P' = H_s(rA)G + B \quad (2)$$

Если сделка Алисы с Бобом в качестве получателя была среди них, тогда $aR = arG = rA$ и $P' = P$.

6. Боб может восстановить соответствующий одноразовый закрытый ключ по следующей формуле:

$$x = H_s(ra) + b, \quad (3)$$

так как $P = xG$. Он может провести этот вывод в любое время, подписав сделку с x .

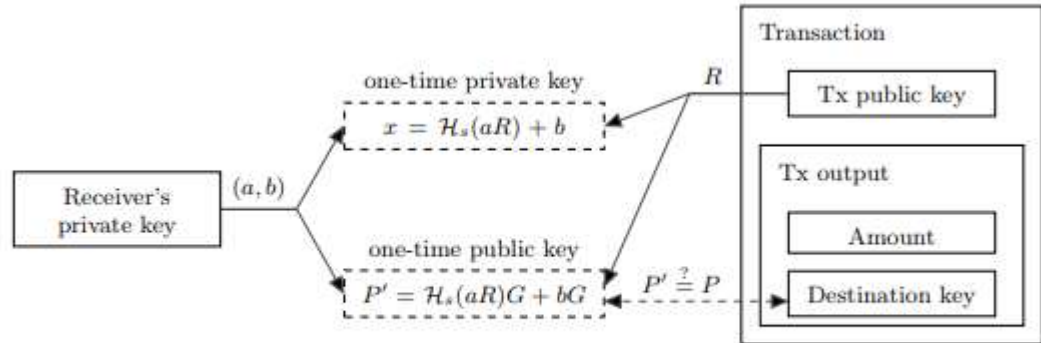


Fig. 5. Incoming transaction check.

Рисунок 4 - Проверка входящей транзакции

В результате Боб получает входящие платежи, связанные с одноразовыми открытыми ключами, которые не могут быть связаны для наблюдателя. Несколько дополнительных примечаний:

- Когда Боб “распознает” свои транзакции (см. шаг 5), он практически использует только половину своей личной информации: (a, B) . Эта пара, также известная как отслеживающий ключ, может быть передана третьей стороне (Кэрл). Боб может поручить ей обработку новых транзакций. Боб не должен явно доверять Кэрл, потому что она не может восстановить одноразовый секретный ключ без полного закрытого ключа Боба (a, b) . Этот подход полезен, когда Бобу не хватает пропускной способности или вычислительной мощности (смартфоны, аппаратные кошельки и т. д.).
- В случае, если Алиса хочет доказать, что она отправила транзакцию на адрес Боба, она может либо раскрыть r , либо использовать любой вид протокола нулевого знания, чтобы доказать, что она знает r (например, подписав транзакцию с r).
- Если Боб хочет иметь совместимый с аудитом адрес, на который можно связать все входящие транзакции, он может опубликовать свой отслеживающий ключ или использовать усеченный адрес. Этот адрес представляет собой только один открытый ес-ключ B , а остальная часть, требуемая протоколом, выводится из него следующим образом: $a = H_s(B)$ и $A = H_s(B)G$. В обоих случаях каждый человек способен “распознать” всю входящую транзакцию Боба, но, конечно же, никто не может потратить вложенные в них средства без секретного ключа b .

Выводы

В статье проведено исследование криптовалюты Мопега, проведён анализ особенностей её работы и транзакций, включая алгоритм, на которых базируется работа криптовалюта, а также угроз, связанных с его применением.

Хоть Мопега и была разработана в качестве производной от доказательства концепции криптовалюты CryptoNote, это не помешало ей вырваться в лидеры криптовалют на мировом рынке. Принудительная конфиденциальность, децентрализация сети, обфусцированные записи транзакций, новая модель транзакции – всё это послужило

тому, что всё больше клиентов выбирают для своих финансовых операций именно Монеро, а не другие, хоть и популярные, криптовалюты.

Литература

1. Захаров Д.Н., Иванов В.Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. 2017. № S2 (20). С. 30-38.
2. Serhack, co-authored by the Monero Community. Mastering Monero. The future of private transactions, 14 с. – Режим доступа: <https://web.getmonero.org/library/Mastering-Monero-Preview.pdf>.
3. Kurt M. Alonso. Zero to Monero: First Edition. A technical guide to a private digital currency; for beginners, amateurs, and experts, 9 с. – Режим доступа: <https://web.getmonero.org/library/Zero-to-Monero-1-0-0.pdf>.
4. Nicolas van Saberhagen. CryptoNote v 2.0 [Электронный ресурс]. – 2013. – Режим доступа: <https://cryptonote.org/whitepaper.pdf>.

Научный руководитель: **Лебедев А.Н.**⁴⁶

Research of Monero cryptocurrency from the point of information security

Velichko I. K.⁴⁷

Abstract. *The article presents the results of the Monero cryptocurrency research, analyzes the features of its operation and transactions, including the algorithm on which the cryptocurrency is based, as well as the threats associated with its application.*

Keywords: *Monero, privacy, user, transaction.*

Principal investigator: **Lebedev A.N.**⁴⁸

⁴⁶ Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lebedevan@bmstu.ru

⁴⁷ Velichko Ivan, student of Bauman Moscow State Technical University, Moscow, ivan_konstantinovich96@mail.ru

⁴⁸ Anatoly Lebedev, Ph.D, Bauman Moscow State Technical University, Moscow, lebedevan@bmstu.ru

Звуковой пользовательский интерфейс обманной системы

Вишневский А.С.⁴⁹, Ключарев П.Г.⁵⁰

Аннотация: В данной статье разработан интерфейс для работы с обманной системой на слух. С помощью звуков закодированы собираемые обманной системой признаки компьютерных атак: вердикт, тип угрозы и точность классификации. Подробные сведения предлагается озвучивать побуквенно, с возможностью перезаписи. Впервые предложено использовать аудиальный интерфейс в приложениях для анализа компьютерных атак, что может снизить зрительную нагрузку для видящих и дать возможность профессиональной работы для инвалидов по зрению.

Ключевые слова: вредоносный код, физическое кодирование, восприятие данных на слух, компьютерные тифлотехнологии.

Введение

Обманные системы – это ловушки для компьютерных атак, собирающие вредоносные объекты для дальнейшего анализа [1]. Большой поток данных вынуждает пользователя обманных систем работать с несколькими мониторами одновременно или часто переключаться между графическими интерфейсами на одном мониторе.

В качестве альтернативы в данной работе предложен звуковой интерфейс, позволяющий перемещаться по структурированному множеству признаков и оценивать на слух вердикт текущего объекта, тип угрозы и точность, с которой они были рассчитаны. Звуковой интерфейс построен на оригинальном методе кодирования признаков компьютерных атак с помощью сочетаний звуков на различных частотах.

Состояние предметной области

Вирусные аналитики находят строки, контрольные суммы, сигнатуры, имена объектов операционной системы и другие признаки, по которым определяют вердикт исследуемого объекта, т.е. наличие или отсутствие вредоносной функциональности в файле, сетевом запросе, электронном письме, на вебсайте т.п. [2].

В научной литературе опубликованы идеи по использованию объемного звука в приложениях для инвалидов по зрению, и упомянуты операционные системы с ограниченным набором прикладного ПО, с которым можно работать на слух, но приложений с аудиальным интерфейсом для специалистов по информационной безопасности нет [3,4,5]. Восполнить дефицит таких инструментов призвана данная работа.

Постановка задачи

Признаком компьютерной атаки будем считать кортеж $\langle u, v, y, z \rangle$, содержащий название потенциально опасного действия $u \in U$, булевый вердикт $v \in Z_2$, название инструмента $y \in Y$, с помощью которого получен признак, и булево значение точности классификации $z \in Z_2$, подразумевающее уверенность или неуверенность в вердикте. Под U и Y подразумеваются списки потенциально опасных действий и инструментов анализа, перечисленные в энциклопедии компьютерных атак ATT&CK от MITRE⁵¹.

⁴⁹ Вишневский Андрей Сергеевич, аспирант, МГТУ им. Баумана, Москва, andrey.s.vishnevsky@gmail.com

⁵⁰ Ключарев Петр Георгиевич, кандидат технических наук, МГТУ им. Баумана, Москва, pk.iu8@yandex.ru

⁵¹ <https://attack.mitre.org>

Требуется так представить множество признаков компьютерных атак, чтобы обеспечить по нему навигацию на слух и аудиальное распознавание вердикта, типа угрозы, атрибутов атаки и рассчитанной точности классификации.

Решение

Все инструменты анализа разделим на репутационные – не требующие наличия исследуемого файла, статические – не требующие запуска файла, динамические – требующие запуска файла в контролируемой среде и гибридные, включающие в себя все предыдущие вида анализа.

Разобьем множество собранных признаков компьютерных атак на четыре списка в зависимости от сложности анализа, к которому относится инструмент у.

$$U = \bigcup_{k \in L_4} U_k, L_4 = \{0,1,2,3\}, \forall u \in U \quad (1)$$

Каждый список разобьем на двенадцать частей и присвоим i -му признаку индекс j равный номеру части, в которой он содержится:

$$j = \left\lfloor \frac{12i}{n} \right\rfloor, j \in \{0,1,2, \dots, 11\}, \quad (2)$$

где n – длина списка признаков.

Пользователь перемещается по списку признаков, нажимая кнопки клавиатуры. Нажатие стрелок вверх (вниз) инкрементирует (декрементирует) номер текущего признака i . Прокрутка списка циклическая, т.е. из последней части переходим в первую. Индекс j инкрементируется при достижении номером текущего признака значения i' , такого что

$$i': \left\lfloor \frac{12i'}{n} \right\rfloor > \left\lfloor \frac{12(i' - 1)}{n} \right\rfloor \quad (3)$$

Навигацию по двенадцатым частям признаков представим в виде циклической группы $(Z_{12}, +)$ относительно операции перехода на двенадцатую часть списка признаков, которая удалена от текущей части на число нажатий клавиши PageDown (PageUp). Учитываются не более 11-ти нажатий за единицу времени. Нажатия PageDown (PageUp) увеличивают (уменьшают) номер просматриваемой части признаков и переводят i в начало другой двенадцатой части списка j' в зависимости от числа нажатий k :

$$\begin{cases} j': (j + k) \bmod 12 \\ i': \left\lfloor \frac{n}{12} \cdot j' \right\rfloor, \end{cases} \quad (4)$$

$$(5)$$

где $j, j', k \in Z_{12}$.

Входной алфавит A для кодирования в звуковом интерфейсе – декартово произведение множеств сложности анализа L_4 , положения в списке N_{12} , вердикта K_2 и точности классификации M_2 .

$$A = L_4 \times N_{12} \times K_2 \times M_2 \quad (6)$$

Выходной алфавит B – множество звуков клавиш фортепиано. Звуковая волна, порождаемая нажатием клавиши фортепиано, описывается суммой гармонических колебаний:

$$x = \sum_{k=1}^n x_{0k} \sin(\omega_k t + \varphi_{0k}), \quad (7)$$

где x_{0k} – амплитуда, ω_k – круговая частота, φ_{0k} – начальная фаза k -го компонента. Субъективное восприятие высоты звука определяется ω_0 – частотой основного тона [9].

Все музыкальные звуки клавиш фортепиано разбиты на октавы и имеют буквенные обозначения: “c” – До, “d” – Ре, “e” – Ми, “f” – Фа, “g” – Соль, “a” – Ля, “b” – Ля-диез, “h” – Си. В контроктаве ноты обозначаются заглавными буквами с нижним индексом 1, в малой октаве – заглавными буквами без индекса, а в октавах с первой по пятую – строчными буквами с верхним индексом, соответствующим номеру октавы. Для обозначения нот, повышенных на полтона, используют суффикс is, а для пониженных – суффикс es [9].

Клавиатура фортепиано содержит восемь полных октав, на границах которых частота основного тона ω_0 удваивается (см. таблицу 1). Каждая октава представлена двенадцатью клавишами с постоянным отношением звуков соседних клавиш равным $\omega_0^i / \omega_0^{i+1} = 2^{1/12}$.

Таблица 1 Шкала частот тона “До” в разных октавах

Тон	C ₂	C ₁	C	c	c ¹	c ²	c ³	c ⁴	c ⁵
ω_0 , Гц	16,35	32,7	65,41	130,81	261,63	523,25	1046,5	2093	4186,01

Опр. Минорным ладом – последовательность из семи звуков одной октавы, таких что отношение частот второго и третьего звуков равно $2^{1/12}$, также как и пятого и шестого, а отношения частот остальных соседних звуков равны $2^{1/6}$. В мажорном ладе $2^{1/12}$ равны отношению частоты третьего звука к четвертому и седьмого к первому следующей октавы.

Опр. Транспонирование на n ступеней — увеличение частоты каждого звука в последовательности звуков в $2^{n/12}$ раз.

$$T_n(x) = x \cdot 2^{n/12} \quad (8)$$

$$T_n(\langle x_1, x_2, \dots, x_m \rangle) = \langle T_n(x_1), T_n(x_2), \dots, T_n(x_m) \rangle, \quad (9)$$

где $\langle x_1, x_2, \dots, x_m \rangle$ – последовательность звуков.

На слух можно определить, к какой октаве и ладу принадлежит последовательность звуков, на сколько ступеней она была транспонирована и завершилась ли она на том же звуке, с которого начиналась [9].

Поскольку удвоение частоты звука при транспонировании на целое число октав субъективно воспринимается как тот же самый звук, звукоряд описывают циклической группой (Z_{12}, T_1) относительно операции транспонирования на одну ступень [10].

Примем в качестве выходного алфавита B декартово произведение множеств октав O_8 , начальных ступеней S_{12} , ладов L_2 и множества завершенных и не завершенных на первоначальном звуке последовательностей P_2 .

$$B = O_8 \times S_{12} \times L_2 \times P_2 \quad (10)$$

Построим изоморфизм $\varphi: A \rightarrow B$. Каждому признаку вредоносного кода u сопоставим минорную звуковую последовательность, а признаку безвредного кода — мажорную. Сложности анализа сопоставим октаву, точности — завершенность последовательности звуков, а положению в списке — первую ступень звуковой последовательности.

$$\varphi(\langle u, v, y, z, \text{position} \rangle) = T_{-12.y} \circ T_{\text{position}}(\text{sound}_{u,v}(z)) \quad (11)$$

Пример закодированного признака компьютерной атаки приведен в таблице 2.

Таблица 2 Признак атаки, закодированный в зависимости от местоположения и типа анализа.

	Гибридный	Динамический	Статический	Репутационный
0	$\langle d, g, \text{fis}, g, d \rangle$	$\langle d^1, g^1, \text{fis}^1, g^1, d^1 \rangle$	$\langle d^2, g^2, \text{fis}^2, g^2, d^2 \rangle$	$\langle d^3, g^3, \text{fis}^3, g^3, d^3 \rangle$
1	$\langle d, g, \text{fis}, g, d \rangle$	$\langle d^1, g^1, \text{fis}^1, g^1, d^1 \rangle$	$\langle d^2, g^2, \text{fis}^2, g^2, d^2 \rangle$	$\langle d^3, g^3, \text{fis}^3, g^3, d^3 \rangle$
2	$\langle e, a, \text{gis}, a, e \rangle$	$\langle e^1, a^1, \text{gis}^1, a^1, e^1 \rangle$	$\langle e^2, a^2, \text{gis}^2, a^2, e^2 \rangle$	$\langle e^3, a^3, \text{gis}^3, a^3, e^3 \rangle$
3	$\langle f, b, a, b, f \rangle$	$\langle f^1, b^1, a^1, b^1, f^1 \rangle$	$\langle f^2, b^2, a^2, b^2, f^2 \rangle$	$\langle f^3, b^3, a^3, b^3, f^3 \rangle$
4	$\langle \text{fis}, h, b, h, \text{fis} \rangle$	$\langle \text{fis}^1, h^1, b^1, h^1, \text{fis}^1 \rangle$	$\langle \text{fis}^2, h^2, b^2, h^2, \text{fis}^2 \rangle$	$\langle \text{fis}^3, h^3, b^3, h^3, \text{fis}^3 \rangle$
5	$\langle g, c^1, h, c^1, g \rangle$	$\langle g^1, c^2, h^1, c^2, g^1 \rangle$	$\langle g^2, c^3, h^2, c^3, g^2 \rangle$	$\langle g^3, c^4, h^3, c^4, g^3 \rangle$
6	$\langle \text{gis}, \text{cis}^1, c^1, \text{cis}^1, \text{gis} \rangle$	$\langle \text{gis}^1, \text{cis}^2, c^2, \text{cis}^2, \text{gis}^1 \rangle$	$\langle \text{gis}^2, \text{cis}^3, c^3, \text{cis}^3, \text{gis}^2 \rangle$	$\langle \text{gis}^3, \text{cis}^4, c^4, \text{cis}^4, \text{gis}^3 \rangle$
7	$\langle \text{gis}, \text{cis}^1, c^1, \text{cis}^1, \text{gis} \rangle$	$\langle \text{gis}^1, \text{cis}^2, c^2, \text{cis}^2, \text{gis}^1 \rangle$	$\langle \text{gis}^2, \text{cis}^3, c^3, \text{cis}^3, \text{gis}^2 \rangle$	$\langle \text{gis}^3, \text{cis}^4, c^4, \text{cis}^4, \text{gis}^3 \rangle$
8	$\langle b, \text{dis}^1, d^1, \text{dis}^1, b \rangle$	$\langle b^1, \text{dis}^2, d^2, \text{dis}^2, b^1 \rangle$	$\langle b^2, \text{dis}^3, d^3, \text{dis}^3, b^2 \rangle$	$\langle b^3, \text{dis}^4, d^4, \text{dis}^4, b^3 \rangle$
9	$\langle h, e^1, \text{dis}^1, e^1, h \rangle$	$\langle h^1, e^2, \text{dis}^2, e^2, h^1 \rangle$	$\langle h^2, e^3, \text{dis}^3, e^3, h^2 \rangle$	$\langle h^3, e^4, \text{dis}^4, e^4, h^3 \rangle$
10	$\langle c^1, f^1, e^1, f^1, c^1 \rangle$	$\langle c^2, f^2, e^2, f^2, c^2 \rangle$	$\langle c^3, f^3, e^3, f^3, c^3 \rangle$	$\langle c^4, f^4, e^4, f^4, c^4 \rangle$
11	$\langle \text{cis}^1, \text{fis}^1, f^1, \text{fis}^1, \text{cis}^1 \rangle$	$\langle \text{cis}^2, \text{fis}^2, f^2, \text{fis}^2, \text{cis}^2 \rangle$	$\langle \text{cis}^3, \text{fis}^3, f^3, \text{fis}^3, \text{cis}^3 \rangle$	$\langle \text{cis}^4, \text{fis}^4, f^4, \text{fis}^4, \text{cis}^4 \rangle$

После прослушивания звуковой последовательности можно запросить словесное пояснение. Если пояснение не содержится в словаре, интерфейс озвучит его по буквам. Любое озвученное по буквам или словарное пояснение пользователь может озвучить самостоятельно, записав свою речь на микрофон.

Выводы

Предложенный метод звукового кодирования сведений о компьютерных атаках позволяет выполнить на слух часть работы вирусного аналитика. Это снижает нагрузку на глаза и открывает возможность профессиональной работы для инвалидов по зрению. В дальнейшем возможна доработка метода кодирования с использованием объемного звучания для отображения большого числа объектов.

Литература

1. Вишневский А.С. Обманная система для выявления хакерских атак, основанная на анализе поведения посетителей веб-сайтов. Вопросы кибербезопасности. Москва, 2018. – С. 54-62. DOI: 10.21681/2311-3456-2018-3-54-62
2. Monnappa K. A. Learning Malware Analysis. Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing, 2018. ISBN 978-1-78839-250-1
3. Frauenberger C., Noisternig M. 3D Audio Interfaces for the Blind. Proceedings of the 2003 International Conference on Auditory Display, Boston, MA, USA, July 6-9, 2003
4. Белоконь М.В. Компьютерные тифлосредства как фактор обеспечения безбарьерной среды для слепых и слабовидящих в высшем инклюзивном образовании. Компьютерные науки и информационные технологии Материалы Международной научной конференции. 2016. С. 63-67.
5. Трунова Л. В., Гречухина И. А. Организация программно-аппаратной системы по сопровождению образовательной деятельности в учреждении профессионального образования для обучающихся с ограниченными возможностями здоровья // Молодой ученый. — 2018. — №24. — С. 324-335.
6. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. Second Edition. Springer Series in Statistics. Springer. 2009
7. Kientzle T. A Programmer's Guide to Sound. Addison-Wesley. 1997. ISBN 5-94074-014-6
8. Сидельников В.М. Теория кодирования.: Учебное пособие. – М.:Физматлит, 2008. – 324 с. ISBN: 978-5-9221-0943-7
9. Кузнецов Л.А. Акустика музыкальных инструментов: Справ.— М.: Легпромбытиздат, 1989. – 389 С. ISBN 5-7088-0166-2.
10. Berry C., Fiore T. Hexatonic Systems and Dual Groups in Mathematical Music Theory. Involve, a Journal of Mathematics. 2016. DOI: 10.2140/involve.2018.11.253

The sound user interface of honeypot Vishnevsky A.S.⁵², Klyucharev P.G.⁵³

Abstract. *This paper proposes an application with audio interface for malicious programs analysis. The sound interface is based on a code, which transforms verdict, class and the accuracy of malicious file to musical pitches. Apparently, for the first time audio interface was proposed for malware analysis.*

Keywords: *malware, line code, the perception of data by ear, applications for people with disabilities.*

⁵² Vishnevsky Andrey Sergeevich, post-graduate student, Bauman Moscow State Technical University, Moscow, andrey.s.vishnevsky@gmail.com

⁵³ Klyucharev P.G., Ph.D., Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

Сравнительный анализ подходов к поиску уязвимостей программного обеспечения методом фаззинг-тестирования

Воронина Е.Н.⁵⁴

В последнее время задача поиска уязвимостей и недеklarированных возможностей в программном обеспечении становится все более актуальной. При решении данной задачи зачастую используется технология фаззинг-тестирования, рассмотрению особенностей которой посвящена настоящая работа. В статье представлена общая схема проведения фаззинга. Кратко описаны основные методы фаззинга, а именно фаззинг на основе грамматики, мутационный фаззинг, фаззинг на основе покрытия кода и фаззинг с применением символьных вычислений. Приведено сравнение этих категорий, по результатам которого выявлена необходимость в разработке нового инструмента фаззинга.

Ключевые слова: информационная безопасность, поиск уязвимостей, фаззинг, тестирование, символьное выполнение, покрытие кода.

Введение

Поиск уязвимостей программного обеспечения (ПО) является одним из важнейших этапов обеспечения информационной безопасности [1]. На практике для анализа исполняемого кода применяются различные подходы, в том числе и технология фаззинга, в основе которой лежит процесс генерации для объекта исследования и отсылки в него намеренно некорректных данных с целью вызвать ситуацию сбоя или ошибку [2].

В настоящее время разработано несколько национальных стандартов (ГОСТ Р 56939-2016, ГОСТ Р 58143-2018), предписывающих проведение фаззинг-тестирования при разработке ПО, что подтверждает значимость этого направления [3].

Основным преимуществом фаззинг-тестирования является его высокая автоматизация по сравнению с другими технологиями проверки, такими как тестирование на проникновение. Часто фаззинг применяется при тестировании методом «черного ящика», т.е. в условиях отсутствия исходных кодов приложения, поскольку это один из немногих методов проверки качества таких приложений. Еще одним преимуществом фаззинга является практически полное отсутствие ложных срабатываний, что нередко встречается при использовании статических анализаторов [4]. Сочетание системного подхода и случайной генерации данных позволяет этому методу находить ошибки, которые пропускались бы при ручном тестировании и отладке.

Схема проведения фаззинга

В этом разделе рассматривается базовая структура системы фаззинга (рис. 1) [5]. Описание предназначения каждого блока приведено после рисунка.

⁵⁴ Воронина Екатерина Николаевна, МГТУ им. Н.Э. Баумана, Москва, voronina-ekaterina@hotmail.com



Рис. 1. Архитектурная схема системы фаззинга

Генератор тестов обычно анализирует и изменяет поданные на вход фаззера (программы, осуществляющей фаззинг) примеры или случайным образом создает входные данные для тестируемого приложения. Сгенерированные данные могут быть файлом определенного типа или потоком сетевых данных.

Модуль доставки принимает образцы из генератора тестов и отправляет их в целевую программу. Модуль доставки тесно связан с характером входных данных целевого приложения; например, модуль доставки системы, которая принимает файлы в качестве входных данных, отличается от модуля доставки, который принимает потоки данных из сети.

Тестируемая программа может быть представлена в бинарном виде с известным исходным кодом или без него, в виде программы для использования файлов или программы сетевого сервиса и т. д.

Когда тестируемая программа дает сбой или сообщает об ошибках при фаззинге, необходимо собрать и проанализировать соответствующую информацию. Эти действия выполняют модуль поиска ошибок и фильтр ошибок соответственно. Некоторые инструменты облегчают обнаружение ошибок и могут также использоваться для записи соответствующей информации об исключениях.

Методы фаззинга

Все фаззеры относятся к одной из двух категорий, отличающихся подходами к генерации входных данных [6]:

- 1) Мутационные фаззеры, которые изменяют существующие образцы данных и создают условия для тестирования;
- 2) Порождающие фаззеры, которые создают условия для тестирования с чистого листа, моделируя необходимый протокол или формат файла.

В свою очередь, эти категории делятся на несколько подклассов. В данной работе рассматриваются 4 метода фаззинга, описание которых приведено далее.

Фаззинг на основе грамматики, или автоматическое порождающее тестирование. Для реализации такого способа требуется предварительно понять и оценить спецификации протокола или определение файла. На основе этих данных создается грамматика – определенный набор правил для построения входных данных. Таким образом разделяются те части пакета или файла, которые должны остаться неизменными и те, которые служат переменными для фаззинга. Затем фаззер проводит динамический анализ этих шаблонов, создает фаззинговые данные и направляет в объект получившийся пакет или файл.

Поскольку тестовые наборы, созданные с помощью таких фаззеров, грамматически верны, они с высокой вероятностью будут верно распознаны тестируемой программой и подойдут для программ со сложной спецификацией входных данных. Одним из недостатков этого подхода является то, что необходимо затратить время для создания грамматики или определения. Также на его возможность применения влияет тот факт, что не на все форматы файлов можно найти документацию, а, следовательно, и составить для них грамматику. Для решения этой проблемы используются методы машинного обучения и вероятностного определения контекстно-зависимой грамматики [7]. Технологию создания грамматики применяют следующие фаззеры: Csmith [8] и Sulley [9].

Фаззинг на основе мутационных алгоритмов. Суть данного метода заключается в следующем: на каждом этапе случайным образом фаззер изменяет входные данные из предыдущих попыток. При этом для старта требуется набор репрезентативных входов (корпус), который будет использоваться для дальнейших мутаций. В качестве корпуса можно взять данные пользователей или существующие тесты. Во время своей работы такой фаззер частично изменяет готовые последовательности (например, переставляя биты и байты), комбинирует и сочетает их вариации и подает в программу. При использовании мутирующих алгоритмов, важно иметь большое количество «образцов», которые фаззер будет изменять и отправлять в тестируемую программу.

Для создания фаззера на основе мутаций требуется только написание специальных алгоритмов мутирования, но входные данные достаточно часто оказываются невалидными и вследствие этого отклоняются на ранней стадии обработки. Например, сигнатуры файлов или байты контрольных сумм должны иметь конкретные значения, что не учитывается алгоритмами мутации. Также вложенные условия в программах не дают таким фаззерам проникнуть в более глубокие части кода. Поэтому они почти всегда генерируют меньшее покрытие кода, чем порождающее тестирование.

В свою очередь, фаззеры на основе мутаций имеют следующие преимущества: быстрота реализации, легкое масштабирование, более широкий спектр программ, на которых их можно применять, по сравнению с алгоритмами на базе грамматики.

Radamsa – один из примеров мутационного фаззинга [10].

Фаззинг на основе покрытия кода. Покрытие кода – это мера, используемая при тестировании программного обеспечения. Она показывает процент исходного кода программы, который был выполнен в процессе тестирования [11]. Техника покрытия кода была одной из первых методик, изобретённых для систематического тестирования программного обеспечения.

Более высокому покрытию кода соответствует больший охват состояний выполнения программы и более тщательное тестирование. Лучшее покрытие приводит к более высокой вероятности обнаружения ошибок. Тем не менее, большинство тестовых образцов охватывают только те же несколько путей, в то время как большая часть кода не может быть достигнута. В результате нецелесообразно достигать высокого охвата только

за счет большого количества генераций тестовых сценариев. Фаззеры на основе покрытия пытаются решить проблему с помощью методов анализа программ, таких, как программная инструментация [12]. Примерами фаззеров на основе покрытия кода являются AFL [13] и Libfuzzer [14].

Фаззинг на основе символьного выполнения. При обычном выполнении программы конкретные данные, подаваемые на вход, обрабатываются в программе и выдаются на выход. В отличие от этого, символьное (или символическое) выполнение позволяет определить зависимость промежуточных и выходных значений переменных от входных в виде формулы. При обычном тестировании программы производится ее многократное выполнение для тестовых наборов из некоторого множества с последующей проверкой результатов. Если используемое число тестов меньше, чем общее число возможных различных входных векторов, некоторые ошибки могут быть не найдены. В отличие от этого, символьное выполнение теоретически позволяет получить зависимость выходных данных от входных за один проход по программе. Поэтому оно может использоваться как мощный инструмент анализа программ в комбинации с другими методами [15]. Результатом символьного выполнения является функция нужного тестового пути (символьная зависимость значений выходных данных от входных) и условие его прохождения. Чтобы получить соответствующее тестовое воздействие, требуется решить задачу удовлетворения ограничений – найти любое значение входных параметров программы, удовлетворяющих заданным ограничениям.

Существенным недостатком данного метода является необходимость решения системы булевых уравнений, что фактически является задачей эквивалентной задаче КНФ-выполнимости, которая в свою очередь по теореме Кука – Левина является NP-полной задачей [16]. На данный момент времени исследования в этой области ведутся в ИСП РАН [17], но предлагаемый проект не завершен и имеет ряд существенных ограничений (например, он не способен анализировать встроенное программное обеспечение, написанное для различных микроконтроллерных архитектур).

В таблице 1 представлено сравнение рассмотренных методов фаззинга.

Таблица 1.

Сравнение различных методов фаззинга

	Фаззинг на основе грамматики	Мутационный фаззинг	Фаззинг на основе покрытия кода	Фаззинг на основе символьных вычислений
Скорость тестирования	Высокая	Высокая	Средняя	Низкая
Вероятность генерации валидных данных	Высокая	Низкая	Высокая	Высокая
Степень покрытия кода	Средняя	Очень низкая	Выше среднего	Очень высокая

	Фаззинг на основе грамматики	Мутационный фаззинг	Фаззинг на основе покрытия кода	Фаззинг на основе символьных вычислений
Возможность проведения тестирования без знания спецификаций входных данных	Отсутствует	Присутствует	Присутствует	Присутствует
Возможность проведения тестирования без предварительной подготовки	Отсутствует	Присутствует, но при этом ухудшается качество тестирования	Присутствует, но при этом ухудшается качество тестирования	Присутствует

Выводы

На данный момент существует множество различных технологий фаззинг-тестирования и реализующего их ПО, обладающего достаточно развитым функционалом. Стандартные технологии фаззинга, такие как мутационное тестирование или тестирование на основе грамматики испытывают сложности в случае необходимости тестирования трудно достигаемых участков кода, что часто обуславливается необходимостью ввода конкретных входных данных. Эту проблему способно решить применение символьного выполнения, но следует помнить, что с увеличением объема программы экспоненциально растет сложность вычислений, что ограничивает «глубину» кода, который можно анализировать таким способом. Таким образом, эти инструменты по отдельности обычно упускают уязвимости, которые лежат в более глубоко расположенных участках кода приложения. Эти соображения можно использовать для объединения нескольких методов анализа, используя их сильные стороны и устраняя их недостатки. Целью дальнейших исследований является разработка фаззера с выборочным символьным выполнением.

Литература

1. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1 (2). С. 36-39.
2. Саттон М., Грин А., Амини П. Fuzzing: исследование уязвимостей методом грубой силы. СПб: Символ плюс, 2009. 560 с.
3. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. - 2015. - № 5 (13). - С. 2-10.
4. Dimastrogiovanni C. Towards Understanding the Value of False Positives in Static Code Analysis / C. Dimastrogiovanni, N. Laranjeiro // 2016 Seventh Latin-American Symposium on Dependable Computing (LADC) Proceedings, 2016, pp. 118-132. DOI: 10.1109/LADC.2016.25.
5. Chen C. A systematic review of fuzzing techniques / C. Chen and others // Computers & Security, 2018, vol. 75, pp. 118-137.
6. Саттон М., Грин А., Амини П. Fuzzing: исследование уязвимостей методом грубой силы. с. 56.
7. Li J. Fuzzing: a survey / J. Li, B. Zhao, C. Zhang // Cybersecurity, 2018, vol. 1 (6). DOI:10.1186/s42400-018-0002-y.
8. Csmith. Режим доступа: <https://embed.cs.utah.edu/csmith/>. (Дата обращения 20.11.2019)
9. Amini P., Portnoy A. Sulley Fuzzing Framework. Режим доступа: <http://www.fuzzing.org/wp-content/SulleyManual.pdf>. (Дата обращения 20.11.2019).

10. Radamsa: a general-purpose fuzzer. Режим доступа: <https://github.com/aoh/radamsa>. (Дата обращения 20.11.2019).
11. Veenendaal E. Standard Glossary of terms used in Software Testing. Version 2.2 / E. Veenendaal // Working Party International Software Testing Qualifications Board Proceedings, 2012. Режим доступа: http://science.df.lu.lv/kaab13/istqb_glossary_of_testing_terms_2.2.pdf. (Дата обращения 20.11.2019).
12. Nethercote N. Dynamic binary analysis and instrumentation / N. Nethercote // University of Cambridge, 2004, 170 -pp. Режим доступа: <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-606.pdf>. (Дата обращения 09.11.2019).
13. AFL: american fuzzy lop - a security-oriented fuzzer. Режим доступа: <https://github.com/google/AFL>. (Дата обращения 20.11.2019).
14. LibFuzzer - a library for coverage-guided fuzz testing. Режим доступа: <https://lvm.org/docs/LibFuzzer.html>. (Дата обращения 20.11.2019).
15. Ломакина Л. Тестирование программных систем на основе компьютерной алгебры / Л.С. Ломакина, А.Н. Вигура // Международный журнал экспериментального образования, № 10-1, 2016, с. 132-134.
16. Cook S.A. The complexity of theorem-proving procedures / S.A. Cook // Proceedings of the third annual ACM symposium on Theory of computing, New York, USA, 1971, pp. 151-158.
17. Инструмент динамического символьного исполнения программ Anxiety. Режим доступа: www.ispras.ru/projects/instrument_dinamicheskogo_simvolnogo_ispolneniya_programm_anxiety/ (Дата обращения 20.11.2019).

Научный руководитель: Марков Алексей Сергеевич, профессор, доктор технических наук, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, a.markov@bmstu.ru.

Comparative analysis of approaches to software vulnerability detection by fuzz testing method **Voronina E.N.**

Recently, the task of searching for vulnerabilities and undeclared features in software has become increasingly important. In solving this problem, fuzzing testing technology is often used; the present work is devoted to the consideration of its features. The article presents a general scheme of fuzzing. The basic methods of fuzzing are described briefly, namely grammar-based fuzzing, mutational fuzzing, code-based fuzzing, and symbolic fuzzing. A comparison of these categories is given, the results of which reveal the need to develop a new fuzzing tool.

Keywords: *information security, vulnerability search, fuzzing, testing, symbolic execution, code coverage.*

**Динамическое изменение структурно-функциональных характеристик
информационной системы в целях снижения эффективности сетевой разведки
Ворончихин И. С.⁵⁵**

***Аннотация:** представлен анализ существующих технических решений, направленных на динамическое изменение структурно-функциональных характеристик информационной системы в целях ограничения эффективности ведения сетевой разведки и последующего деструктивного воздействия злоумышленника. В качестве основных технических решений по защите предлагают динамическое управление структурно-функциональными характеристиками информационной системы. Предлагается сформулировать и выявить ряд основных недостатков уже существующей стратегии защиты и предложить технические решения по их ликвидации. Полученные результаты позволяют выработать рекомендации по использованию динамического изменения параметров структурно-функциональных характеристик систем для будущих исследований в области противодействия сетевой разведке.*

***Ключевые слова:** защита информации, moving target defense, защита перестановкой, распределенные информационные системы, компьютерная атака, маскирование структуры сети.*

Введение

Современные технологии сетевой безопасности в защите информационных систем (далее – ИС) сосредоточены на надежной защите периметра. Межсетевые экраны, прокси-серверы, шлюзы прикладного уровня, а также всевозможные системы обнаружения сетевых вторжений, предназначены для предотвращения, запрета и/или обнаружения доступа злоумышленника к защищаемым информационным ресурсам. Применение этих средств защиты для защиты структуры ИС от сетевой разведки в целях упреждения деструктивных действий злоумышленника не позволяет обеспечить требуемый уровень защищенности. Это обусловлено тем, что структура большинства современных ИС является неизменной на протяжении всего времени их функционирования, что обеспечивает достоверность полученной о них злоумышленником информации по результатам ведения разведки в течение длительного интервала времени, что предоставляет злоумышленнику возможность планирования компьютерной атаки без угрозы компрометации своих действий [1, 2].

Свойства детерминированности и статичности структурно-функциональных характеристик ИС позволяют злоумышленнику в удобное для него время неоднократно выполнять обнаружение и анализ уязвимостей с тщательным последующим их тестированием на проникновение для конкретной цели, пока не будет достигнут конечный результат [3, 4].

Это обусловлено тем, что однородность сетевых конфигураций, их сетевых параметров и настроек, позволяет злоумышленникам легко и с небольшими вычислительными затратами проводить крупномасштабную атаку на десятки, сотни и тысячи сетевых узлов после успешной реализации хотя бы одной угрозы безопасности в одном из однотипных узлов этой ИС.

⁵⁵ Ворончихин Иван Сергеевич, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, 5.00@mail.ru

Анализ существующих средств противодействия сетевой разведке

Для снижения риска реализации данного типа атак предлагается применять ряд дополнительных мер, основанных на информационном сокрытии защищаемых узлов ИС с сохранением базовой сетевой функциональности [5-7].

Одной из перспективных технологий защиты, позволяющей скрывать истинные структурно-функциональные характеристики ИС или их элементов и формировать о них ложное представление у злоумышленника является технология, реализующая принципы динамического изменения параметров структурно-функциональных характеристик систем [8, 9]. Она обеспечивает относительно высокую результативность защиты от несанкционированных воздействий за счет регулярного изменения *IP*-адресов абонентов ИС через равные предварительно заданные интервалы времени [10-14].

Однако можно выделить ряд недостатков данной технологии защиты. В первую очередь – это достаточно узкая область применения, которая обусловлена тем, что изменение *IP*-адресов происходит в рамках одной подсети. Это накладывает ограничение на используемый диапазон перестройки параметров защищаемой ИС и может привести к возможности вычисления злоумышленником алгоритма изменения значений *IP*-адресов и принятию им мер по обходу системы защиты [15].

Также можно отметить относительно низкую результативность защиты, которая связана с изменением значений *IP*-адресов узлов через предварительно заданные и равные значения времени аренды *IP*-адресов абонентов ИС вне зависимости от условий ее функционирования и действий злоумышленника. Это может привести к несвоевременному переводу ИС в заранее определенную конфигурацию, обеспечивающую защиту информации, влекущему за собой пропуск несанкционированного воздействия или ложное срабатывание системы защиты [16, 17].

Еще одним недостатком рассматриваемой технологии динамического изменения параметров структурно-функциональных характеристик систем является ее относительно высокая ресурсоемкость, связанная с увеличением затрачиваемого вычислительного ресурса на регулярное, в том числе необоснованное изменение структурно-функциональных характеристик вне зависимости от наличия в ИС процессов сетевой разведки [18].

Устранение выявленных недостатков достигнуто путем динамического изменения таких структурно-функциональных характеристик ИС, как значение номера сети ИС, значение времени продолжительности аренды *IP*-адресов, значения *IP*-адресов сетевых устройств. Для изменения указанных параметров предлагается использовать следующие функции и математические операции.

В качестве функции выбора значения номера сети ИС и *DHCP*-сервера предлагается использовать последовательность чисел Фибоначчи. Это позволит существенно снизить угрозу вычисления злоумышленником последовательности изменения значения номера вычислительной сети *DHCP*-сервера.

В качестве функции выбора значения времени продолжительности аренды *IP*-адресов сетевых устройств предлагается использовать случайное значение в пределах от 700 до 2592000 секунд. Это необходимо для исключения возможности предугадывания злоумышленником интервалов времени, через которые будет осуществляться изменение структурно-функциональных характеристик ИС.

В качестве функции выбора значения *IP*-адреса сетевого устройства ИС предлагается использовать последовательность чисел Люка. Это позволит исключить возможность вычисления злоумышленником последовательности изменения значений *IP*-адресов сетевых устройств.

Наличие в определенный момент времени сетевой разведки в ИС заранее не известно, однако обеспечивая переход системы в защищенное состояние, мы решаем ресурсную задачу по своевременному переводу компонентов ИС в безопасное состояние (с точки

зрения своевременности выбора новых значений структурно-функциональных характеристик ИС, сохранения сетевого взаимодействия и достоверности получаемой компонентами системы информацией) [19, 20].

Формализованная постановка задачи

Таким образом, чтобы корректно сформулировать ресурсную задачу, можно рассмотреть два состояния ИС, первое – когда система функционирует в условиях сетевой разведки, то есть злоумышленник в настоящий момент времени ведет сетевую разведку, второе – когда ИС функционирует без воздействия злоумышленника. Спрогнозировать момент времени, когда противник начнет вести сетевую разведку мы не можем, поэтому моменты возможных переходов ИС из состояния в состояние неопределенны, случайны и происходят под действием потоков событий, характеризующиеся их интенсивностями, являющимися важной характеристикой потоков событий и характеризующими среднее число событий, приходящееся на единицу времени.

Рассмотрим переход от детерминированной постановки задачи к постановке задачи в условиях неопределенности. Тогда финальную вероятность состояния S_i ИС можно будет интерпретировать как среднее относительное время пребывания ИС в этом состоянии.

Дано: S – информационная система;

MIP – множество входных параметров модели, параметры контроля наличия сторонних соединений, от англ. *Model Input Parameters*,

$$CP \subseteq \{WQ, FIP\}, \quad (1)$$

где $WQ = [0, 1, \dots, 65535]$ – широковещательные запросы сторонних сетевых устройств, $FIP = [IP_1, IP_2, \dots, IP_i]$ – пакеты сообщений несанкционированных пользователей (с ложными IP-адресами);

P_i – множество выходных параметров модели, значения финальных вероятностей состояний системы S ,

$$P_i = \lim_{t \rightarrow \infty} P_i(t), \quad (2)$$

где $i = 1, 2, \dots, h$, причем число состояний конечно и из каждого из них можно за конечное число шагов перейти в любое другое;

Z – множество внутренних параметров модели,

$$Z \subseteq \{S_i, \Lambda_j\}, \quad (3)$$

где $S_i = \{S_1, \dots, S_h\}$, $\Lambda_j = \{\lambda_1, \lambda_2, \dots, \lambda_L\}$ перечень моделируемых состояний системы и интенсивностей потоков событий в ней;

IP – множество параметров условий функционирования, где IP – протоколы транспортного уровня семейства протоколов TCP/IP , поддерживаемые моделируемой системой, условие допустимости,

$$IP \subseteq \{TCP, UDP\}, \quad (4)$$

T – множество параметров условий функционирования, где T – значение время аренды IP-адресов узлов, поддерживаемые моделируемой системой, условие допустимости,

$$T = [700, 701, \dots, 2592000], \quad (5)$$

D – множество параметров условий функционирования, где D – номера подсетей, поддерживаемые моделируемой системой, условие допустимости,

$$D = [1, 2, \dots, z], \quad (6)$$

где z – максимальное количество номеров подсетей

Q – показатель эффективности функционирования ИС,

$$Q = \lim_{t \rightarrow \infty} P_{II}^{CP}(t), P_{II}^{CP}(t) \rightarrow \max, \quad (7)$$

Найти: закономерность изменения множества P_i выходных параметров модели функционирования ИС и множества Q показателей эффективности функционирования ИС от множества CP значений входных параметров, множества Z значений внутренних параметров, множества IP, T, D значений параметров условий функционирования. На значения параметров множеств CP, P_i, Z, IP, T, D наложены условия их допустимости.

Тогда формальная постановка задачи на моделирование ИС:

$$\mu : \langle S, CP, Z, IP, T, D \rangle \rightarrow P_i, Q \mid CP \subseteq \{WS, ACK\}, P_i = \lim_{t \rightarrow \infty} P_i(t), \quad (8)$$

$$IP \subseteq \{TCP, UDP\}, T = [700, 701, \dots, 2592000], D = [1, 2, \dots, z], \quad (9)$$

а формальная постановка задачи для минимизации вероятности простоя сетевой разведки:

$$\langle S, CP, Z, IP, T, D \rangle \rightarrow \max P_{II}^{CP} \mid P_{II}^{CP} \in \{P_i\}, i = 1, 2, \dots, h, \quad (10)$$

Анализ промежуточных итогов показывает, что за счет изменения IP -адресов в рамках задаваемого диапазона подсетей значительно увеличивается продолжительность времени полного сканирования ИС злоумышленником,

Также, за счет изменения IP -адресов в рамках задаваемого диапазона подсетей устранена уязвимость, заключающийся в возможности расчета злоумышленником времени последующего изменения IP -адресов сетевых устройств, что позволяло ему выполнять настройку средств сетевой разведки с опциями, позволяющими запоминать MAC -адреса уже просканированных устройств в ИС.

Применение случайных значений времени аренды IP -адресов увеличивает общую продолжительность времени сканирования ИС злоумышленником (рис.1).

В ходе проведенного исследования получены предварительные результаты сканирования злоумышленником вычислительной сети, состоящей из 350 сетевых узлов (рис. 1). C – момент времени, соответствующий изменению IP -адресов сетевых устройств, B – временные интервалы определения злоумышленником сетевых параметров и выбора ключей запуска средства сетевой разведки, d – период работы $DHCP$ -сервера (раздача IP -адресов устройствам сети). Красный график отображает время полного сканирования злоумышленником вычислительной сети без изменения номера подсети, с изменяющимися IP -адресами через равные промежутки времени, - время сканирования составляет 140 минут.

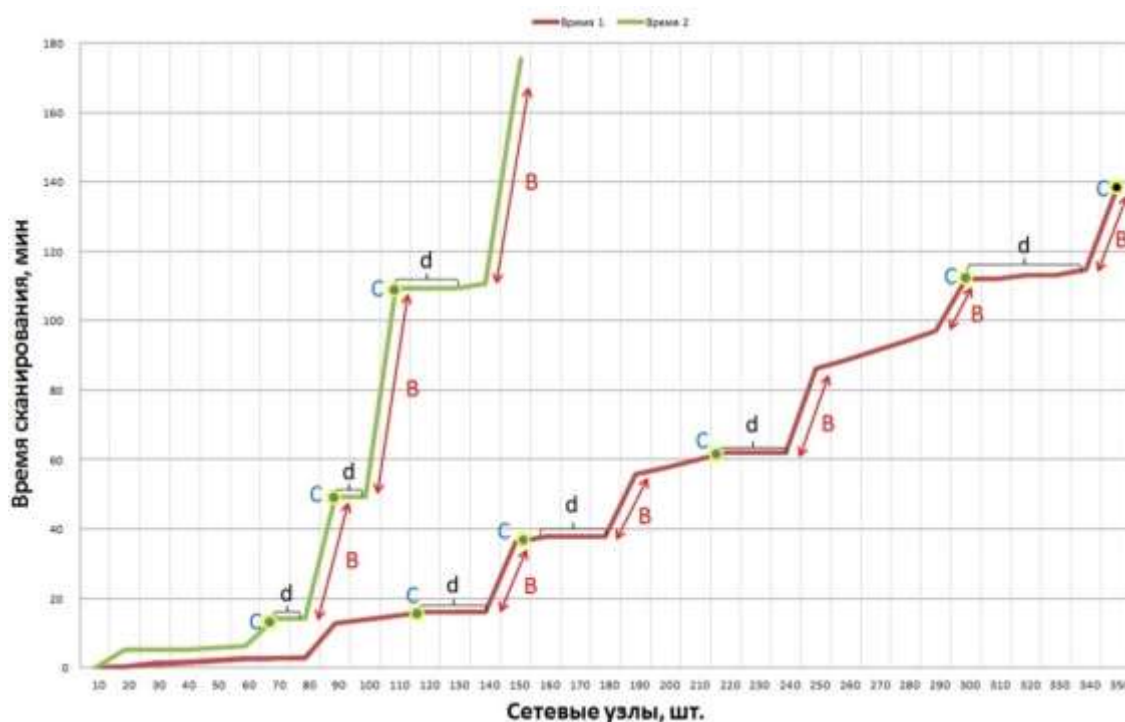


Рис.1. Полученные в ходе выполнения задачи результаты

Зеленый график отображает время полного сканирования злоумышленником вычислительной сети с изменяющимися номерами подсети, значения которых определены последовательностью чисел Фибоначчи, а также, с изменяющимися IP-адресами через случайные промежутки времени, значения которых определены последовательность чисел Люка, - время сканирования в рамках проводимого исследования не определено и составляет более 1440 минут.

Выводы

Внедрение предлагаемых научных решений в структуру ИС позволит обеспечить ослабление влияния или нейтрализацию сетевой разведки злоумышленником за счет снижения доступности элементов ИС и процессов управления, а также лишит злоумышленника необходимой информации о структуре распределенной ИС за счет снижения информативности демаскирующих признаков и процессов управления.

Таким образом, в работе обоснована необходимость динамического конфигурирования непосредственно структурно-функциональных параметров сетевых устройств ИС для повышения уровня ее защиты от сетевой разведки.

Литература

1. Sokolovskiy S. P., Voronchikhin I. S., Telenga A. P. Moving target defense for securing distributed information systems // Информатика: проблемы, методология, технологии. Материалы XIX Международной научно-методической конференции. Под ред. Д.Н. Борисова. 2019. С. 639-643.
2. Ворончихин И.С., Иванов И.И., Максимов Р.В., Соколовский С.П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 92-101. DOI: 10.21681/2311-3456-2019-6-92-101.
3. Соколовский С.П., Ворончихин И.С., Гритчин А.Д. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров. Сборник XXIII Международной научно-практической конференции «Решетневские

- чтения» / под общ. ред. Ю.Ю. Логинова – Красноярск.: СибГУ им. ак. М.Ф. Решетнева, 2019. Том 2. С. 447-448.
4. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Особенности детектирования и способы маскирования демаскирующих признаков средств проактивной защиты вычислительных сетей // Радиолокация, навигация, связь: Сборник трудов XXIV Международной научно-технической конференции. Том 2. – Воронеж: ООО «Вэлборн», 2018. С. 169-179.
 5. Максимов Р.В., Кожевников Д.А., Павловский А.В., Юрьев Д.Ю. Способ выбора безопасного маршрута в сети связи (варианты) // Патент на изобретение RU 2331158, опубл. 10.08.2008, Бюл. № 22, 34 с.
 6. Максимов Р.В., Орехов Д.Н., Соколовский С.П., Барабанов В.В., Ефремов А.А., Ворончихин И.С. // Патент на изобретение RU 2696330, опубл. 01.08.2019, Бюл. № 22, 30 с.
 7. Максимов Р.В., Берест П.А., Богачев К.Г., Выговский Л.С., Игнатенко А.В., Кожевников Д.А., Краснов В.А., Кузнецов В.Е. Способ сравнительной оценки структур информационно-вычислительной сети // Патент на изобретение RU 2408928, опубл. 10.01.2011, Бюл. № 1, 16 с.
 8. Искольный Б.Б., Максимов Р.В., Шарифуллин С.Р. Оценка живучести распределенных информационно-телекоммуникационных сетей // Вопросы кибербезопасности. 2017. № 5 (24). С. 72-82. DOI: 10.21681/2311-3456-2017-5-72-82.
 9. Maximov R., Krupenin A., Sharifullin S., Sokolovsky S. Innovative Development of Tools and Technologies to En-sure the Russian Information Security and Core Protective Guidelines // Voprosy kiberbezopasnosti [Cybersecurity issue], 2019, N 1 (29), pp. 10-17. DOI: 10.21681/2311-3456-2019-1-10-17.
 10. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation “Secure Information Technologies” (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 83-87.
 11. Шерстобитов Р. С., Шарифуллин С. Р., Максимов Р. В. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 136-175. URL: <http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf>.
 12. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation “Secure In-formation Technologies” (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 59-65.
 13. Gavrilov A.L., Maximov R.V., Sokolovsky S.P. Hiding computer network pro-active security tools unmasking features // Selected Papers of the VIII All-Russian Conference with International Participation “Secure In-formation Technologies” (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 88-92.
 14. Максимов Р.В., Соколовский С.П., Чернолес В.П., Шарифуллин С.Р. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. №3 (233). С. 28-35.
 15. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50-99. DOI: 10.24411/2410-9916-2019-10403
 16. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С. 28-35. DOI: 10.21681/2311-3456-2014-1-28-35
 17. Максимов Р.В., Иванов И.И. Этюды технологии маскирования функционально-логической структуры информационных систем / Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции. 11-12 октября 2017 года. – СПб.: ВАС, 2017 – 358 с. С. 147-154.
 18. Максимов Р.В., Иванов И.И. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях / Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции. 11-12 октября 2017 года. – СПб.: ВАС, 2017 – 358 с. С. 138-147.
 19. Соколовский С.П., Волков А.В., Душкин А.В. Устранение интервальной неопределенности при распознавании признаков угроз безопасности информационным телекоммуникационным системам // Системы управления и информационные технологии. 2007. Т.29. № 3. С. 70-73.

20. Соколовский С.П., Бухаров Е.О., Калач А.В., Зыбин Д.Г., Поддержка принятия управленческих решений в сфере информационной безопасности в терминах теории игр // Вестник Воронежского института ФСИИ России. 2018. № 2. С. 46-54.

Научный руководитель: Максимов Роман Викторович, доктор технических наук, профессор, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, rvmaxim@yandex.ru.

Dynamic change of structural and functional characteristics of the information system in order to reduce the effectiveness of network intelligence

Voronchikhin I. S.⁵⁶

Abstract: *the analysis of existing technical solutions aimed at dynamic changes in the structural and functional characteristics of the information system in order to limit the effectiveness of network intelligence and the subsequent destructive impact of the attacker. Dynamic management of structural and functional characteristics of the information system is offered as the main technical solutions for protection. It is proposed to formulate and identify a number of major shortcomings of the existing protection strategy and propose technical solutions to eliminate them. The obtained results make it possible to develop recommendations on the use of dynamic changes in the parameters of structural and functional characteristics of systems for future research in the field of countering network intelligence.*

Keywords: *information protection, moving target defense, permutation protection, distributed information systems, computer attack, network structure masking.*

⁵⁶ Voronchikhin Ivan Sergeevich, Krasnodar higher military school named after army General S. M. Shtemenko, Krasnodar, 5.00@mail.ru

Криптографические операции на устройствах малой производительности

Галимов Ш.У.⁵⁷

В данной работе исследована применимость алгоритмов криптографии для устройств малой производительности. Выполнен обзор и анализ основных криптографических алгоритмов и проведены измерения основных параметров при работе на устройствах малой производительности. Сделан и обоснован выбор критериев оценки эффективности криптографических алгоритмов. Сделан и обоснован выбор криптографических алгоритмов для решения поставленной задачи.

Ключевые слова: микроконтроллеры, *atmel, avr, aes, des, rsa, ecdsa, ram, rom* оценка времени исполнения, криптография, алгоритмы

Введение

В настоящее время восьмиразрядные микроконтроллеры широко используются в различных областях сферы деятельности человека, таких как интеллектуальные бытовые приборы, системы автоматизации производства, RFID-карты, устройства POS (точки продаж), телефоны нового поколения, карманные компьютеры, различные сетевые устройства и автомобили.

Криптография является важным требованием в таких устройствах для безопасной загрузки программного обеспечения в микроконтроллер, для выполнения безопасного обмена сообщениями и для аутентификации пользователя. В таких устройствах личная информация должна быть зашифрована с помощью криптографических алгоритмов таким образом, чтобы воспрепятствовать доступу для злоумышленника к важной информации. В этих областях применения безопасность является одним из наиболее важных вопросов.

Таким образом необходимо знать и использовать методы шифрования, которые могут обеспечить высокую производительность, разумный уровень безопасности и хорошую энергоэффективность, предназначены для удовлетворения требований безопасности восьмибитных микроконтроллеров.

Объектом исследования являются криптографические алгоритмы, реализованные на микроконтроллере малой вычислительной способности и дальнейший анализ полученной информации

Цель исследования – оценка производительности широко распространённых алгоритмов шифрования, таких как AES (Advanced Encryption Standard) с размером ключа в 128 бит, 192 бит и 256 бит[1], DES (Data Encryption Standard)[2], Triple DES[3], RSA (Rivest, Shamir и Adleman)[4], ECDSA (Elliptic Curve Digital Signature Algorithm)[5] на 8-битном микроконтроллере Atmel Atmega1280. Производительность выбранных способов шифрования оценивалась с точки зрения требований к коду и памяти данных занимаемый им, времени выполнения и энергоэффективности.

Общие сведения об архитектуре Atmel Atmega1280 и причина ее выбора в качестве исследуемой платформы

Микроконтроллер Atmel Atmega1280 выполнен по архитектуре AVR. AVR — семейство 8-битных микроконтроллеров, разработанная в 1996 году американской фирмой Atmel и приобретенных компанией Microchip Technology в 2016 году. [5].

AVR представляет собой модифицированную машину архитектуры Гарварда, где программа и данные хранятся в отдельных физических системах памяти, которые

⁵⁷ Галимов Шамиль Уралович, студент ИУ8-31М, МГТУ им. Баумана, Москва, galimovshu@student.bmstu.ru

отображаются в разных адресных пространствах, но имеют возможность считывать данные из памяти программы с помощью специальных инструкций.

Atmega 1280 был выбран в качестве исследуемой платформы ввиду его широкого распространения, дешевизны и общей знакомостью с платформой.

Программные средства для программирования, отладки и моделирования микроконтроллера Atmel Atmega1280

Для написания и отладки программного обеспечения требуемый для выполнения научно-исследовательской работы необходим ряд инструментов такие как:

- редактор кода программы;
- компилятор;
- отладчик кода программы (с помощью симулятора и/или аппаратного отладчика);
- интерфейсы аппаратных отладочных средств (эмуляторы, программаторы, отладчики).

Для ускорения процесса создания программного обеспечения также могут использоваться мастера автоматической генерации кода программы, библиотеки функций и другое вспомогательное ПО.

Для исключения возможности написания неоптимизированного кода для криптографических алгоритмов были использованы ряд специальных криптографических библиотек.

Конечный список использованного ПО:

- ISIS Proteus — пакет программ для автоматизированного проектирования (САПР) электронных схем необходимая для синтеза и моделирования непосредственно электронных схем[6].

- Atmel Studio — основанная на Visual Studio бесплатная проприетарная интегрированная среда разработки (IDE) для разработки приложений для 8- и 32-битных микроконтроллеров семейства AVR и 32-битных микроконтроллеров семейства ARM от компании Atmel. Так же Atmel Studio содержит компилятор GNU C/C++ , позволяющий без особых сложностей написать программу для микроконтроллера[7].

- WinAVR — программный пакет, включающий в себя кросс-компилятор и инструменты разработки для микроконтроллеров серий AVR и AVR32 фирмы Atmel [8].

Используемые криптобиблиотеки:

- Relic-toolkit криптографическая библиотека для создания эффективных криптографических алгоритмов, адаптированных для микроконтроллеров архитектуры AVR возможность выбора конкретных уровней безопасности и алгоритмов [9].

- Crypto-avr-lib – библиотека с набором реализаций различных криптографических алгоритмов. Из-за особых ограничений микроконтроллеров (очень мало места, ОЗУ и флэш-память варьируются от нескольких байтов до нескольких КБ), имеющая в своем составе эталонные и оптимизированные специальные реализации, которые учитывают крайне ограниченные ресурсы приложений микроконтроллеров [10].

- Micro-ECC – небольшая криптобиблиотека имеющая оптимизированную реализацию ECDH и ECDSA для 8-битных, 32-битных и 64-битных процессоров [11].

При написании кода использовалась одинаковая схема построения программ, что позволит в дальнейшем сравнивать и анализировать полученных результатов. Структурная схема представлена на рисунке 1.



Рисунок 2 – Структурная схема программы для замеров параметров работы криптографических алгоритмов на микроконтроллере

Методика измерения интересующих параметров при работе алгоритмов на микроконтроллере

Для проведения сравнительных измерений работы алгоритмов были выбраны следующие параметры: используемый объем памяти программ (ROM), используемый объем памяти данных (RAM), а также время выполнения шифрования и расшифрования.

Для оценки времени выполнения и энергопотребления параметры были установлены следующим образом: напряжение питания-5В, тактовая частота процессора-16 МГц (максимально доступная реальному микроконтроллеру).

Одним из выбранных для измерения параметров является память программ, необходимая для функционирования программ. Вычисления с помощью специальных операций, реализованных в криптографических библиотеках, а также большие числа, используемые в асимметричных криптографических алгоритмах, увеличивают

потребление этого дефицитного для микроконтроллеров ресурса, вследствие чего необходимо внимательно следить за ее использованием.

Оценка использования памяти программ (ROM) Память является одним из наиболее дефицитных ресурсов микроконтроллеров, основанных на архитектуре AVR, поэтому при создании программ для микроконтроллеров необходимо строго отслеживать потребление памяти. Применяемые при вычислениях в криптоалгоритмах большие числа обрабатываются при помощи специальных операций, реализованных в составе криптобиблиотек. Специальные вычислительные операции и большие числа значительно увеличивают размер приложений. Оценку использования памяти программ осуществлялся с помощью IDE Atmel Studio при компиляции готового приложения.

Следующим выбранным параметром является память данных (RAM), также необходимая для функционирования программ.

Самый дефицитный ресурс для микроконтроллера — память данных. В микроконтроллере Atmel ATmega1280, являющемся достаточно мощным для микроконтроллеров данной архитектуры, присутствует всего 8 КБ памяти данных, что вносит дополнительные ограничения на использование криптоалгоритмов.

Оценку использования памяти данных также осуществляет при компиляции IDE Atmel Studio. Однако это не самое точное средство измерения, так как компилятор вычисляет только «гарантированное» потребление памяти данных, так как при работе данное значение может существенно увеличиться. Для контроля данного недостатка при проведении измерений использования памяти данных в приложение была интегрирована функция `check_mem()`, определяющая положение высшей точки, занимаемой динамическими данными в памяти данных (`heapptr`), и положение указателя стека (`stackptr`).

Так же измеряемым параметром является время выполнения программы. Чем меньше оно будет, тем больший поток данных можно зашифровывать и передавать с ее помощью.

В силу отсутствия на микроконтроллере операционной системы, автоматизированная возможность оценить время исполнения отсутствует даже в виде сторонней библиотеки. Для оценки времени исполнения в приложение были включены простейшие средства — изменение состояния одного из портов ввода/вывода, переключённого в режим работы на вывод. Состояние порта изменялось перед стартом исполнения участка кода, требующего оценки времени его исполнения, а также после. Разница между точками остановки является временем исполнения участка кода. Изменение состояния порта интерпретируется одной двухбайтовой командой на ассемблере, поэтому на оценки работы алгоритмов переключение состояния порта повлияло в крайне малой степени. Для своевременной паузы исполнения программы был использован встроенный инструмент ISIS Proteus, реализованный в окне Watch Window под названием Watchpoint Condition.

Все результаты проведенных измерений представлены в таблице 2

Таблица 2. Результаты всех проведенных измерений.

Алгоритм	ROM (Байт)	RAM (Байт)	Время шифрования (Секунды)	Время расшифровки (Секунды)
AES-128 Speed	2 424	52	0.000243313	0.000375938
AES-128 Code	1 216	57	0.000500813	0.000658688
AES-192 Speed	2 800	82	0.000346875	0.000536188
AES-192 Code	1 320	86	0.000706	0.000962
AES-256 Speed	2 742	68	0.000347	0.000534875
AES-256 Code	1 310	72	0.000732375	0.000955813

DES	1 748	52	0.000657375	0.000655813
TDES-2K	1 748	60	0.001972938	0.001971375
TDES-3K	1 748	60	0.001972938	0.001971625
RSA ($e=2^{16}+1$)	4 488	770	0.96875	1.41825
CRT RSA	6264	1 110	13.4375	19.6725
RSA-OAEP ($e=2^{16}+1$)	9680	1 334	0.9875	1.4457
RSA-OAEP CRT	10278	1 674	13.625	19.947
RSA-PSS ($e=2^{16}+1$)	12934	1 486	0.9875	1.4457
RSA-PSS CRT	11158	1 638	13.625	19.947
ECDSA-192	14426	918	5.375	10.8125
ECDSA-224	14426	1 020	8.3125	16.9375
ECDSA-256	14426	1 122	12.1875	24.875

Для удобства сравнения результатов они представлены в виде гистограммы на рисунках 2, 3, 4 и 5 для ROM, RAM, времени шифровки и времени расшифровки соответственно.

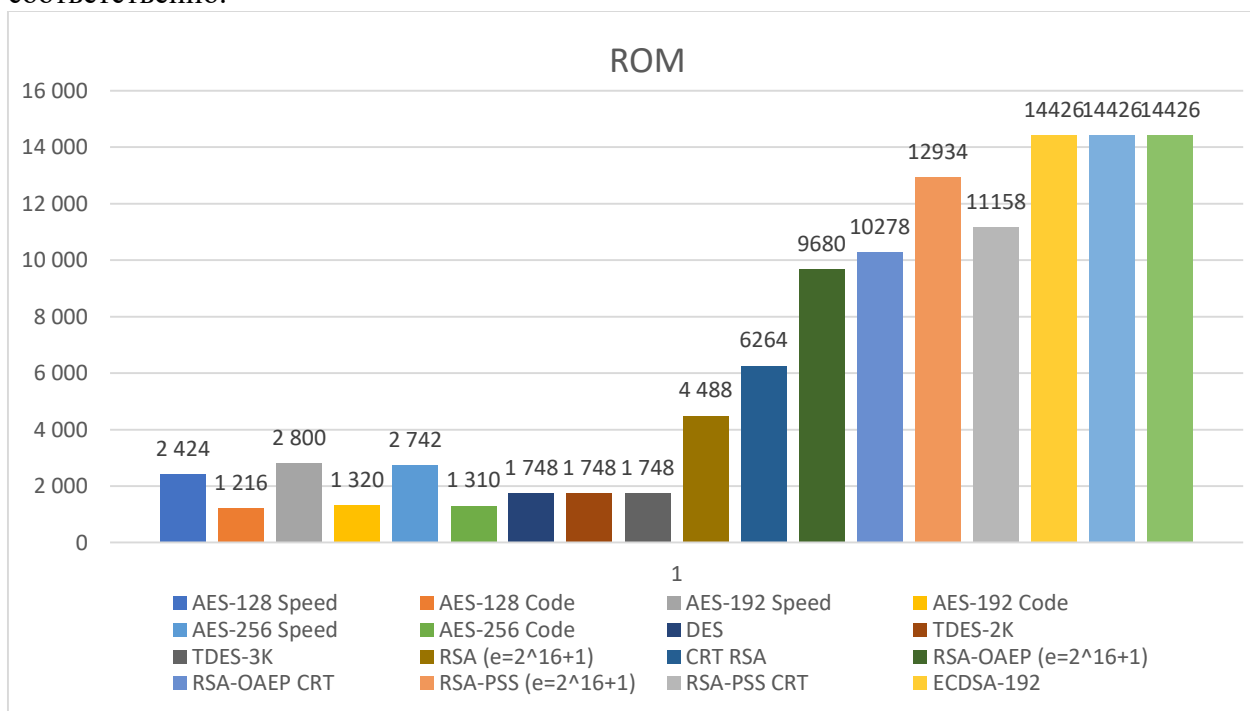


Рисунок 6– Гистограмма используемой ROM памяти для всех используемых видов алгоритмов

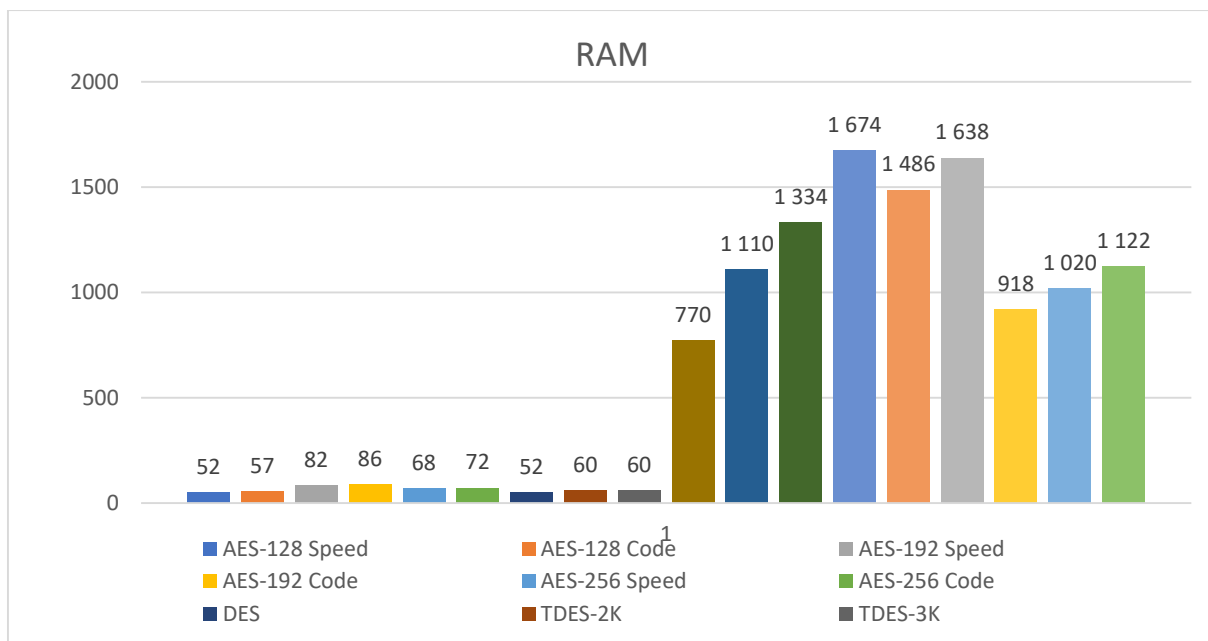


Рисунок 7 – Гистограмма используемой RAM памяти для всех используемых видов алгоритмов

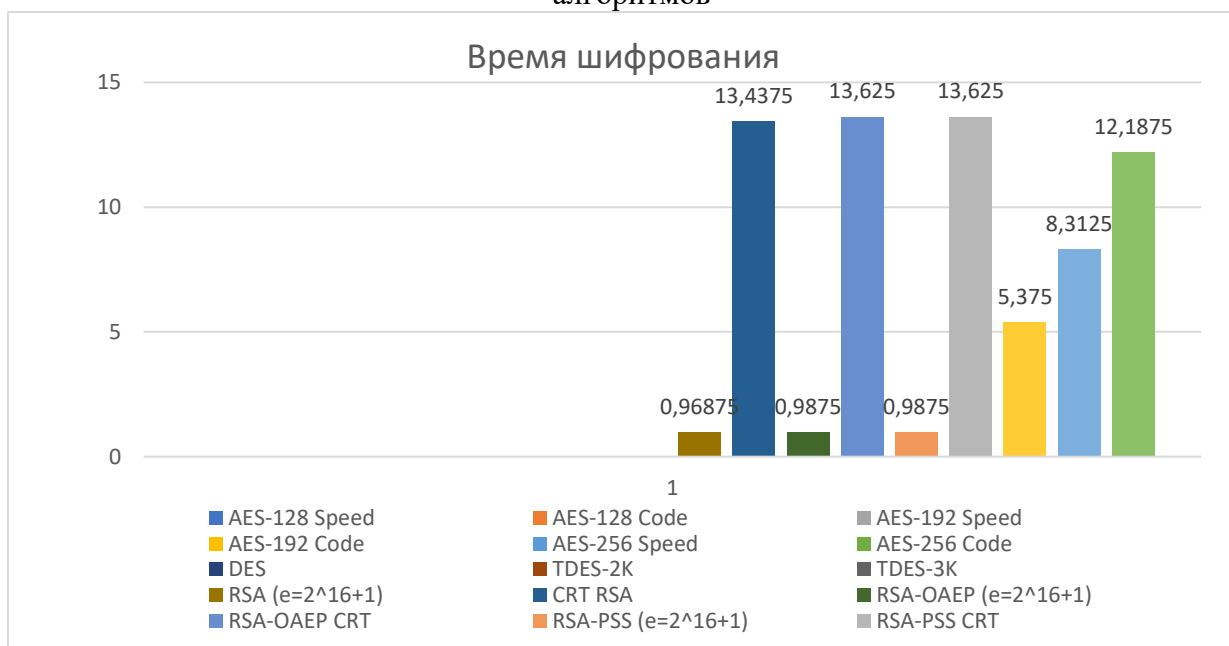


Рисунок 8 – Гистограмма времени необходимого для шифрования для всех используемых видов алгоритмов

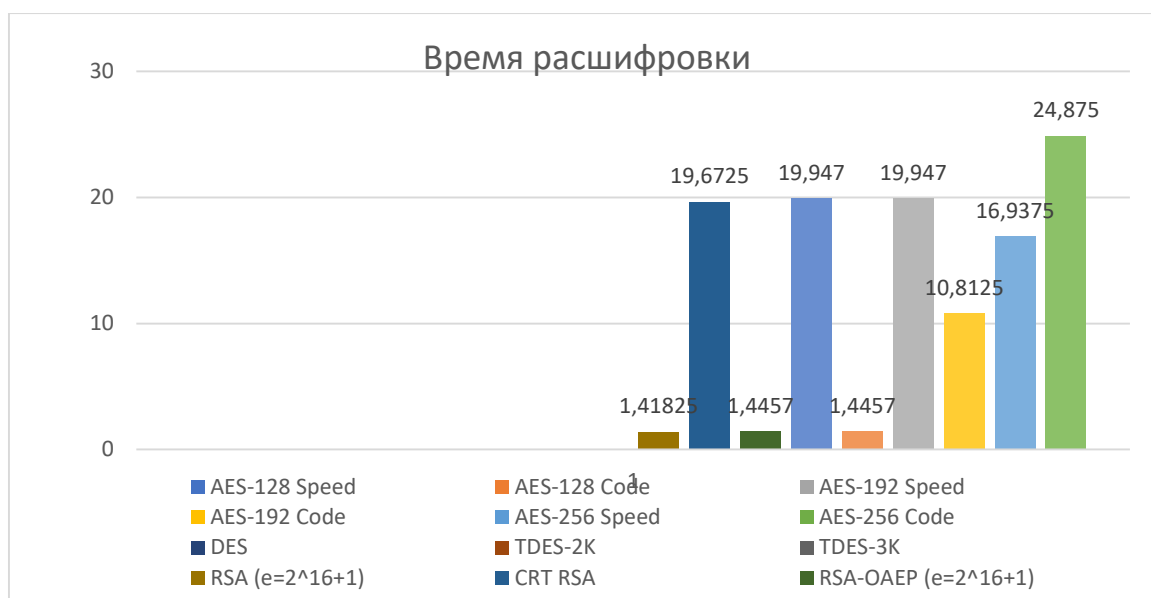


Рисунок 9 – Гистограмма времени необходимого для расшифровки для всех используемых видов алгоритмов

Вывод

В данной работе исследована применимость алгоритмов криптографии для устройств малой производительности. Выполнен обзор и анализ основных криптографических алгоритмов и проведены измерения основных параметров при работе на устройствах малой производительности. Сделан и обоснован выбор критериев оценки эффективности криптографических алгоритмов. Сделан и обоснован выбор криптографических алгоритмов для решения поставленной задачи. На основе проделанной работы можно сделать выводы об оптимальном использовании различных криптографических алгоритмов и их параметров для определённых задач, и целей.

Литература

1. Алгоритм AES [Электронный ресурс] // Лекции ИТЭФ-МФТИ: [сайт]. [2019]. URL: <http://book.itep.ru/6/aes.htm> (дата обращения: 17.04.2019).
2. Алгоритм DES [Электронный ресурс] // Лекции ИТЭФ-МФТИ: [сайт]. [2019]. URL: http://book.itep.ru/6/des_641.htm (дата обращения: 17.04.2019).
3. Алгоритм RSA [Электронный ресурс] // Лекции ИТЭФ-МФТИ: [сайт]. [2019]. URL: http://book.itep.ru/6/rsa_642.htm (дата обращения: 17.04.2019).
4. Алгоритм ECDSA [Электронный ресурс] // ru.wikipedia.org: [сайт]. [2019]. URL: <https://ru.wikipedia.org/wiki/ECDSA> (дата обращения: 17.04.2019).
5. Datasheet ATMEGA1280 [Электронный ресурс] // Microchip Technology: [сайт]. [2019] URL: <http://www.microchip.com/devices/ATMEGA1280.pdf> (дата обращения: 06.05.2019).
6. Webpage Proteus VSM Simulation [Электронный ресурс] // PCB Design and Circuit Simulator Software-Proteus: [сайт]. [2019]. URL: <https://www.labcenter.com/> (дата обращения: 17.04.2019).
7. Atmel Studio IDE [Электронный ресурс] // Atmel Studio: [сайт]. [2019]. URL: <https://www.microchip.com/mplab/avr-support/atmel-studio-7> (дата обращения: 17.04.2019).
8. Winavr IDE [Электронный ресурс] // Сайт ПАЯЛЬНИК 'cxem.net': [сайт]. [2019]. URL: <http://cxem.net/software/winavr.php> (дата обращения: 17.04.2019).
9. Криптобиблиотека Relic-toolkit [Электронный ресурс] // Github.com: [сайт]. [2019]. URL: <https://github.com/relic-toolkit> (дата обращения: 17.04.2019).

10. Криптобиблиотека Crypto-lib-avr [Электронный ресурс] // Github.com: [сайт]. [2019]. URL: <https://github.com/cantora/avr-crypto-lib> (дата обращения: 17.04.2019).

11. Криптобиблиотека Micro-Есс [Электронный ресурс] // Github.com: [сайт]. [2019]. URL: <https://github.com/kmackay/micro-ess> (дата обращения: 17.04.2019).

Научный руководитель: Лебедев, Анатолий Николаевич, к.ф.-м.н., с.н.с., доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, lebedevan@bmstu.ru

Cryptographic operations on low-performance devices Galimov.Sh.U.

In this paper, the applicability of cryptography algorithms for low-performance devices is investigated. A review and analysis of the main cryptographic algorithms is carried out and the main parameters are measured when working on low-performance devices. The choice of criteria for evaluating the effectiveness of cryptographic algorithms is made and justified. The choice of cryptographic algorithms for solving the problem has been made and justified.

Keywords: MICROCONTROLLERS, ATMEL, AVR, AES, DES, RSA, ECDSA, RAM, ROM, Runtime Evaluation, Cryptography, Algorithms

Безопасное обновление операционных систем для мобильных устройств**Глинская Е.В.⁵⁸**

Статья посвящена обеспечению безопасности при установке новых версий операционных сред, а также их безопасному обновлению для гаджетов с различной архитектурой, построенных на современной элементной базе, обеспечению доверенной загрузки современных ARM-процессоров, в которых интегрировано ПЗУ с предзагрузчиком. Определены наиболее незащищенные места при загрузке операционной системы на ARM и предложено применение Secure Boot для обеспечения информационной безопасности и обеспечения доверенности исполнения любой операционной системы на ARM Cortex-A.

Ключевые слова: безопасность, доверенная загрузка, операционная система, гаджеты, загрузчик, предзагрузчик

Введение*Разновидности ARM-процессоров*

Установка новых версий операционных сред и систем (ОС) для портативных и мобильных устройств является актуальной задачей, т.к. именно на этом этапе возможно появление внедрение вредоносного программного обеспечения, если не будет обеспечена доверенная загрузка [1-4, 11].

Рассматривая проблему безопасного обновления ОС для гаджетов, необходимо сначала остановиться на их современной элементной базе, а именно провести краткий обзор линии ARM-процессоров [5, 11].

Архитектура ARM (Advanced RISC Machine — усовершенствованная RISC-машина; Acorn RISC Machine) — семейство лицензируемых 32-битных и 64-битных микропроцессорных ядер разработки компании *ARM Limited*.

В настоящее время при производстве и функционировании популярны микропроцессоры ARM пяти архитектур, а именно: ARMv4, ARMv5, ARMv6, ARMv7 и ARMv8⁵⁹. Компания ARM даёт этим архитектурам коммерческие названия, поэтому ARMv4 называется, например, ARM7, ARMv5 – ARM9, а название Cortex имеют микропроцессоры на архитектурах ARMv6, v7, v8 (см. например, [6, 7]).

К слову, смартфоны используют Cortex-A, а простые кнопочные телефоны - ARM7. Новейшие смартфоны конструируются главным образом на базе ARMv8 (64-битных). В промышленности в различных контроллерах, сетевом оборудовании использовались микропроцессоры класса ARM7 и ARM9, а сейчас в основном внимание переходит на использование в них Cortex-A. Например, для обеспечения безопасности электронных приборов в бытовой технике используются микроконтроллеры Cortex-M.

Устройства ARM делятся на использующие микроконтроллеры и использующие проблемно-ориентированные микропроцессоры (Application Processor, AP). AP - это компонент, как правило, микропроцессорное ядро, используемый в проектировании систем на кристалле.

Для выполнения специфичных программ была сформирована специальная система команд AP. Данная система команд по специализации ядра позволяет решить задачу о согласовании между универсальностью CPU (процессора общего назначения) и высокой производительностью AP(проблемно-ориентированного микропроцессора).

- Микроконтроллеры имеют Flash-память и рабочую ОЗУ на кристалле. Они используются для решения автоматизации проектирования простых изделий.

⁵⁸ Глинская Елена Вячеславовна. Старший преподаватель кафедры «Информационная безопасность» МГТУ имени Н.Э. Баумана, glinskaya-iu8@rambler.ru

⁵⁹ <https://www.aladdin-rd.ru/company/pressroom/articles/zagruzka-os-na-arm>

- Application Processor чаще использует внешнюю память — DDRAM и Flash. Далее в тексте будем обозначать их как микропроцессоры. Область применения у их гораздо выше.

В течении большого периода одинаковые архитектуры ARM7, ARM9 применялись для проектирования микропроцессоров и микроконтроллеров. Но в настоящее время с разработкой и выпуском линейки Cortex для микроконтроллеров используется Cortex-M, а для микропроцессоров Cortex-A и Cortex-R [11].

Виды и варианты загрузки ОС

Малая ОС реальным появлением линейки Cortex произошло разделение, и теперь времени (RTOS) или просто программа без ОС обычно прогоняется на микроконтроллерах. На микропроцессорах чаще запущена ОС общего применения (Linux, Android), иногда RTOS (типа vxWORKS) [8, 9].

Для примера рассмотрим использование ОС в некоторых средствах:

- в планшетах и смартфонах - Android, iOS, Linux;
- в телекоммуникационном оборудовании – Linux, RTOS;
- в бытовом оборудовании – RTOS, программа вообще без ОС.

Далее в тексте речь будет идти только о загрузке ОС (Linux, Android) или RTOS на ARM. По способу загрузки "большие" RTOS сгруппируем с Linux, а "малые" RTOS сгруппируем с программами вообще без ОС.

Для загрузки Linux чаще используют такие микропроцессоры как ARM9, ARM11, Cortex-A. Можно запустить и усечённую версию Linux на ARM7, Cortex-M4 и Cortex-M7, что является не эффективным.

При загрузке малых RTOS применяют устройства ARM7, ARM9, Cortex-M. Иногда для RTOS применяют стартовые модели Cortex-A, такие как, Cortex-A5. Основная часть микропроцессоров Cortex-A является проблемной, реально применение вместе с разработанными поставщиками Linux/Android SDK, это объясняет применение Linux [11].

Загрузчик ОС

Системное ПО вычислителя можно разделить на две компоненты: системный загрузчик и ОС. Главную задачу решает программа, функционирующая при администрировании ОС или RTOS.

Загрузчик выполняет запуск ОС, а также некоторые вспомогательные функции, такие, как:

- исследование целостности ОС при загрузке;
- сервисное обновление программ;
- начальный контроль при первом запуске;
- тестирование.

При применении RTOS программа прогона обычно разрабатывается проектировщиком изделия и представляет собой специализированную программу (рис. 1). При использовании ОС общего применения в основном используются загрузчики с открытым исходным кодом, таким как, u-boot.

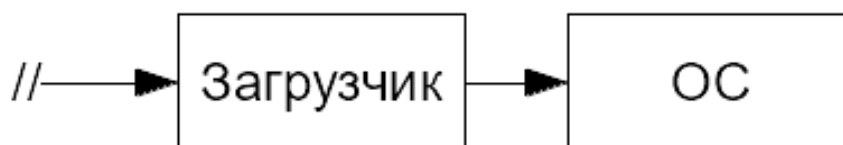


Рис. 1. Запуск ОС с точки зрения разработчика изделия⁶⁰

⁶⁰ <https://habr.com/ru/company/aladdinrd/blog/338806/>

На рисунке 1 две наклонные черты // обозначают точку ввода питания или сброса микропроцессора. Представленный метод прогона использовался ранее в ARM-процессорах⁷. Запуск "Загрузчик-ОС" является практически простым и удобным, при этом функции загрузчика таковы:

- инициализация памяти перед запуском ОС и загрузка ядра ОС в память;
- инициализация периферийных устройств;
- хранение текущего и резервного образов ОС или образа ОС для восстановления;
- контроль перед загрузкой.

Например, для прогона Linux на ARM загрузчик должен инициализировать память, хотя бы один терминал, загрузить образ ядра и Device Tree в память и передать управление на ядро. Код инициализации ядра Linux не будет делать сам то, что должен делать загрузчик [10].

А загрузчик чаще всего даже не предусматривает защиту или же в лучшем случае обеспечивает слабую защиту. В бытовых и домашних роутерах легко самостоятельно открыть крышку, затем существует возможность подключения к разъёму UART. После чего появляется доступ к меню управления загрузчиком. В более сложном оборудовании более высокого класса, например, телекоммуникационном, можно войти в меню загрузчика по недокументированной комбинации клавиш или нажатой кнопке в момент включения устройства. То-есть, часто устройство загрузчика не обеспечивает защиту от локального инсайдера.

В реальности почти никогда не бывает, чтобы команды загрузчика выполнялись первыми после включения или сброса микропроцессора. В современных системах используются другие виды памяти, потому что они дешевле, а объём больше⁶¹. Это NAND, eMMC, SPI/QSPI Flash. Эти типы памяти уже не работают по принципу: подал адрес — читаешь данные, а значит, для прямого исполнения команд из них не подходят. Даже для простого чтения тут требуется написать драйвер, и мы имеем проблему «курицы и яйца»: драйвер нужно откуда-то заранее загрузить.

По этой причине в современные микропроцессоры ARM интегрировано ПЗУ с предзагрузчиком. ПЗУ отображено в памяти микропроцессора на адрес 0, и именно с него начинается исполнение команд микропроцессор.

В задачи предзагрузчика входят следующие:

- определение конфигурации подключённых устройств;
- определение загрузочного носителя (ЗН);
- инициализация устройств и ЗН;
- чтение загрузчика с ЗН;
- передача управления загрузчику.

Конфигурация предзагрузчика обычно устанавливается одним из двух способов:

- схемотехнически, подключением определённых выводов микропроцессора к земле или шине питания;
- записывается в однократно-программируемую память микропроцессора на этапе производства.

В целом почти всегда есть возможность задать единственный вариант загрузки или основной и несколько альтернативных. При этом в числе альтернативных может быть

⁶¹ ARM Architecture Reference Manual. ARM Limited. URL: <http://people.freebsd.org/~chuckr/arm/ARMArchitectureRefMan.pdf>

первичная загрузка через USB или последовательный порт, что очень удобно при первоначальной инициализации на производстве.

Подобный предзагрузчик устанавливается как в микропроцессорах ARM, таких, как Cortex-A, так и в микроконтроллерах, даже таких маленьких, как Cortex-M0. Вместе с предзагрузчиком процедура выполнения ОС представлена на рис.2 [11].

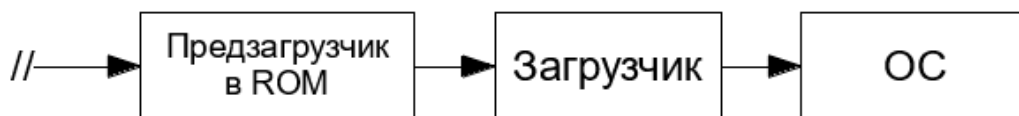


Рис. 2. Процедура выполнения ОС вместе с предзагрузчиком⁶²

Анализ угроз на этапе загрузки

Исходный код предзагрузчика разрабатывается производителем микропроцессора, а не компанией ARM, является частью микросхемы как продукта компании-производителя и защищён авторским правом. Например, в микропроцессорах ARM компаний Atmel и NXP предзагрузчики написаны, соответственно, Atmel и NXP. Можно рассматривать предзагрузчик как вариант BIOS, которого в ARM-системах нет⁶³.

Сам по себе предзагрузчик в ROM несёт в себе угрозу нарушения порядка загрузки и выполнения произвольного кода. Но после того, как управление передано загрузчику ОС, эти угрозы не существенны (рис.3).

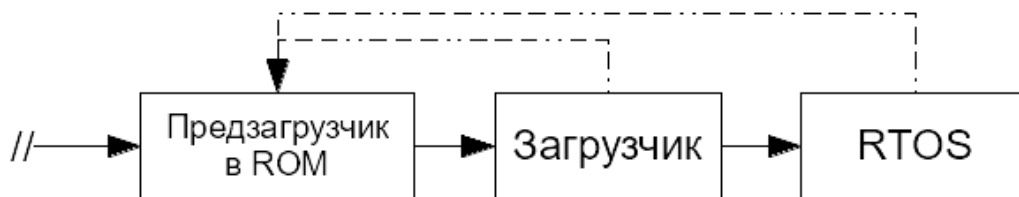


Рис. 3. Передача управления загрузчику ОС с предзагрузчиком⁶⁴

Такая ситуация встречается только в некоторых микроконтроллерах на архитектуре ARM. На таких микроконтроллерах обычно запускаются программы без ОС или малые RTOS, и разработчик системы может оценить риски⁶⁵ [11].

Загрузка с доверенной зоны (TrustZone)

Такие микропроцессоры чаще используются в смартфонах и планшетных компьютерах. Технология TrustZone применяется для проектирования в режиме Secure доверенной "песочницы" для выполнения программы, связанной с криптографической защитой, DRM, хранением пользовательской информации.⁶⁶

В режиме Secure при технологии TrustZone загружается специализированная ОС - TEE (Trusted Execution Environment, доверенная среда исполнения). Простая ОС, например, Linux, Android, iOS, может быть загружена в режиме Non-Secure. В этом случае, права доступа к некоторым устройствам будут ограничены для простой нормальной ОС, называемой также гостевой ОС.

⁶² <https://habr.com/ru/company/aladdinrd/blog/338806/>

⁶³ ARM9 Technical Reference Manual. ARM Limited. URL:

<http://infocenter.arm.com/help/topic/com.arm.doc.ddi0222b/DDI0222.pdf>

⁶⁴ <https://habr.com/ru/company/aladdinrd/blog/338806/>

⁶⁵ https://www.liveinternet.ru/community/rss_rss_hh_full/post422122942/

⁶⁶ <https://habr.com/ru/company/aladdinrd/blog/338806/>

Такой гостевой ОС необходимо в определенное время использовать функции TEE для выполнения проверочных операций.

TEE в настоящее время используется совместно с гостевой ОС во время своей работы, гостевая ОС не может работать без использования функций TEE, таких как: включения и выключения ядер микропроцессора, хранения данных банковских карт и т.п. и ключей шифрования, выполнения криптографической защиты.

Для контроля ситуации в микропроцессоры с поддержкой TrustZone встроен механизм Secure Boot (механизм протокола безопасной загрузки).

С механизмом протокола безопасной загрузки предзагрузчик исследует подпись загружаемого образа с помощью прошитого на этапе производства открытого ключа [6]. Этим гарантируется то, что загружен будет только подписанный образ. В этом состоит функция безопасности.

Рассмотрим схему работы загрузчика фирмы Atmel⁶⁷ для контроллеров с ARM-архитектурой (рис.4).

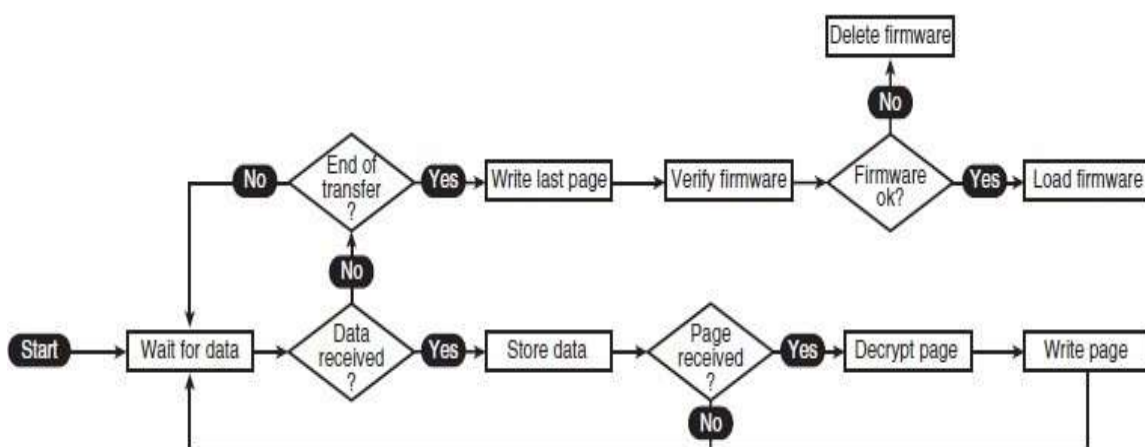


Рис. 4. Схема работы загрузчика фирмы Atmel для контроллеров с ARM-архитектурой

Передача данных в загрузчике осуществляется через порты USB или USART. Образ ОС разбивается на блоки данных и передает их поочередно. При получении каждого блока данных проверяется, корректно ли была произведена передача. Когда все блоки данных переданы, из них собирается образ ОС и проверяется его подлинность. Если проверка пройдена, производится обновление ОС.

Выводы

Загрузчик ОС представляет собой наиболее слабый и уязвимый участок у микропроцессоров линейки ARM в процессе запуска.

Современные микропроцессоры ARM включают в себя TrustZone, поэтому необходима загрузка доверенной среды исполнения TEE перед ОС.

TEE является самой уязвимой точкой в процессе загрузки ОС на ARM Cortex-A, потому что обращения к TEE приводят к исполнению закрытого системного кода, известного только производителю, но скрытого от нас. Без применения Secure Boot невозможно обеспечить безопасность и доверенность исполнения любой ОС на ARM Cortex-A.

⁶⁷ http://www.electronics.ru/files/article_pdf/0/article_603_31.pdf

Литература

1. Горюнов М.Н., Ершов А.Л., Поляков С.А. Подход к сертификации мобильных устройств по требованиям безопасности информации // Вопросы кибербезопасности. 2019. № 2 (30). С. 29-35.
2. Маркин Д.О., Комашинский В.В., Сенотрусов И.А. Методика оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности // Вопросы кибербезопасности. 2017. № 4 (22). С. 21-31.
3. Новиков С.В., Зима В.М., Андрушкевич Д.В. Модель угроз информационной безопасности мобильных персональных устройств // Защита информации. Инсайд. 2014. № 2 (56). С. 60-64.
4. Сидак А.А., Ильин А.В., Кубарев А.В. Мобильные устройства в информационных системах и угрозы безопасности информации. Взаимосвязи // Вопросы кибербезопасности. 2014. № 3 (4). С. 29-34.
5. Хартов В.Я. Микропроцессорные системы. М.: Издательский центр «Академия», 2018. 352 с.
6. Курниц А. Программирование и отладка микроконтроллеров ARM Cortex-m4 фирмы Atmel в среде операционной системы Linux // Компоненты и технологии. 2016. № 2 (175). С. 60-66.
7. Макаров Д.О., Антонов А.С. Использование отладочной платы Stm32f3 Discovery для изучения микроконтроллеров с ядром ARM // Политехнический молодежный журнал. 2018. № 3 (20). С. 8.
8. Варданян Н.Г. Анализ операционных систем реального времени, реализованных в современных системах обеспечения безопасности движения поездов // Труды Ростовского государственного университета путей сообщения. 2018. № 3. С. 8-10.
9. Shen E., Zhang T., Huang L., Liang B., Song J. A Real-Time Simulation System for Satellite Based on Rtw and Vxworks // In: ISSCAA2010 - 3rd International Symposium on Systems and Control in Aeronautics and Astronautics 3rd International Symposium on Systems and Control in Aeronautics and Astronautics, ISSCAA2010. Harbin, 2010. P. 859-864.
10. Fitzpatrick, J. An interview with Steve Furber. // Communications of the ACM. 2017. Т. 54, № 5. С. 34-39.
11. Волков А. Загрузка ОС на ARM. Материалы компании "Аладдин Р.Д.", 2017. URL: <https://www.aladdin-rd.ru/company/pressroom/articles/zagruzka-os-na-arm>

Рецензент: Медведев Н.В., к.т.н., доцент кафедры МГТУ им.Н.Э.Баумана

Secure Update of Operating Systems for Mobile Devices Glinskaya E.V.⁶⁸

The article is devoted to ensuring security when installing new versions of operating systems, as well as safe updating of operating systems for gadgets with various architectures built on a modern element base, ensuring trusted loading of modern ARM processors, in which ROM with a preloader is integrated. The most vulnerable points in the process of loading the OS on ARM were identified and the use of Secure Boot was proposed to ensure the security and power of attorney of any OS on ARM Cortex-A.

Keywords: security, trusted boot, operating system, gadgets, bootloader, preloader

⁶⁸ Elena Glinskaya. Teacher of the Department of "Information Security" MSTU named after N.E. Bauman, glinskaya-ju8@rambler.ru

Подход к обоснованию мер по защите информации в информационно-телекоммуникационных сетях

Гончаров Н.И.⁶⁹

Описан процесс формирования условий обеспечения безопасности информации, циркулирующей в современных информационно-телекоммуникационных сетях. Предложены методики ранжирования и оценки приоритетности условий обеспечения безопасности информации по частным критериям, основанные на применении метода анализа иерархий и морфологического метода. В рамках предложенных методик ранжирования, используются критерии как для обобщённых подсистем условий обеспечения безопасности информации, так и для каждого условия в отдельности. Приведён пример ранжирования условий обеспечения безопасности информации для обоснования выбора защитных мер в конкретной информационно-телекоммуникационной сети.

Ключевые слова: безопасность информационно-телекоммуникационных сетей, меры защиты информации, оценка приоритетности.

Введение

Формирование условий обеспечения безопасности информации (БИ), циркулирующей в информационно-телекоммуникационной сети (ИТКС) [1-7] производится администраторами БИ с учётом технических условий её реализации. При этом, деятельность системных администраторов по созданию таких технических условий во многих случаях предшествует постановке задач защиты информации, что не позволяет определить типовой сценарий обеспечения БИ. Множество возможных сценариев представляет собой комбинации организационных и технических условий обеспечения БИ, которые выбираются для каждого объекта индивидуально.

Для конкретной рассматриваемой информационно-телекоммуникационной сети (ИТКС), или для элементов ИТКС, может существовать множество комбинаций достаточных в соответствии с требованиями действующей нормативной документации условий обеспечения безопасности информации. Такие условия можно классифицировать по группам, и ранжировать по приоритетности для формирования наиболее эффективной комбинации защитных мер.

Целью данной работы является разработка подхода к ранжированию возможных организационных и технических условий обеспечения безопасности информации в информационно-телекоммуникационной сети на основе индивидуальных критериев.

1. Условия обеспечения безопасности информации и критерии их сравнения

Группы условий обеспечения БИ рассматриваются как множество обобщённых подсистем (ОПС), состоящих в свою очередь из элементов подсистем (альтернатив) (рис. 1).

Оценка наиболее и наименее приоритетных условий обеспечения БИ проводится с использованием ряда частных показателей. Во-первых, целесообразно проводить оценку по критериям $C_n^{ОПС}$, относящимся к

⁶⁹ Гончаров Никита Игоревич, АО «НПО «Инфобезопасность», г. Воронеж, manager@infobez.org

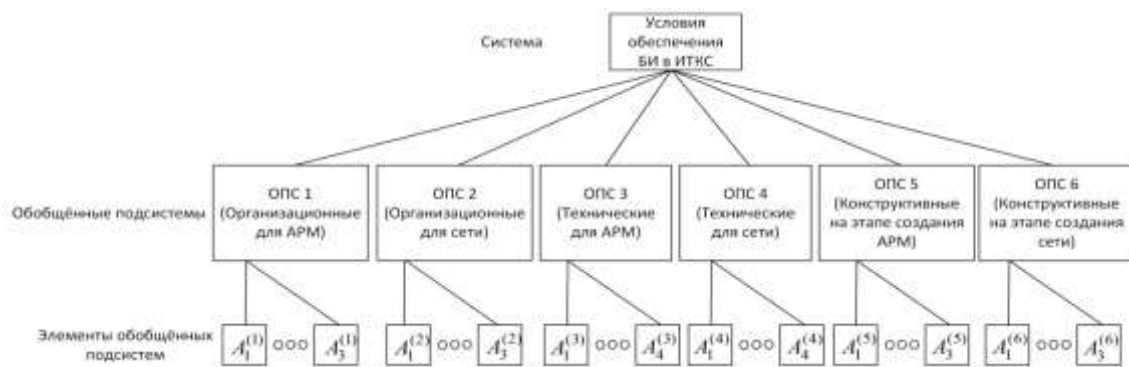


Рис. 1. Декомпозиция условий обеспечения безопасности информации

ОПС в целом. Например: $C_1^{ОПС}$ – экономическая целесообразность применения рассматриваемого типа мер; $C_2^{ОПС}$ – возможность использования необходимых человеческих ресурсов; $C_3^{ОПС}$ – целесообразность выбора рассматриваемого типа мер с точки зрения сложности их реализации в условиях объекта; $C_4^{ОПС}$ – целесообразность выбора рассматриваемого типа мер с точки зрения сложности контроля их выполнения; $C_5^{ОПС}$ – возможность соблюдения экологичности и скрытности при применении рассматриваемого типа мер. Кроме того, при проведении анализа целесообразно рассматривать и критерии, относящиеся к конкретному перечню составляющих элементов рассматриваемой подсистемы, такие как: C_1^A – эффективность меры защиты информации в условиях рассматриваемого объекта; C_2^A – период, в течении которого система защиты информации не потребует обновления (и/или перенастройки); C_3^A – сложность обнаружения и использования уязвимости рассматриваемой меры защиты в случае добросовестного выполнения своих обязанностей администраторами информационной безопасности; C_4^A – сложность обнаружения и использования уязвимости рассматриваемой меры защиты в случае недобросовестного выполнения своих обязанностей администраторами информационной безопасности; C_5^A – обоснованность применения рассматриваемой меры относительно важности защищаемой информации.

Таким образом, в предлагаемом подходе в результате оценки по критериям $C^{ОПС, A} = \{C_1^{ОПС}, \dots, C_n^{ОПС}\}$, $\{C_1^A, \dots, C_n^A\}$, экспертами составляется многоаспектное и комплексное обоснование применимости условий обеспечения безопасности информации на рассматриваемом объекте. В данной работе рассматривается оценка исключительно по качественным показателям, однако, в приведённый аппарат возможно интегрировать и количественные показатели [8-12].

2. Ранжирование условий обеспечения безопасности информации

Для сформированных иерархий определяются векторы приоритетов [8] альтернатив $W_i^A, i = \overline{1, L}$, принадлежащих каждой обобщенной подсистеме, и вектор приоритетов собственно обобщенных подсистем $W^{ОПС}$.

Для выявления вектора $\tilde{x}' = (\tilde{x}'_1, \dots, \tilde{x}'_n)^T$ локальных приоритетов – весов сравниваемых элементов (критериев, альтернатив), а также оценки их согласованности для любой получаемой в ходе опроса матрицы парных сравнений $A' = \|a'_{ij}\|$ используются следующие соотношения:

$$\tilde{x}' = (\tilde{x}'_1, \dots, \tilde{x}'_n)^T, \quad \tilde{x}'_i = \frac{x'_i}{\sum_{k=1}^n x'_k}, \quad x'_i = \sqrt[n]{\prod_{k=1}^n a'_{ik}}, \quad (1)$$

$$\lambda_{\max} = \sum_{i=1}^n y_i, \quad y = (y_1, \dots, y_n)^T = A' \tilde{x}', \quad ИС = \frac{\lambda_{\max} - n}{n-1}, \quad ОС = \frac{ИС}{ИС_r} \cdot 100\%, \quad (2)$$

где $A' = \|a'_{ij}\|$ – исследуемая матрица, $\lambda_{\max}$ – максимальное собственное число матрицы, $ОС$ – отношение согласованности, $ИС$ – индекс согласованности, $ИС_r$ – индекс согласованности, получаемый при усреднении множества данных для матриц парных сравнений различной размерности при случайном равновероятном (то есть полностью не осмысленном) выборе количественных значений суждений из шкалы Саати [8], но с сохранением свойства обратной симметрии.

В рамках описанного подхода, величина ОС считается приемлемой, если она имеет значения порядка 10% и менее (иногда можно допустить в качестве порога значение 20%).

После того, как получены достаточно согласованные оценки на различных уровнях и соответствующие им локальные приоритеты, осуществляется синтез глобальных приоритетов выбора. Для этого по каждой i -ой альтернативе вычисляется величина

$$\Gamma_i = \sum_{k=1}^{n_2} \tilde{x}_k^{(2)} \tilde{x}_i^{(3),k}, \quad (3)$$

где $\tilde{x}_i^{(3),k}$ – компоненты вектора локальных приоритетов $\tilde{x}^{(3),k} = (\tilde{x}_1^{(3),k}, \dots, \tilde{x}_{n_3}^{(3),k})^T$ для i -ой альтернативы третьего (нижнего) уровня относительно k -го критерия верхнего уровня; $\tilde{x}_k^{(2)}$ – компоненты вектора локальных приоритетов $\tilde{x}^{(2)} = (\tilde{x}_1^{(2)}, \dots, \tilde{x}_{n_2}^{(2)})^T$ критериев второго уровня; n_2, n_3 – количество элементов, выделенных в иерархии на втором и третьем уровнях.

При проведении оценок сравниваются все элементы, чтобы сравнения были релевантными. В некоторых задачах при формировании оценок парных суждений следует учитывать совокупное мнение группы независимых участников опроса. В этом случае каждая оценка a_{ij} формируется как геометрическое среднее мнений участников

$$a_{ij} = \sqrt[k]{\prod_{r=1}^k a_{ij}^{(r)}}, \quad (4)$$

где $a_{ij}^{(r)}$ – $r = \overline{1, k}$ – мнения k участников опроса. Такое преобразование данных единственно обеспечивает обратно симметричный характер матрицы парных сравнений.

Таким образом, предлагаемый подход предполагает: 1. Сравнение частных показателей (критериев) и оценку интенсивности (важности) их влияния с точки зрения общей цели анализа ОПС; 2. Сравнение альтернатив и определение для них векторов приоритетов с точки зрения определения их предпочтительности по отдельным показателям; 3. Окончательный расчет векторов приоритетов применительно к элементам ОПС.

При проведении исследования в качестве экспертов использовались специалисты с опытом работы в области технической защиты информации более 10 лет. В результате получены значения векторов приоритетов альтернатив в рамках каждой конкретной ОПС.

Для получения нормированных векторов приоритетов условий обеспечения безопасности информации (рис. 2), производится иерархический синтез по алгоритму, предназначенному для осуществления свёртки в иерархиях с несколькими ветвями, имеющих различное число альтернатив под критериями.

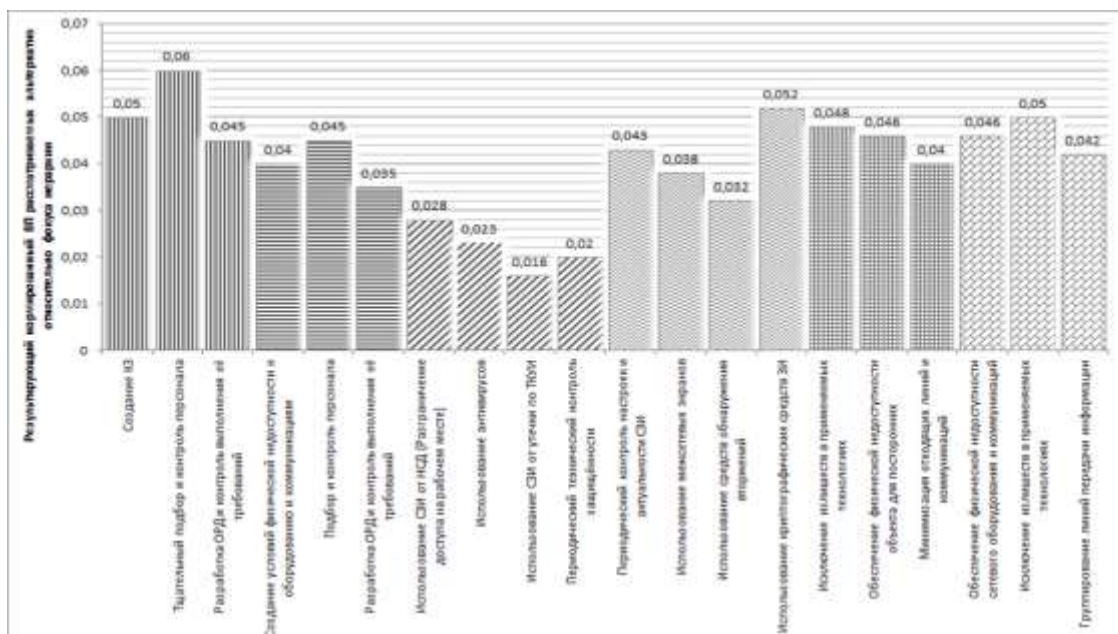


Рис. 2 – Результирующие нормированные векторы приоритетов элементов всех рассматриваемых подсистем относительно фокуса иерархии

Большие значения векторов приоритетов относительно меньших (рис. 2) характеризуют потенциально более предпочтительные условия обеспечения безопасности информации в рассматриваемой ИС.

Таким образом, по результатам проведённого ранжирования условий обеспечения безопасности в рассматриваемой системе на основе выбранных критериев, рассчитано что наименьшим приоритетом обладает условие использования СЗИ от утечки по техническим каналам, а наибольшим тщательный подбор и контроль персонала для предупреждения случаев появления инсайдеров.

Заключение

В работе описан процесс формирования условий обеспечения безопасности информации в современных информационных системах специального назначения.

Обоснован подход к ранжированию и нахождению наиболее и наименее приоритетных условий обеспечения безопасности информации. Подход позволяет проводить обоснование выбора защитных мер на основе оценок экспертов и их математической обработки.

При использовании индивидуальных критериев оценки описанный алгоритм возможно применять как при разработке защищённых ИТКС, так и при обеспечении безопасности информации уже существующих ИТКС.

Достоверность результатов ранжирования достигается вычислением отношения согласованности. Если ОС выходит из заданного предела, то в рамках описанного подхода, следует вернуться к предыдущим этапам структуризации и анализа проблемы в целом или её отдельных составляющих.

Литература

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. - М.: НИЦ «Аналитика», 2008. - 436 с.
2. Кондратьев А.В. Техническая защита информации. Практика работ по оценке основных каналов утечки. – М.: Горячая линия-Телеком, 2016. – 304 с.

3. Гончаров Н. И., Сирота А.А., Гончаров И.В. Анализ защищённости сетевых систем обработки данных по отношению к техническим каналам утечки информации // Специальная техника, 2017. С. 39-44.
4. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. - 192 с.
5. Марков А.С., Матвеев В.А., Фадин А.А., Цирлов В.Л. Эвристический анализ безопасности программного кода // Вестник Московского государственного технического университета им. Н.Э.Баумана. Серия: Приборостроение. 2016. № 1 (106). С. 98-111. DOI: 10.18698/0236-3933-2016-1-98-111.
6. Гончаров Н.И., Смирнов А.С., Пандыклы Н.Р., Душкин А.В. Исследование эффективности мер защиты при выявлении признаков наличия активности вредоносного программного обеспечения // Промышленные АСУ и контроллеры. – 2019. – №1. С. 40-52.
7. Гончаров Н.И., Касаткина Т.И., Россихина Л.В., Душкин А.В., Кузьменко Р.В. Применение технологий нейронных сетей в подсистеме безопасности информационных систем // Приборы и системы: управление, контроль, диагностика. – 2019. – № 1. С. 31-38.
8. Саати Т.Л. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1989. 316 с.
9. Алгазинов Э. К. Анализ и компьютерное моделирование информационных процессов и систем/ Под общ. ред. д.т.н. А. А. Сироты/ А. А. Сирота; М.: Диалог-МИФИ, 2009. 416 с.
10. Андрейчиков А.В. Анализ, синтез, планирование решений в экономике/ Андрейчикова О.В., М.: Финансы и статистика, 2004. 432 с.
- 11.Прядко С.А. Принятие решений с учетом неформализуемых критериев // Вопросы радиоэлектроники. – 2012 № 2. С. 12-19.
- 12.Машкина И.В., Васильев В.И., Рахимов Е.А. Проектирование системы защиты информации объекта информатизации // Информационные технологии. – 2006, №10. С. 12-17.

Научный руководитель: Душкин Александр Викторович, д.т.н., профессор, Национальный исследовательский университет «Московский институт электронной техники», email: a_dushkin@mail.ru.

Approach to the justification of information security measures in information and telecommunication networks

Goncharov N.I.⁷⁰

Abstract. *The article describes the process of forming the conditions for ensuring the security of modern information and telecommunication networks. The methods of ranking and assessing the priority of the conditions for ensuring the security of information according to particular criteria based on the application of the hierarchy analysis method and the morphological method are proposed. An example is given of the ranking of information security conditions to justify the choice of protective measures in a particular information and telecommunication system.*

Keywords: *security of information and telecommunication networks, information security, priority assessment.*

⁷⁰ Goncharov Nikita, JSC “NGO” Infosecurity, Voronezh, email: manager@infobez.org

О числе допустимых решений систем булевых уравнений

Леонтьев В.К.⁷¹, Гордеев Э.Н.⁷²

Многие математические модели, в том числе и в области информационной безопасности, базируются на решении систем булевых уравнений. Решение таких систем или даже ответ на вопрос о существовании допустимого решения – это NP-полная проблема. В связи с этим актуален вопрос о нахождении мощности множества допустимых решений или оценок этой мощности. В работе анализируются комбинаторные аспекты этой проблемы на основе метода производящих функций. Получены формулы и оценки для числа допустимых решений. На их основе могут быть построены вычислительные алгоритмы. Все это может быть использовано для оценки адекватности и качества исходной математической модели.

Ключевые слова: системы булевых, допустимые решения, производящие функции, оценки числа решений, NP-полнота.

Введение

Задача о рюкзаке с булевыми переменными имеет вид:

$$\begin{aligned} \sum_{j=1}^n c_j x_j &\rightarrow \max; \\ \sum_{i=1}^n a_i x_i &\leq b, \end{aligned} \quad (1)$$

где $x=(x_1, \dots, x_n)$ – n -мерный булевский вектор.

Пусть $L(x_1, \dots, x_n)$ – линейная форма:

$$L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i, \quad (2)$$

Где все параметры $\{a_i\}$ и неизвестные $\{x_i\}$ – натуральные числа.

Так, в булевой задаче о ранце переменные полагаются булевыми, а множество допустимых решений должно удовлетворять условию $\sum_{i=1}^n a_i x_i \leq b$, то есть вектора $x=(x_1, \dots, x_n)$ должны

лежать ниже гиперплоскости $L(x_1, \dots, x_n)=b$.

В матричной форме система ограничений имеет вид

$$xA=b, \quad (3)$$

где $A=\|a_{ij}\| - (m, n)$ – матрица.

Это классическая задача комбинаторной оптимизации (см.[1]). Различные ее аспекты, связанные с тематикой данной работы, изучались, например, в [2], [3], [4].

Везде в дальнейшем будем считать, что все параметры рассматриваемой задачи, числа $c_1, \dots, c_n; a_1, \dots, a_n; b$ – неотрицательные целые числа.

Производящие функции для числа допустимых решений

Обозначим через $L^*(a)$ – множество решений уравнения $L(x)=a$, т.е. множество булевых векторов, доставляющих значение a линейной форме $L(x)$.

Таким образом система уравнений $L_i(x)=a_i, i=1, \dots, m$, порождает систему подмножеств $\{L_i^*(a_i)\} = V \subseteq 2^{B^n}$.

⁷¹ Леонтьев Владимир Константинович, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, vkleontiev@yandex.ru.

⁷² Гордеев Эдуард Николаевич, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, tatmigor@gmail.com.

Обозначим через $t_{b_1 \dots b_m}(A)$ -число допустимых решений задачи булева программирования с системой ограничений вида $\mathbf{x}\mathbf{A}=\mathbf{b}$, где $A = \|a_{ij}\| - (m, n)$ - матрица.

Зафиксируем матрицу ограничений и будем варьировать вектор правых частей. Получим последовательность чисел $\{t_{b_1 \dots b_m}(A)\}$. Для этой последовательности построим производящую функцию $F_A(z_1, \dots, z_n)$ в виде полинома

$$F_A(z_1, \dots, z_n) = \sum_{\{b_1, \dots, b_m\}} z_1^{b_1} z_2^{b_2} \dots z_n^{b_m} t_{b_1 \dots b_m}(A).$$

Заметим, что согласно введенным обозначениям, вектор $(a_{1k}, \dots, a_{mk})$ – это k -й столбец матрицы ограничений.

Лемма 1. *Справедлива формула: $F_A(z_1, \dots, z_n) = \prod_{k=1}^n (1 + z_1^{a_{1k}} \dots z_m^{a_{mk}})$.*

Следствие. *Число разрешимых систем булевых уравнений вида $\mathbf{x}\mathbf{A}=\mathbf{b}$ равно числу мономов, входящих с ненулевыми коэффициентами в полином $F_A(z_1, \dots, z_n)$.*

Следствие. *Число разрешимых систем булевых уравнений вида $\mathbf{x}\mathbf{A}=\mathbf{b}$ не превышает степени полинома $F_A(z_1, \dots, z_n)$.*

Оценка числа допустимых решений

Рассмотрим теперь еще одну комбинаторную задачу, которую можно решить с помощью доказанной леммы.

В связи с этим интересны оценки числа $t_{b_1 \dots b_m}(A)$. Следующая теорема дает одну такую оценку.

Теорема 2. *Пусть $v = \sum_{k=1}^n \max_{r=1, \dots, m} a_{rk}$, тогда справедливо неравенство:*

$$\max_{\{b_1, \dots, b_m\}} t_{b_1 \dots b_m}(A) \geq \frac{2^n}{m^v}. \quad (3)$$

Доказательство. С одной стороны, сумма всех коэффициентов полинома $F_A(z_1, \dots, z_n)$ равна $F_A(1, \dots, 1)$, то есть равна 2^n .

Из леммы 1 имеем

$$F_A(z_1, \dots, z_n) = \sum_{\{b_1, \dots, b_m\}} z_1^{b_1} z_2^{b_2} \dots z_n^{b_m} t_{b_1 \dots b_m}(A) = \prod_{k=1}^n (1 + z_1^{a_{1k}} \dots z_m^{a_{mk}}).$$

Поэтому, с другой стороны, можно оценить общее число мономов в $\prod_{k=1}^n (1 + z_1^{a_{1k}} \dots z_m^{a_{mk}})$.

Положим по определению, что степень монома $W = z_1^{v_1} \dots z_m^{v_m}$ равна

$$\deg W = \max_{i=1, \dots, m} v_i.$$

Тогда справедливо неравенство:

$$\deg(W_1 W_2) \leq \deg W_1 + \deg W_2.$$

Теперь имеем сначала равенство:

$$\deg W = \deg(z_1^{a_{1k}} \dots z_m^{a_{mk}}) = \max_{r=1, \dots, m} a_{rk},$$

$$\text{а затем соотношение } \deg\left(\prod_{k=1}^n (1 + z_1^{a_{1k}} \dots z_m^{a_{mk}})\right) = \sum_{k=1}^n \max_{r=1, \dots, m} a_{rk} = v.$$

Отсюда следует, что степень любого монома в не превосходит v . Поэтому общее число мономов не превосходит m^v .

Но это означает, что хотя бы один коэффициент у полинома $F_A(z_1, \dots, z_n)$ не меньше, чем $\frac{2^n}{m^v}$

Теорема доказана.

Конечно, оценка (3) очень слабая и бывает полезна только в специальных случаях. Но так и должно быть, так как проблема проверки разрешимости задачи булева программирования является NP-трудной.

Формулы для числа допустимых решений

Рассмотрим теперь вопрос о числе допустимых решений системы булевых уравнений с несколько иной точки зрения. (Описанный ниже подход основан на методах, изложенных в [5]).

Ответ на вопрос: разрешимо ли хотя бы одно уравнение $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i = b$ в булевых

переменных - все еще NP-полная задача.

Рассмотрим линейную форму (2) с булевыми переменными. Множество значений этой линейной формы обозначим через $L^*(a_1, \dots, a_n)$. (А если это не вызывает неопределенности, то просто через L^*). Сама же форма $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i$ зависящая от переменных $x_1, \dots, x_n$,

будет для краткости обозначаться через L .

Утверждение 1. Уравнение $L(x) = b$ разрешимо тогда и только тогда, когда $b \in L^*$.

Определение. Формы $L_1(x_1, \dots, x_n)$ и $L_2(x_1, \dots, x_n)$ называются эквивалентными, если $L_1^* = L_2^*$.

Утверждение 2. Две формы $L_1(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i$ и $L_2(x_1, \dots, x_n) = \sum_{i=1}^n a_i' x_i$ являются

эквивалентными тогда и только тогда, когда $a_i = a_i', i = 1, \dots, n$.

Пусть, как обычно, n – число переменных, а N – целое число такое, что

$1 \leq a_k \leq N, k = 1, \dots, n$.

Через $t(n, N)$ обозначим число линейных форм с параметрами n и N .

Лемма 2. Справедливо равенство $t(n, N) = C_{N+n-1}^n$.

Лемма 3. Справедливо соотношение

$$t_b(a_1, \dots, a_n) = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{(1+u^{a_1}) \dots (1+u^{a_n})}{u^{b+1}} du, \rho < 1.$$

Следствие. Справедливо соотношение

$$t_b(a_1, \dots, a_n) = t_b(a_2, \dots, a_n) + t_{b-a_1}(a_3, \dots, a_n) + t_{b-a_2}(a_3, \dots, a_n) + t_{b-a_1-a_2}(a_3, \dots, a_n).$$

Рассмотрим теперь вопрос о среднем значении $t_b(a_1, \dots, a_n)$ для фиксированного значения b по всему булеву кубу при условиях (9) и (10). Обозначим это число через $\bar{t}_b$.

Лемма 4. Справедлива формула

$$\bar{t}_b = \frac{1}{C_{n+N-1}^n} \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{\left(N + \frac{u - u^{N+1}}{1-u}\right)^n}{u^{b+1}} du, \rho < 1.$$

Теорема 2. При $N=2$ справедливо соотношение:

$$\bar{t}_b = \frac{1}{n+1} \sum_{k=0}^n C_n^k C_k^{b-k} 2^{n-k}.$$

Пусть теперь $L = \sum_{i=1}^n a_i x_i$ и все $a_i \leq N, i=1, \dots, n$. Обозначим множество таких форм через $L(n, N)$ и пусть $l(n, N) = \max_{L \in L(n, N)} |L^*|$.

Значение $l(n, N)$ и его оценки могут представлять интерес при оценке качества переборных алгоритмов

Теорема 3. *Справедливо соотношение: $l(n, n) \leq n^2$.*

Для доказательства нижней оценки в теореме использовалась линейная форма достаточно специального вида, поэтому на практике, видимо, следует ожидать для $|L^*|$ значений существенно меньших. Вопрос же о среднем значении этой величины – тяжелая задача теории чисел.

Вывод

Метод производящих функций может быть успешно применен для анализа задач, имеющих «комбинаторную» природу. В приведенном исследовании с его помощью получены новые формулы и оценки для числа допустимых решений в задаче булева программирования.

Они могут быть существенно улучшены и уточнены при рассмотрении систем уравнений не общего, а специального вида. Именно такие задачи и возникают в конкретных прикладных областях, в частности в математических моделях информационной безопасности, учитывающих реальные особенности исходных постановок.

Поэтому изложенные здесь результаты могут быть хорошим базисом для дальнейших исследований.

Достоверность результатов следует из корректности определений и доказательств теорем.

Литература

1. Пападимитриу Х., Стайглиц С. Комбинаторная оптимизация. М.: Мир. 1989. 512 с.
2. Горшков С.П., Тарасов А.В. Сложность решения систем булевых уравнений. М.: Курс. 2017. 192с.
3. Леонтьев В.К., Тоноян Г.П. О системах булевых уравнений// ЖВМ и МФ. 2013. №5 (53). С.109-116. DOI:10.7868/S0044466913050098.
4. Леонтьев В.К. Булевы полиномы и линейные преобразования// ДАН. 2009. Т.425. №3. С. 320-322.
5. Леонтьев В.К. Комбинаторика и информация. Часть 1. Комбинаторный анализ. М.: МФТИ, 2015. 174 с.

On the number of solutions of systems of Boolean equations

Leontiev V.K.⁷³, Gordeev E.N.⁷⁴

Abstract. *Many mathematical models, including in the field of information security, are based on solving systems of Boolean equations. Solving such systems, or even answering the question of the existence of a valid solution – is an NP-complete problem. In this regard, the question of finding the power of the set of admissible solutions or estimates of this power is relevant. The paper analyzes combinatorial aspects of this problem on the basis of the method of generating functions. Formulas and estimates for the number of solutions are obtained. Computational algorithms can be built on their basis. All this can be used to assess the adequacy and quality of the mathematical models.*

Keywords: *Boolean systems, admissible solutions, generating functions, estimates of the number of solutions, NP-completeness.*

⁷³ Leontiev Vladimir, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, vkleontiev@yandex.ru.

⁷⁴ Gordeev Eduard, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, tatmigor@gmail.com.

О приближенных «решениях» несовместных систем булевых уравнений

Леонтьев В.К.⁷⁵, Гордеев Э.Н.⁷⁶

Рассматривается система линейных уравнений с булевыми переменными. Нахождение ее решения или даже ответ на вопрос о существовании такого решения – это NP-полная проблема. В работе анализируется два возможных подхода к «решению» несовместных систем таких уравнений. Первый подход можно аргументировать тем, что «значимость» различных уравнений системы не одинакова, а также тем, что достоверность исходной информации о системе разная для различных исходных параметров системы. Второй подход опирается на предположении о возможной декомпозиции исходной системы с возможностью дальнейшего агрегирования решения системы из решений ее подсистем. В этом случае используются различные комбинаторные характеристики системы.

Ключевые слова: диофантовы уравнения, совместные системы, приближенные решения, глубина матриц.

Введение

Линейные диофантовы уравнения и неравенства являются стандартным объектом для различного рода математических моделей, относящихся к целочисленной оптимизации, защите информации, теории чисел, геометрии и т.д.

Классическая задача о ранце с булевыми переменными имеет вид:

$$\sum_{j=1}^n c_j x_j \rightarrow \max ;$$

$$\sum_{i=1}^n a_i x_i \leq b , \quad (1)$$

где $x=(x_1, \dots, x_n)$ – n -мерный булевский вектор.

Пусть $L(x_1, \dots, x_n)$ – линейная форма:

$$L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i , \quad (2)$$

Где все параметры $\{a_i\}$ и неизвестные $\{x_i\}$ – натуральные числа. Накладывая определенные условие на вид этой формы, можно получить разные частные случаи общей задачи.

Так, в булевой задаче о ранце переменные полагаются булевыми, а множество допустимых

решений должно удовлетворять условию $\sum_{i=1}^n a_i x_i \leq b$, то есть вектора $x=(x_1, \dots, x_n)$ должны лежать ниже гиперплоскости $L(x_1, \dots, x_n)=b$.

В матричной форме система ограничений имеет вид

⁷⁵ Леонтьев Владимир Константинович, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, vkleontiev@yandex.ru.

⁷⁶ Гордеев Эдуард Николаевич, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, tatamigor@gmail.com.

$$\mathbf{x}\mathbf{A}=\mathbf{b}, \quad (3)$$

где $A = \|a_{ij}\| - (m, n)$ - матрица.

Накладывая определенные ограничения на матрицу $\mathbf{A}$ и вектор $\mathbf{b}$, получаем различные частные случаи задачи. (См. [1]).

Везде в дальнейшем будем считать, что все параметры рассматриваемой задачи, числа $c_1, \dots, c_n; a_1, \dots, a_n; b$ – неотрицательные целые числа.

Несовместные системы. Преобразование систем.

Рассмотрим систему (3) с произвольными переменными.

При использовании задачи линейного программирования в прикладных моделях реальных систем несовместность системы (3) может иметь следующую интерпретацию.

Уравнения в прикладном понимании неравноценны: одни из них описывают «важные и глобальные» аспекты прикладной проблемы, а другие – «второстепенные», причем связь этих частей не выяснена или ошибочно интерпретирована. Это делает естественным на стадии моделирования применение следующих эвристических подходов:

1. Путем «изменения» вида уравнений или удаление части из них попытаться сделать из несовместной системы совместную.
2. Разбить исходную систему (множество ее уравнений) на некоторое количество (обычно на минимально возможное) совместных систем.

Например, первый подход как выделение (за счет отбрасывания минимально возможного количества уравнений) из системы максимальной по мощности совместной подсистемы рассмотрен в работах [2],[3].

На эту тему имеется значительное число и других публикаций, где полемизируются и обсуждаются различные подходы. Математические результаты, как правило, состоят в приведении и обосновании алгоритмов построения максимальных совместных подсистем.

В прикладном плане подобные работы относятся к различным областям, в первую очередь, видимо, стоит сказать о задачах в сфере распознавания образов (см., например, [4]). В идейном плане примерами подхода являются работы [5], [6].

Другой подход связан со стремлением «минимально» изменить параметры системы для получения из исходной системы совместной. Количественное измерение этой «минимальности» приводит к понятию «меры совместности» системы.

Обозначим через $\mathbf{a}_1, \dots, \mathbf{a}_m$ вектор-строки матрицы $\mathbf{A}$. Вектора $\mathbf{b}$, $\mathbf{a}_1, \dots, \mathbf{a}_m$ назовем параметрами системы (3)

Проблема. Пусть система (3) несовместна. Какое минимальное число параметров системы (3) нужно изменить, чтобы новая система стала совместной?

Пример 1. Уравнение $2x_1 + 3x_2 = 6$ не имеет решения в булевых переменных, но достаточно изменения одного параметра, чтобы сделать его разрешимым. Например, так измененные уравнения: $3x_1 + 3x_2 = 6$ или $2x_1 + 3x_2 = 5$ уже имеют решения в булевых переменных.

Теорема 1. Для того, чтобы сделать несовместную систему линейных уравнений вида (3) совместной при $m > 1$ достаточно изменения $(m-1)$ параметра. Существуют несовместные системы вида (3), для которых изменение этого числа параметров является необходимым.

Доказательство. Пусть дан вектор $c = (c_1, \dots, c_n)$. Рассмотрим несовместную систему

$$\begin{cases} (c, x) = b_1 \\ (c, x) = b_2 \\ \dots \\ (c, x) = b_m \end{cases}$$

Где $b_i \neq b_j$ для всех $i \neq j$. Ясно, что следующая система

$$\begin{cases} (c, x) = b_1 \\ (c, x) = b_1 \\ \dots \\ (c, x) = b_1 \end{cases}$$

Является совместной и получена из исходной путем изменения $m-1$ параметра, причем изменение вектора $c = (c_1, \dots, c_n)$ никак не отражаются на свойстве системы быть совместной. Изменение же меньшего числа параметров не приводит к совместности системы.

С другой стороны, если система

$$\begin{cases} (a_1, x) = b_1 \\ (a_2, x) = b_2 \\ \dots \\ (a_m, x) = b_m \end{cases}$$

является несовместной, то система

$$\begin{cases} (a_1, x) = b_1 \\ (a_2, x) = (a_2, x_0) = b_2 \\ \dots \\ (a_m, x) = (a_m, x_0) = b_m \end{cases}$$

Является совместной при любом x_0 таком, что $(a_1, x_0) = b_1$. И вновь изменения $m-1$ параметра достаточно.

Теорема доказана.

Замечание. В случае одного уравнения в теореме $m-1$ меняется на m , как это видно из вышеприведенного примера с булевым уравнением.

Несовместные системы. Разбиение на подсистемы.

Пусть система (3) несовместна. Требуется разбить ее на совокупность совместных подсистем, решениями которых являются вектора $u_1, u_2, \dots, u_r$.

Определение. Множество $\{u_1, u_2, \dots, u_r\}$ называется обобщенным решением системы (3).

Как построить обобщенное решение?

Рассмотрим систему (3) с булевыми переменными.

Пусть

$$\begin{cases} (a_1, x) = f_1(x) \\ (a_2, x) = f_2(x) \\ \dots \\ (a_m, x) = f_m(x) \end{cases}$$

И $L^*(f_1), L^*(f_2), \dots, L^*(f_m)$ - множество значений, принимаемых функциями $f_1, \dots, f_m$ на B^n .

Если x_0 – классическое решение совместной системы

$$\begin{cases} (a_1, x) = f_1(x) = b_1 \\ (a_2, x) = f_2(x) = b_2 \\ \dots \\ (a_m, x) = f_m(x) = b_m, \end{cases} \quad (4)$$

то необходимым и достаточным условием разрешимости системы (3) является выполнение соотношения

$$b_i \in \bigcap_{k=1}^m L^*(f_k), i=1, \dots, m.$$

Обозначим через $L^*(a)$ - множество решений уравнения $L(x)=a$, т.е. множество булевых векторов, доставляющих значение a линейной форме $L(x)$.

Таким образом система уравнений $L_i(x)=a_i, i=1, \dots, m$, порождает систему подмножеств $\{L_i^*(a_i)\} = V \subseteq 2^{B^n}$.

Определение. Подмножество $M \subseteq B^n$ называется протыкающим для системы множеств V , если выполняется условие $M \cap V \neq \emptyset$.

Таким образом, элементы протыкающего множества имеют представителей в каждом из подмножеств системы. В нашем случае это означает, что каждое из уравнений системы (4) удовлетворяется хотя бы одной из точек протыкающего множества. В частности, если $|M|=1$, то M является обычным решением системы (4).

Итак, пусть $M=\{y_1, \dots, y_r\}$ – протыкающее множество для V и V_i – множество уравнений из системы (4), для которых точка y_i является решением, тогда разбиение множества

уравнений $\{L_i^*(a_i)\} = \bigcup_{i=1}^r V_i$ есть разбиение на подсистемы, каждая из которых совместна.

Нахождение протыкающего множества наименьшей мощности эквивалентно разбиению несовместной системы на минимальное число совместных подсистем.

Формально это выглядит следующим образом.

Определение. Подмножество T строк $(0,1)$ - матрицы A называется покрытием, если в подматрице A' , образованной этими строками, нет нулевых столбцов.

Число строк $|T|$ называется мощностью покрытия, а минимум этой величины по всем покрытиям матрицы – глубиной матрицы. Обозначим эту величину через $\xi(A)$.

Пусть $B^n = \{x_1, x_2, \dots, x_{2^n}\}$ и $V = \{W_1, \dots, W_m\}$, где $W_i = \{L_i^*(a_i)\}, i = 1, \dots, m$. Рассмотрим $(0,1)$ -матрицу $W = \|w_{ij}\|$ размеров $2^n \times m$, где

$$w_{ij} = \begin{cases} 1, & \text{если } x_j \in W_i \\ 0, & \text{если } x_j \notin W_i \end{cases}.$$

Теорема 2. Минимальное число совместных подсистем, на которое можно разбить систему (4) равно глубине матрицы W .

Пример 2. Рассмотрим следующую несовместную систему уравнений:

$$\begin{cases} L_1 = x_1 + x_2 + x_3 = 1 \\ L_2 = x_1 + 2x_2 + x_3 = 2 \\ L_3 = x_1 + 2x_2 + 3x_3 = 3 \end{cases}.$$

Для нее имеем $L_1^*(1) = \{(001), (010), (100)\}$, $L_2^*(2) = \{(010), (101)\}$, $L_3^*(3) = \{(001), (110)\}$. Тогда вышеупомянутая матрица W имеет вид

$$W = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Покрытиями матрица являются, например, подмножества $\begin{pmatrix} 101 \\ 010 \end{pmatrix}, \begin{pmatrix} 110 \\ 001 \end{pmatrix}$, а $\xi(W)=2$.

Вывод

Попытка учесть в математической модели определенную информацию о моделируемом объекте может привести к противоречиям внутри модели за счет разного смысла и степени важности различных аспектов моделируемого объекта. Для случая, когда математическое описание сводится к набору булевых уравнений в работе приведены два метода получения из противоречивой модели некоторого ее корректного аналога.

В первом случае показано, что путь подбора и уточнения отдельных параметров задачи может привести к необходимости почти полного их пересмотра.

В то же время, учет комбинаторики исходной задачи является более логичным и эффективным.

Достоверность результатов следует из корректности определений и доказательств теорем.

Литература

1. Пападимитриу Х., Стайглиц С. Комбинаторная оптимизация. М.: Мир. 1989. 512 с.
2. Горшков С.П., Тарасов А.В. Сложность решения систем булевых уравнений. М.:Курс, 2017. 192 с.
3. Леонтьев В.К., Тоноян Г.П. О системах булевых уравнений// ЖВМ и МФ. 2013. №5 (53). С.109-116. DOI:10.7868/S0044466913050098.
4. Torshin I.Yu., Rudakov K. V. On the application of the combinatorial theory of solvability to the analysis of chemographs // Pattern Recognition and Image Analysis. 2014. Vol. 24. P. 11–23.
5. Леонтьев В.К., Тоноян Г.П. Приближенные решения систем булевых уравнений// ЖВМ и МФ. 1993. №9 (93). С.1383-1390.
6. Леонтьев В.К. Комбинаторика и информация. Часть 1. Комбинаторный анализ. М.: МФТИ, 2015. 174 с.

On approximate "solutions" of overdetermined systems of Boolean equations

Leontiev V.K.⁷⁷, Gordeev E.N.⁷⁸

Abstract. A system of linear equations with Boolean variables is considered. Finding its solution, or even answering the question of the existence of such a solution – is an NP-complete problem. The paper analyzes two possible approaches to the "solution" of overdetermined systems of such equations. The first approach is to argue that the "importance" of the various equations of the system are not the same, and that the accuracy of the initial information about the system is different for different initial parameters of the system. The second approach is based on the assumption of a possible decomposition of the original system with the possibility of further aggregation of the solution of the system from the solutions of its subsystems. In this case, different combinatorial characteristics of the system are used.

Keywords: Diophantine equations, overdetermined systems, approximate solutions, depth of matrices.

⁷⁷ Leontiev Vladimir, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, vkleontiev@yandex.ru.

⁷⁸ Gordeev Eduard, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, tatmigor@gmail.com.

Средства фоноскопической экспертизы нового поколения

Горшков Ю.Г.⁷⁹

Рассмотрены основные характеристики средств фоноскопического исследования аудиозаписей на основе преобразования Фурье. Изложены принципы частотно-временного анализа речевого сигнала с использованием вейвлет-технологии. Представлены примеры построения вейвлет-сонограмм с высоким частотно-временным разрешением. Проведено сравнение частотно-временных характеристик сонограмм звуков речи, полученных с использованием преобразования Фурье и многоуровневого вейвлет-преобразования.

Ключевые слова: фоноскопическое исследование, преобразование Фурье, многоуровневый вейвлет-анализ, сонограмма

Введение

Вопросы создания инструментальных средств фоноскопического исследования аудиозаписей, их эффективного применения в практике экспертов за последние годы относятся к наиболее важным [1-3]. Особое значение при разработке новых методов анализа фонограмм придается решению задач, связанных с созданием надежной технологии обнаружения признаков их монтажа. Широкое распространение звуковых редакторов, доступных программ обработки и монтажа аудиозаписей привели к ситуации, когда фальсификация вещественных доказательств, в качестве которых могут быть фонограммы речи, является даже для непрофессионала относительно простой задачей. В то же время вопросы обнаружения признаков монтажа фонограмм, как правило, всегда относились к трудно разрешимым.

Средства фоноскопического исследования аудиозаписей на основе преобразования Фурье. В настоящее время анализ звуков речи основывается на спектральной модели для стационарного сигнала. К недостаткам данной модели следует отнести отсутствие характеристик произносимых согласных и это при том, что в большинстве языков основная речевая информация передается согласными звуками. Практически во всех комплексах фоноскопического исследования аудиозаписей реализованы алгоритмы идентификации личности по голосу с использованием исключительно характеристик гласных звуков.

В последние годы широкое применение находят аппаратно-программные средства «Икар Лаб», «Justiphone» и «OTExpert». Принятие решения при идентификации личности по голосу в перечисленных средствах основывается на оценке спектральных характеристик гласных звуков, полученных на основе преобразования Фурье.

Средства фоноскопического исследования аудиозаписей с использованием многоуровневого вейвлет-анализа «Эксперт МВА». Назначение средств «Эксперт МВА» - фоноскопическое исследование аудиозаписей, включающее определение подлинности фонограмм и идентификацию диктора [4-7]. Технические характеристики аппаратной части средств «ЭКСПЕРТ МВА»: 4-х каналный ввод звуковых сигналов с использованием модуля NI 9234, National Instruments (USA), 24 бита, 51.2 кС/с, динамический диапазон 102 дБ; голосовой ввод на базе измерительного микрофона МПА-201, AKG (Австрия), полоса частот: 10 Гц - 20 кГц. Программные средства анализа сигналов «WaveView VSA» обеспечивают получение частотно-временных параметров не

⁷⁹ Горшков Юрий Георгиевич, к.т.н., г. Москва, МГТУ им. Н.Э.Баумана, e-mail: y.gorshkov@npo-echelon.ru

только гласных, но и согласных звуков. На рис. 1 представлена вейвлет-сонограмма речевого сигнала слова «Крюк».

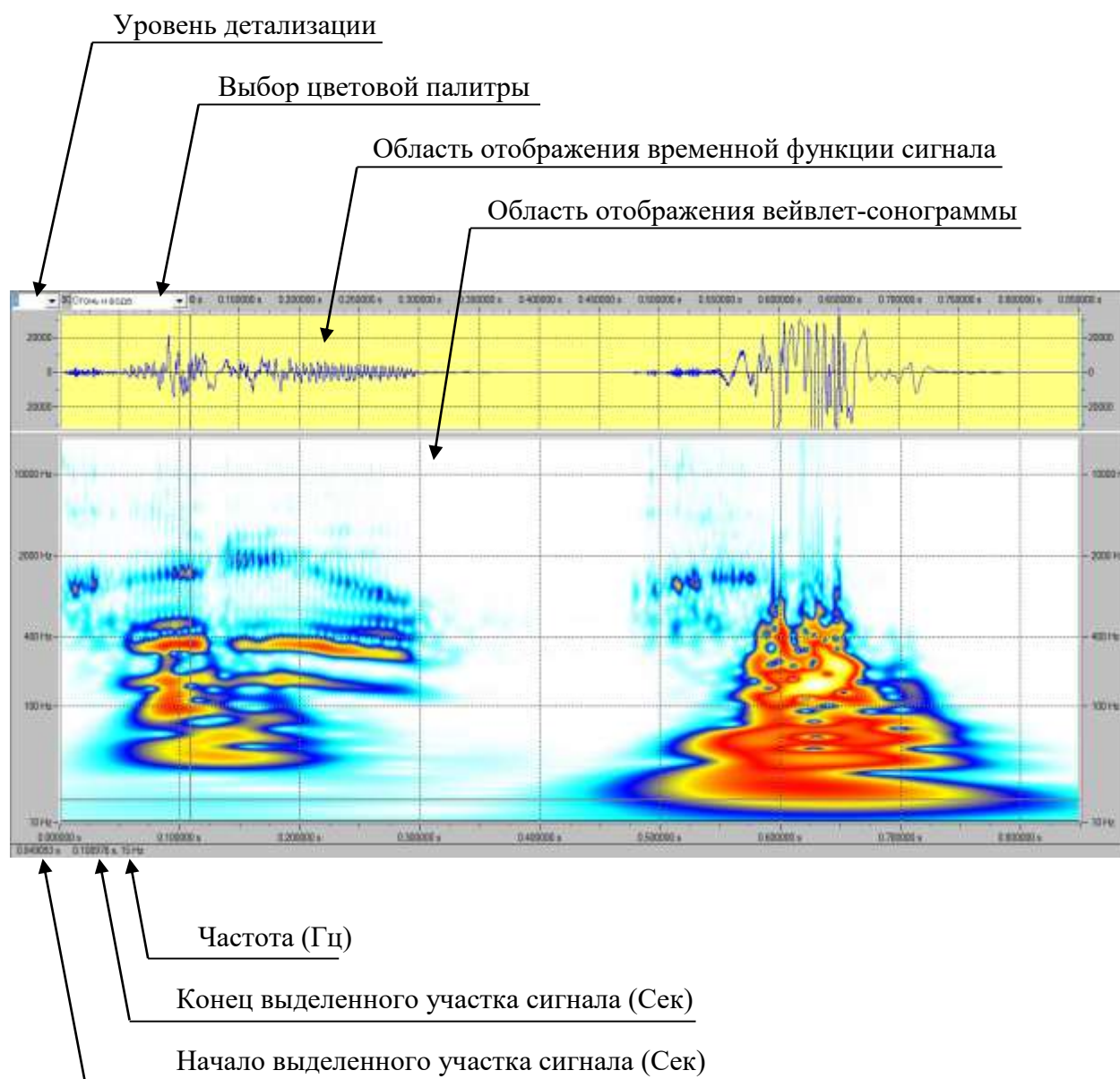


Рис. 1. Вейвлет-сонограмма речевого сигнала слова «Крюк»

Все операции, выполняемые программным средством «WaveView VSA» можно разделить на 3 группы. *Первая группа* находится в разделе меню «Правка», включает такие операции, как «вырезать», «копировать», «вставить». *Вторая группа* операций находится в разделе меню «Вид», обеспечивает получение информации об анализируемом сигнале: «Приближение» - изменение масштаба изображения; «Интерполяция» - отображение отсчетов сигнала при значительном увеличении; «Сонограмма» - построение вейвлет-сонограммы по заданным параметрам; «W-фильтрация» - фильтрации сигнала с использованием вейвлетов Добеши, Койфмана, Шеннона; «Фазовая составляющая» - вычисление фазы сигнала; «Информация о звуке» - отображение значений частоты дискретизации, разрядности, длительности записи и отношения сигнал/шум. *Третья группа*

операций находится в разделе меню «Преобразования». Возможна обработка всего файла сигнала, либо выделенной его части. Виды операций: «Инверсия времени» - считывание отсчетов сигнала в обратном порядке; «Инверсия по частоте» - преобразование сигнала в частотной области; «Режекция частотной составляющей» - удаление из сигнала указанной частоты; «Сдвиг по частоте» - сдвиг сигнала на заданную величину в герцах; «Инверсия по фазе» - поворот фазы сигнала на 180 градусов. С использованием программных средств комплекса «Эксперт МВА» разработана новая методика инструментального исследования акустических сигналов аудиозаписей. Отличие данной методики от распространенных, построенных на основе Фурье-анализа, заключается в том, что в ней применяется технология цифровой обработки речевых сигналов нового поколения - многоуровневый вейвлет-анализ (МВА).

Отличительные особенности аппаратно-программных средств «Эксперт МВА» при проведении фоноскопической экспертизы:

1. Определение подлинности аудиозаписи с использованием функции «звуковой микроскоп»; выделение сигналов фона сети питания 50 Гц малого уровня (до -60 дБ).
2. Получение биометрических маркеров уровня эмоциональной напряженности говорящего за счет выделения низкочастотных биомедицинских сигналов в диапазоне 10-30 Гц.
3. Получение частотно-временных параметров согласных звуков.

Выводы

Средства криминалистического исследования фонограмм с использованием многоуровневого вейвлет-анализа «Эксперт МВА» относятся к технологиям фоноскопической экспертизы нового поколения, находят все большее применение. Существенные преимущества разработанной технологии показаны на примерах судебной практики при проведении инструментального исследования фонограмм, выполненного на основании официальных запросов адвокатской конторы «САНКТАЛЕКС» (№ 36) КА МГКА.

Уникальные возможности комплекса «Эксперт МВА» демонстрировались в 2019 году на мероприятиях:

1. XVII Международная выставка по электронике, компонентам, оборудованию и технологиям «ChipEXPO-2019». 16-18 октября, Экспоцентр, Москва.
2. XXIII Международная выставка «INTERPOLITECH-2019»: безопасность, определяющая будущее. 22-25 октября, ВДНХ, Москва.

Литература

1. Горшков Ю.Г. Криминалистическое исследование фонограмм. Методические указания к лабораторным работам. МГТУ им. Н.Э. Баумана. 2017. 32 с.
2. Горшков Ю.Г. Обработка речевых и акустических биомедицинских сигналов на основе вейвлетов / Научное издание. М.: Радиотехника. 2017. 240 с.
3. Галяшина Е. И. К вопросу о достоверности криминалистической идентификации личности по цифровым фонограммам устной речи // Известия Тульского государственного университета. Экономические и юридические науки. 2016. Том 3, № 2. С. 19-25.
4. Горшков Ю.Г. Многоуровневый вейвлет-анализ акустических сигналов при решении задач фоноскопической экспертизы / «Информатизация и информационная безопасность правоохранительных органов»: Материалы XX Международной научной конференции. 2011. Москва. С. 379-387.
5. Горшков Ю. Г. Применение комплекса «ЭКСПЕРТ МВА» при криминалистическом исследовании фонограмм // Материалы XXIII Всероссийской научной конференции «Информатизация и информационная безопасность правоохранительных органов», 28 мая 2014 г. Москва. С. 212-217.

6. Горшков Ю. Г. Визуализация многоуровневого вейвлет-анализа фонограмм // Электронный журнал «Научная визуализация». Национальный Исследовательский Ядерный Университет «МИФИ». 2015. № 2. Том 7, квартал 2. С. 96-111.

7. Горшков Ю. Г., Каиндин А. М., Марков А. С., Цирлов В. Л. Система определения подлинности фонограмм. Патент на полезную модель RUS 150244. 30.12.2013. Заявка № 2013158829/08. Бюл. № 4.

Means of Phonoscopic Examination of the New Generation **Y.G. Gorshkov⁸⁰**

Abstract. *The main characteristics of the means of phonoscopic research of audio recordings based on the Fourier transform are considered. The principles of the time-frequency analysis of a speech signal using wavelet technology are stated. Examples of constructing wavelet sonograms with high frequency-time resolution are presented. The frequency-time characteristics of sonograms of speech sounds obtained using the Fourier transform and a multilevel wavelet transform are compared.*

Keywords: *phonoscopic research, Fourier transform, multilevel wavelet analysis, sonogram*

⁸⁰ Yuri Gorshkov, Ph.D., Bauman MSTU, Moscow, y.gorshkov@npo-echelon.ru

Обработка изображений в информационной безопасности

Дамдинова Т.Ц.⁸¹, Базарон С.С.⁸², Абатнин А.А.⁸³

Аннотация

В статье рассматриваются задачи обработки изображений применительно к информационной безопасности. Приведены результаты анализа литературы последних лет, из которого видно, что методы и средства обработки цифровых изображений продолжают развиваться и находят новые области применения. Основные задачи связаны с информационной безопасностью в биометрических системах и защитой авторских прав.

Ключевые слова: защита информации, биометрические системы, авторское право, обработка цифровых изображений, цифровой водяной знак, аберрации цифровых изображений, выделение линий, распознавание образов.

Введение

В области защиты информации задачи обработки изображений используются для организации мер технической защиты от несанкционированного доступа. Одним из наиболее широко используемых и эффективных средств от несанкционированного доступа к информации является установка видеокамер. Данной теме посвящено много научных работ последних лет, направленных на улучшение качества видеoinформации. Кроме того, имеется ряд работ в области защиты видеoinформации от несанкционированного использования и авторских прав на видео и другую информацию.

Обработка изображений в области информационной безопасности

Для защиты информации как собственности в последние время большое внимание получили способы добавления специальных опознавательных знаков в видео, цифровое изображение, электронный текст. В качестве таких средств защиты информации от несанкционированного использования разрабатываются методы внедрения цифрового водяного знака [1,2]. Код цифрового водяного знака анализируются специальным декодером, который определяет наличие информации о правообладателе, другие данные, подтверждающие подлинность или авторское право на видео или изображении содержащего рисунки или текст.

При обработке данных из видеопотока, полученного с камер слежения, кроме задачи анализа изменения сцены и обнаружения движения на видео [3,4] возникает необходимость выполнять покадровый анализ данных с целью поиска и распознавания объектов. Автоматизация данной задачи позволяет значительно сократить время обработки.

Обработка изображений используется также в биометрических системах как средство идентификации и аутентификации пользователя. Наиболее популярными системами идентификации являются сканирование отпечатков пальцев, ладони руки, сетчатки и радужной оболочки глаза, анализ лица человека [5]. Применительно к процессам

⁸¹Дамдинова Татьяна Цыбиковна, к.т.н., доцент, Восточно-Сибирский государственный университет технологий и управления, г.Улан-Удэ, dtatyanac@mail.ru

⁸²Базарон Сэсэг Арсалановна, к.т.н., доцент, Восточно-Сибирский государственный университет технологий и управления, г.Улан-Удэ, seseg003@gmail.com

⁸³Абатнин Александр Андреевич, студент, Восточно-Сибирский государственный университет технологий и управления, г.Улан-Удэ, a.abatnin@mail.ru

сканирования и анализа отпечатков пальцев имеется много работ посвященных методам повышения качества при решении подобных задач [6-9].

Распознавание объектов на биометрических данных, обработка сцен видеок кадров базируются на анализе контуров [10-12]. Этот этап обработки изображений играет решающую роль для дальнейшего анализа с целью распознавания. При этом необходимо учитывать, что на изображение могут влиять помехи формирования изображения [13,14]. Для улучшения качества изображения с целью корректировки аппаратных помех необходимо компенсировать возникшие аберрации [15].

Для анализа границ выделенных объектов реализовано множество различных методов, основным требованием к которым является точность или соответствие допустимому отклонению. Одним из значимых показателей при описании контура является его гладкость [16]. Вычислительные мощности современных компьютеров позволяют выполнять расчеты с достаточно высокой скоростью, что позволяет использовать разработанные методы в системах реального времени.

В связи с развитием технологий 3D сканирования и 3D печати появляются новые возможности в области проектирования и изготовления изделий, существенно влияющие на скорость и экономию времени и материальных ресурсов при производстве и, соответственно, появляются новые задачи и в области защиты информации. [17,18]. Во-первых, это относится к вопросу защиты авторских прав, особенно это касается производства конструкторских изделий с грифами секретности. Во-вторых, усовершенствование способов обработки и создания моделей, появление все новых материалов для 3D печати ставят под угрозу эффективность биометрических систем [19,20]. Это в свою очередь будет способствовать дальнейшему развитию и новым исследованиям по повышению информационной безопасности.

Выводы

Методы и способы обработки цифровой информации находят широкое применение в области информационной безопасности. С развитием информационных технологий 3D печати появляются новые задачи в области защиты авторских прав и повышения защиты информации.

Литература

1. Горбенко Р. К. Исследование механизмов защиты цифровой видеoinформации при её передаче в распределенных компьютерных сетях // Молодой ученый.-2018. №9.- с. 29-34.
2. Абасова А.М., Бабенко Л.К. Разработка алгоритма внедрения цифрового водяного знака на базе морфологической обработки изображения и модулярной арифметики для противодействия угрозам хищения объектов интеллектуальной собственности // Международный журнал прикладных и фундаментальных исследований. – 2018. -№6–С.9-14
3. Козлов В.А., Потапов А.С."Анализ методов выделения движущихся объектов на видеопоследовательностях с шумами // Научно-технический вестник информационных технологий, механики и оптики, №. 3 (73), 2011, с. 39-43.
4. Макаров М.А., Берестнева О.Г., Андреев С.Ю. Решение задачи описания и классификации контуров движущихся объектов на видео. // Известия Томского политехнического университета. Информационные технологии. 2014. Т. 325. №5... С. 77–83
5. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с
6. Гудков В. Ю. Способы математического описания и идентификации отпечатков пальцев. // Труды ИСА РАН 2008. Т. 38 с.336-356
7. Рыканов А.С. Анализ методов распознавания отпечатков пальца. // Системи обробки інформації, 2010, випуск 6 (87).- с.164-
8. Фам Зуй. Тхай. Некоторые вопросы применения методов сравнения отпечатков пальцев для биометрических систем идентификации личности // Международный научно-исследовательский журнал. — 2015. — №7 (38) Часть 1. — С. 127—130.

9. Бехтольд О.В., Гудков В.Ю. Модификация алгоритма анализа области частот для отпечатков пальцев. // Труды конференции GraphiCon, 2017, с.101-102
10. Гонсалес Р., Вудс Р., Цифровая обработка изображений. — М.: Техносфера, 2005, 2006. — 1072 с.
11. Фурса Н.Е. Метод поиска объектов на изображении с помощью контурного анализа по заданным характеристикам их контуров. Открытые информационные и компьютерные интегрированные технологии №64, 2014. -172-175
12. Новиков А.И., Саблна В.А., Горячев Е.О. Применение контурного анализа для совмещения изображений. Известия ТулГУ. Технические науки. 2013. Вып. 9. Ч.1. – с.260-269
13. Jahne Bernd, Haussecker Horst., Computer Vision and Applications. A Guide for Students and Practitioners - Academic Press, 2000 — 702 p.
14. Дамдинова Т.Ц. Способы формирования цифровых изображений и анализ их погрешностей // Вопросы кибербезопасности. 2014. №5. с.43-46.
15. Tatiana Ts. Damdinova, Liubov D. Zhimbueva, Innokentii T. Bubeev, Nasak N. Dampilov. Correction of Digital Images Distortion. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 45-48.
16. Дамдинова ТЦ., Бубеев ИТ., Мотошкин ПВ. Метод моделирования кривой первого порядка гладкости. //Программные системы и вычислительные методы. - 2019.- вып.17. с.12-17
17. Николаева Н.И. 3D-печать и интеллектуальная собственность: правовая охрана 3d-моделей.//Цифровые технологии февраль 2019. https://www.kommersant.ru/region/novosibirsk/files/novosibirsk/pdf/cifrovye_tehnologii.pdf. [Электронный ресурс:] дата обращения 20/11/2019
18. Наумов В, Загородная А., Ахобекова Р. Правовые аспекты 3D-печати. // Журнал IT-News [№ 03/2017] [Электронный ресурс:] дата обращения 20/11/2019
19. 3D-печатные очки помогли обмануть биометрическую систему распознавания лиц. // <https://3dtoday.ru/blogs/news3dtoday/3dprinted-glasses-helped-to-deceive-a-biometric-system-of-face-recogni/>[Электронный ресурс:] дата обращения 20/11/2019
20. 3D-перчатка обманывает любую биометрическую систему безопасности// https://hightech.fm/2016/10/24/fingerprints_copy_gloves [Электронный ресурс:] дата обращения 20/11/2019

Image processing in information security

Damdinova T.⁸⁴, Bazaron S.⁸⁵, Abatnin A.⁸⁶

Annotation

The article discusses the task of image processing in relation to information security. The results of the analysis of recent literature are presented, from which it is clear that the methods and means of digital images processing continue to evolve and find new areas of application. The main tasks are related to information security in biometric systems and copyright protection.

Keywords: *information security, biometric system, copyright, digital image processing, digital watermark, aberration of digital images, edge detection, pattern recognition.*

⁸⁴Damdinova T., Ph.D., Associate Professor, East-Siberia State University of Technology and Management, Ulan-Ude, datyanac@mail.ru

⁸⁵Bazaron S., Ph.D., Associate Professor, East-Siberia State University of Technology and Management, Ulan-Ude, seseg003@gmail.com

⁸⁶Abatnin A., Student, East-Siberia State University of Technology and Management, Ulan-Ude, a.abatnin@mail.ru

Обзор методов распознавания компьютерных атак

Добкач Л. Я.⁸⁷

Статья посвящена рассмотрению ряда существующих методов обнаружения вторжений с позиций их достоинств и недостатков, а также с учётом их классификации. Ввиду постоянно возникающих новых и более сложных вызовов безопасности информационных ресурсов требуется разработать иные методы, которые будут более эффективно выявлять аномалии сетевого трафика и злоупотребления. Перспективной группой методов выступают гибридные методы, и на основе соотнесения наиболее значимых недостатков разобранных методов предлагается гибридный метод, использующий преимущества как искусственных нейронных сетей, так и сигнатурных методов.

Ключевые слова: информационная безопасность, обнаружение вторжений, поведенческие методы, сигнатуры атак, искусственные нейронные сети, гибридные методы.

Введение

Существует множество методов, имеющие свои достоинства и недостатки, но нельзя сказать, что есть хотя бы один, который может выявлять любую атаку, в том числе неизвестную ранее.

Целью настоящего доклада ставится изучение разработанных методов обнаружения компьютерных атак для последующего создания более эффективного метода.

Теоретическая значимость нашего исследования заключается в введении эффективного метода распознавания атак и его формализации.

Практическая значимость связана с будущей реализацией такого метода в системе обнаружения вторжений, что позволит лучше распознавать атаки, а значит, и защищать информационные активы пользователей и предприятий.

ПОВЕДЕНЧЕСКИЕ МЕТОДЫ

Важную роль в обнаружении аномалий играют поведенческие методы [1-3]. К ним можно отнести **вейвлет-анализ**, **спектральный** [4], **статистический анализ** [5-7], **анализ энтропии** и др.

Объединяет перечисленные выше методы сравнение параметров наблюдаемого поведения с нормальным профилем системы. Им характерен вероятностный фактор, из-за чего не всегда СОВ реагирует только на аномалии.

Повышение точности сопряжено со значительными временными затратами. Гораздо хуже, если на этом этапе злоумышленник планомерно внесёт злонамеренные действия в нормальный профиль системы, тогда средство защиты информации будет воспринимать аномалии как должное.

⁸⁷ Добкач Леонид Яковлевич, специалист, аспирант, МГТУ им. Н. Э. Баумана, Москва, dobkachleo@mail.ru

МЕТОДЫ НА ОСНОВЕ ЗНАНИЙ

Методы из данной группы чаще применяются для обнаружения злоупотреблений. Широко распространённые **сигнатурные методы** гарантируют высокую точность распознавания, но только известных атак. Также, из-за больших баз сигнатур, страдает производительность СОВ [8].

Адаптивность **языков описания сценариев атак** сопряжена с вычислительной сложностью и низким быстродействием. Для **анализа систем состояний** характерны наглядность и точность, но и отсутствие адаптивности [4, 9]. Достоинство **сетей Петри** — упреждение атаки, недостаток — сложность реализации [4].

Экспертные системы имеют высокое быстродействие и точность, однако требуют объёмной обучающей выборки для создания правил, откуда вытекает низкая адаптивность к неизвестным атакам [4, 9]. Аналогичные достоинства присущи **методу проверки на модели** [3], а также независимость представления от формы данных аудита. Практическая реализация крайне трудна, а сам метод лучше работает вместе с подсистемой обнаружения аномалий [3, 4].

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ

Деревьям решений присущи адаптивность, быстродействие, верифицируемость, относительная точность и зависимость от объёма обучающей выборки [4, 10, 11].

Байесовские сети и её частный случай — **байесовский метод** (предполагается независимость входных переменных модели) — способны работать в режиме реального времени и выявлять конкретно аномалии. Недостаток: влияние измерений друг на друга, что сильно усложняет сам метод [3, 4].

МЕТОДЫ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА

Алгоритмы большинства методов этой группы имитируют явления живой природы, обеспечивая высокую адаптивность и быстродействие. Яркий пример — **искусственные нейронные сети** (ИНС), чья точность зависит от качества обучения и объёма обучающей выборки [9, 12, 13]. Гибкость ИНС обеспечивает достаточно высокий уровень защищённости информации [6, 11, 14].

Искусственные иммунные сети (ИИС) основаны на иммунной системе человека. В основе их обучения лежат такие алгоритмы, как отрицательный отбор и клональная селекция [4, 15, 16]. Подобны нейронным сетям.

Генетические алгоритмы (ГА), имитирующие процессы естественного отбора, обеспечивают точность и малое ресурсопотребление [4]. Нередко ГА применяют вместе с другими моделями классификации данных, например, с ИИС [17].

Метод опорных векторов применяется обычно для классификации элементов из двух линейно разделимых множеств. При линейной неразделимости на два множества вытекают недостатки: сложность интерпретации параметров модели, невозможность калибровки вероятности попадания в определённый класс и эффективность метода только для решения задач с двумя классами [4, 9, 18].

Исходя из приведённых характеристик разобранных методов интеллектуального анализа, можем сделать вывод о неточности распознавания в угоду адаптивности. Затраты памяти

или снижение производительности из-за вычислительной сложности алгоритма также возможны.

ГИБРИДНЫЕ МЕТОДЫ

С практической точки зрения, можно достичь высоких показателей выявления атак путём нахождения наилучшего совмещения нескольких методов [4, 18]. Их недостатки не должны усугублять друг друга, поэтому изучим отрицательные стороны разобранных методов с помощью таблицы 1.

Таблица 1.

Недостатки методов распознавания атак

Метод	Группы недостатков				
	Затраты времени	Затраты памяти	Сложность реализации	Нет адаптивности	Неточность (на известных данных)
1. Поведенческие методы					
Вейвлет-анализ	+		+		
Спектральный анализ	+		+		
Статистический анализ		+			+
Анализ энтропии		+			+
2. Методы на основе знаний					
Сигнатурные методы	+	+		+	
Языки описания сценариев атак	+		+		
Анализ систем состояний				+	
Сети Петри			+		
Экспертные системы		+		+	
Метод проверки на модели			+		
3. Методы машинного обучения					
Деревья решений					+
Байесовские сети			+		
Байесовский метод			+		

4. Методы вычислительного интеллекта					
Нейронные сети					+
Иммунные сети					+
Генетические алгоритмы	+		+		+
Метод опорных векторов			+		

Несмотря на вынужденную неполноту картины, можно предложить метод на основе нейронных сетей, обучаемых на базе сигнатур, которые затем используются для уточнения выходных данных. Дополнительную точность могут придать ансамблевые структуры [4, 15, 19] из малого числа нейронных сетей. Принцип действия описывается формулой (1):

$$K(x) = \begin{cases} \left[\frac{\sum_{i=1}^n \frac{T_i SK^2(x)}{P_i(x)}}{n} \right], SK(x) \neq 0 \\ \left[\frac{\sum_{i=1}^n T_i P_i(x)}{n} \right], SK(x) = 0 \end{cases}, \quad (1)$$

где x — событие сетевого трафика, n — количество ИНС, $K(x)$ — класс события x , T_i — точность i -й ИНС (уровень ложной тревоги [10]), $P_i(x)$ — вероятный класс события x для i -й ИНС, $SK(x)$ — класс события x (если известна его сигнатура).

Пример с несколькими вариантами распределения значений класса (от 0 для незнакомых событий и от 1 до 5 для известных) приведён в таблице 2.

Таблица 2.

Теоретический эксперимент

$SK(x) \setminus T_i$	0,7	0,3	0,9	
1	4	3	2	1 (0,2)
3	2	2	2	3 (2,8)
0	3	4	1	1 (1,4)
5	5	1	4	5 (5,5)
3	1	2	5	3 (3,1)

Выводы

На основе анализа преимуществ и недостатков порядка двадцати методов из четырёх групп предложен гибридный метод, использующий как адаптивность ИНС, так и точность сигнатурных методов.

Теоретический эксперимент (табл. 2) демонстрирует целесообразность применения предложенного метода в несигнатурных СОВ [19, 20], что может обеспечить более высокий уровень защищённости информационных систем и сетей.

Литература

1. Ананьин Е. В. Методы обнаружения аномалий и вторжений / Е. В. Ананьин, И. С. Кожевникова, А. В. Лысенко, А. В. Никишова // Проблемы современной науки и образования. — № 34 (76). — Иваново: Олимп, 2016. — С. 48-50.
2. Добкач Л. Я. Анализ эффективности систем обнаружения вторжений // Всероссийская студенческая конференция «Студенческая научная весна», посвященная 165-летию со дня рождения В.Г. Шухова: сборник тезисов докладов / Федеральное агентство по делам молодежи (Росмолодежь), Московский государственный технический университет им. Н.Э. Баумана, СНТО им. Н.Е. Жуковского. — М.: ООО «Издательский дом «Научная библиотека», 2018. — С. 314-315.
3. Корниенко А. А. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования / А. А. Корниенко, И. М. Слюсаренко: дисс. ... докт. техн. наук. — СПб.: ПГУПС, 2009. — Режим доступа: http://citforum.ru/security/internet/ids_overview/ (дата обращения: 12.11.2019).
4. Браницкий А. А. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, И. В. Котенко // Труды СПИИРАН. — № 2 (45), 2016. — С. 207-244.
5. Басараб М.А., Строганов И.С. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4 (7). С. 30-40.
6. Слесарчик К.Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопросы кибербезопасности. 2018. № 1 (25). С. 19-27.
7. Ieracitano C. Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection / C. Ieracitano, A. Adeel, M. Gogate and etc. / 9th International Conference on Brain Inspired Cognitive Systems (BICS 2018). — Cham: Springer, 2018. — С. 759-769.
8. Кусякина Н. М. Методы анализа сетевого трафика как основа проектирования системы обнаружения сетевых атак // International Scientific Review of the Problems and Prospects of Modern Science and Education: сборник трудов XLI Международной научно-практической конференции. — Бостон: Problems of Science, 2018. — С. 28-31.
9. Гамаюнов Д. Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: дисс. ... канд. физ.-мат. наук: 05.13.11. — Москва, 2007. — 88 с.: ил. РГБ ОД, 61:07-1/1269
10. Брюховецкий А. А. Обнаружение уязвимостей в критических приложениях на основе решающих деревьев / А. А. Брюховецкий, А. В. Скатков, П. О. Березенко // Радиоэлектронные и компьютерные системы. — № 5 (64), 2013. — С. 18-23.
11. Кочетов Д. А. Нейросетевая технология обнаружения сетевых вторжений / Д. А. Кочетов, Е. П. Лукашик // Прикаспийский журнал: Управление и высокие технологии. — № 2(42), 2018. — С. 104-112.
12. Добкач Л. Я. Создание модуля распознавания атак для систем обнаружения вторжений // Всероссийская студенческая конференция «Студенческая научная весна», посвященная 85-летию Ю.А. Гагарина: сборник тезисов докладов / Министерство науки и высшего

образования РФ, Московский государственный технический университет им. Н.Э. Баумана, СНТО им. Н.Е. Жуковского. — М.: ООО «Издательский дом «Научная библиотека», 2019. — С. 36–37.

13. Тарасов Я.В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. № 5 (24). С. 23-29.

14. Чистоходова А. А. Модернизированный метод обнаружения низкоинтенсивных распределённых атак типа «Отказ в обслуживании» / А. А. Чистоходова, И. Д. Сидоров // Успехи современной науки, т. 1. — № 12, 2017. — С. 169-175.

15. Брюховецкий А. А. Адаптивная модель обнаружения вторжений в компьютерных сетях на основе искусственных иммунных систем / А. А. Брюховецкий, А. В. Скاتков // Электротехнические и компьютерные системы. — № 12 (88), 2013. — С. 102-111.

16. Петренко С.А., Курбатов В.А., Бугаев И.А., Петренко А.С. Когнитивная система раннего предупреждения о компьютерном нападении // Защита информации. Инсайд. 2016. № 3 (69). С. 74-82.

17. Jeya P. G. Efficient Classifier for R2L and U2R Attacks / P. G. Jeya, M. Ravichandran, C. S. Ravichandran // International Journal of Computer Applications. — Vol. 45, № 21. — NY: Foundation of Computer Science, 2012. — С. 28-32.

18. Абрамов Е. С. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на Web-сервисы / Е. С. Абрамов, И. В. Тарасов // Инженерный вестник Дона. — № 3 (46), 2017. — С. 59.

19. Петренко С.А., Цирлов В.Л. Импортзамещение решений IDS и SIEM // Защита информации. Инсайд. 2017. № 5 (77). С. 46-51.

20. Барабанов А., Марков А., Цирлов В. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. С. 31-33.

Научный руководитель: Цирлов Валентин Леонидович, к.т.н., CISSP, CISM, AMBCI, доцент МГТУ им. Н.Э. Баумана, генеральный директор НПО «Эшелон», v.tsirlov@npo-echelon.ru

The review of methods for identification of computer attacks

Dobkacz L. Ya.⁸⁸

The article is devoted to the viewing the number of existing methods of intrusion detection from the perspective of their advantages and disadvantages and also takes their classification into account. For reasons of ever new and more complicated challenges, the development of alternative methods which will identify anomalies of the network traffic and abuses is required. Hybrid methods represent a promising group of such methods, and the hybrid method that can use strengths of artificial neural networks, as well as of signature-based methods is suggested in accordance with the correlation of the most significant weaknesses in the analyzed methods.

Keywords: intrusion detection, behavioral methods, attack signatures, artificial neural networks, hybrid methods

⁸⁸ Leonid Yakovlevich Dobkacz, specialist, postgraduate, Bauman MSTU, Moscow, dobkachleo@mail.ru

Анализ проектов электронной идентификации граждан в Латинской Америке

Ефремов Е.А.⁸⁹, Ершова Ю.А.⁹⁰, Чуфистов А.А.⁹¹

Аннотация: Высокий уровень криминогенной обстановки в странах Латинской Америки вынуждает правительства государств искать новые технологические подходы к решению проблем безопасности, в том числе и в банковской сфере. В 2014 году Латинская Америка была названа крупнейшим растущим рынком биометрических технологий. В работе приводится анализ различных проектов электронной идентификации граждан стран Латинской Америки.

Ключевые слова: электронная идентификация, e-card, биометрические технологии

Введение

Биометрические технологии на данный момент являются передовым решением проблем идентификации граждан, так как основаны на идентификации человека по уникальным, присущим только ему биологическим признакам.

В настоящее время в мире продолжается поиск новых форм использования биометрических технологий [1].

НАЦИОНАЛЬНЫЕ ПРОЕКТЫ БРАЗИЛИЯ

В 1997 г. в Бразилии был подписан закон о создании единой системы регистрации. Программа находится на стадии реализации, прототип ID-карты с биометрическими данными уже есть, как и централизованная система идентификации по отпечаткам пальцев (АДИС⁹²).

В 2015 г. был анонсирован проект обеспечению 14 аэропортов Бразилии системами идентификации по лицу [2][3][4][5].

МЕКСИКА

В 2011 г. в Мексике началась программа выдачи электронных ID детям до 17 лет. В чипы этих ID-карт включаются сведения об отпечатках пальцев и радужной оболочке глаза.

В 2016 г. запущен пилотный проект по тестированию различных биометрических технологий (сканирование лица и сетчатки глаза) для оценки перспектив их использования на американско-мексиканской границе.

⁸⁹ Ефремов Егор Андреевич, студент, МГТУ имени Н. Э. Баумана, Москва, e.efremov2014@gmail.com

⁹⁰ Ершова Юлия Андреевна, студент, МГУ имени М. В. Ломоносова, Москва, ErshovaIA@spa.msu.ru

⁹¹ Чуфистов Александр Алексеевич, студент, МГТУ имени Н. Э. Баумана, Москва, mega.loool@inbox.ru

⁹² Автоматизированные дактилоскопические информационные системы (АДИС) – базы данных с возможностью создавать и хранить в электронном виде большие массивы дактилоскопической информации, производить по ним поиск с использованием папиллярных узоров пальцев (или ладоней) рук.

В 2016 г. французская технологическая компания Safran подписала пятилетний контракт с Национальным избирательным институтом, в рамках которого планируется усовершенствовать систему выборов в Мексике. Многие мексиканцы, живущие за границей, не могли голосовать на выборах без необходимости личного получения своей карты для голосования (не ранее чем за 90 дней до выборов). На выборах 2018 г. мексиканцы смогли голосовать при наличии Voter ID cards (электронная карта гражданина) [2].

ПЕРУ

С 2006 года в Перу начала работу электронная система подтверждения личности. Сейчас Национальный Реестр Идентификации и Гражданского статуса (RENIEC) выдает идентификационный документ (DNI) при рождении, который предоставляет доступ к медицинским, образовательным, банковским и другим услугам [6][7].

PKI инфраструктуру для создания, хранения и распространения цифровых сертификатов для выдачи электронного паспорта Перу разработала компания X Infotech. [8].

Первый биометрический загранпаспорт был выдан в конце февраля 2016 года. В настоящее время данные документы имеют более 50 уровней защиты.

КОЛУМБИЯ

С мая 2000 года выпускается текущий формат карты гражданства, основанный на технологии AFIS⁹³, которая позволяет автоматически проверять личность людей с помощью сравнения отпечатков пальцев.

С 1 января 2010 в Колумбии начал карта гражданства стала единственным документом, удостоверяющим личность гражданина.

Помимо карты гражданства в стране действует удостоверение личности, биометрический формат которого выполнен по аналогии с картой гражданства. Биометрический формат удостоверения личности несет на лицевой стороне двумерный штрих-код с биометрической информацией о владельце, что делает невозможным подделку документа. Он также включает в себя цветную фотографию, подпись, отпечаток пальца, место и дату рождения, место и дату выпуска, а также микротексты, радужную печать и защитную бумагу, которая обеспечивает более высокие стандарты неувязимости [9].

С сентября 2015 года граждане могут оформить биометрический заграничный паспорт.

ВЕНЕСУЭЛА

Венесуэла стала первой страной, которая стала выпускать биометрические паспорта в Латинской Америке. Первый паспорт был выпущен в июле 2007 года. RFID – чип внутри паспорта содержит фотографию владельца и его отпечатки пальцев.

⁹³ Automated Fingerprint Identification System

С 5 ноября 2018 года услугу выдачи биометрического паспорта можно оплатить с помощью местной криптовалюты.

УРУГВАЙ

Новая национальная идентификационная карта Уругвая, выпущенная 4 мая 2015 года, открывает путь к надежной онлайн-аутентификации и включает возможности для упрощения инициатив электронного правительства.

Карта eID, имея два чипа, может осуществлять взаимодействие с более чем 20 сайтами по всей стране [10].

Для выезда в Чили и Боливию граждане могут использовать идентификационную карту.

АНАЛИЗ НАЦИОНАЛЬНЫХ ПРОЕКТОВ

Выбор долгосрочной стратегии реализации программы электронной идентификации граждан оказывает сильное влияние на развитие информационных технологий в отдельно взятом регионе.

Проведем анализ технологий и возможностей, которые внедряются правительствами стран Латинской Америки. Для удобства введем ряд аббревиатур:

- ИОП – идентификация по отпечаткам пальцев;
- ИБПЛ – идентификация по биометрическим параметрам лица;
- ИСЧ – идентификация по сетчатке глаза;
- ИРОГ – идентификация по радужной оболочке глаза;
- ИМТ – идентификация с использованием мобильного телефона(смартфона);
- ПК – пограничный контроль;
- ЭДГУ – электронный доступ к государственным услугам;
- ДКИИ – доступ к критической информационной инфраструктуре;
- ЭДКУ – электронный доступ к коммерческим услугам;
- ЭЦП – возможность хранения и использования электронно-цифровой подписи;
- ДИП – доступ к избирательному праву.

Таблица 1. Используемые технологии в решениях электронной идентификации

Страна\Технология	ИОП	ИБПЛ	ИСЧ	ИРОГ	ИМТ
Бразилия	X	X		X	
Мексика	X			X	
Перу	X				
Колумбия	X				
Венесуэла	X				

Уругвай	X				
Чили	X	X			X

Таблица 2. Возможности средств электронной идентификации

Страна\Технология	ПК	ЭДГУ	ДКИИ	ЭДКУ	ЭЦП	ДИП
Бразилия	X		X			
Мексика	X		X	X		X
Перу	X	X	X	X		
Колумбия	X					
Венесуэла	X					
Уругвай	X	X	X	X	X	
Чили	X	X	X	X	X	

Выводы

Анализируя результаты реализации национальных программ электронной идентификации, стоит отметить опыт Перу, Уругвая и Чили, которые стремятся к повсеместному внедрению современных технологий. Данный подход открывает новые возможности для использования и глобализации технологий идентификации.

Взаимосвязь систем идентификации Уругвая, Чили и Боливии является важным шагом к глобализации. Создание единой международной идентификационной системы с стандартизированным форматом карты eID является важной задачей для мирового сообщества, так как позволит осуществлять быстрый обмен информацией между государствами и государственными органами, а также повысит уровень физической и информационной безопасности.

Литература

1. Обзор международного рынка биометрических технологий и их применение в финансовом секторе. [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf (дата обращения: 15.04.2019)
2. Минаев В.А., Вайц Е.В., Ефремов Е.А., Ковалевский А.Е. Безопасность и технологии электронной идентификации в странах Латинской Америки. // Вестник Российского нового университета. Серия «Сложные системы модели, анализ и управление». Выпуск 2/2019. С. 142 – 151.
3. Argotchno to offer Galitt payment system testing tools in Brazil [Электронный ресурс]. – Режим доступа: <https://www.biometricupdate.com/201808/argotchno-to-offer-galitt-payment-system-testing-tools-in-brazil> (дата обращения: 13.04.2019)
4. Zwipe, Thomas Greg & Sons do Brasil partner to develop and launch biometric payment cards [Электронный ресурс]. – Режим доступа: <https://www.biometricupdate.com/201904/zwipe-thomas->

- greg-sons-do-brasil-partner-to-develop-and-launch-biometric-payment-cards (дата обращения: 13.04.2019)
5. EyeLock and COMTEX Partner to Bring Iris Biometrics to Brazil and Latin America [Электронный ресурс]. – Режим доступа: <http://www.eyelock.com/index.php/media-details/91-news/178-eyelock-and-comtex-partner-to-bring-irisbiometrics-to-brazil-and-latin-america> (дата обращения: 15.04.2019)
 6. ID4D Country Diagnostic: Peru/ [Электронный ресурс]. – Режим доступа: <http://pubdocs.worldbank.org/en/245571518449918214/ID4D-diagnostic-report-Peru-101818.pdf> (дата обращения: 13.04.2019)
 7. Identification as a centerpiece for development: What can other countries learn from Peru? / [Электронный ресурс]. – Режим доступа: <https://blogs.worldbank.org/voices/identification-centerpiece-development-what-can-other-countries-learn-peru> (дата обращения: 13.04.2019)
 8. PKI решение для электронного паспорта Перу/ [Электронный ресурс]. – Режим доступа: <https://www.x-infotech.com/ru/pki-reshenie-dlya-yelektronnogo-pasporta-pe/> (дата обращения: 13.04.2019)
 9. UMANICK strengthens presence in Latin America with new office in Colombia [Электронный ресурс]. – Режим доступа: <https://www.biometricupdate.com/201612/umanick-strengthens-presence-in-latin-america-with-new-office-in-colombia> (дата обращения: 13.04.2019)
 10. Uruguay's eID card: Leading the way in Latin America [Электронный ресурс]. – Режим доступа: <https://www.gemalto.com/govt/customer-cases/uruguay-eid> (дата обращения: 16.04.2019)

Научный руководитель: Вайц Екатерина Викторовна, к.т.н., доцент кафедры ИУ10 «Защита информации» МГТУ имени Н.Э. Баумана, vaitcev@yandex.ru

Analysis of electronic citizens identification projects in Latin America **Egor Efremov⁹⁴, Yulia Ershova⁹⁵, Alexander Chufistov⁹⁶**

Abstract. The aggravation of the criminal situation in Latin America has led to the search for new technological solutions to the security problems of States and citizens. LA has become the largest market for biometric technologies. In the countries of LA, the identification by fingerprints is the most widespread among BT, the second most common is the set of biometric parameters of the face and the iris. The coverage of the BT identification of various areas of public life is as follows (in descending order): border control, critical infrastructure, the area of public and commercial services, digital signature, access to the election process. It is concluded that the experience of national implementation programs of electronic identification in LA countries indicates the growing international integration of BT identification, allowing to accelerate the exchange of information between States and improve the level of physical and information safety of countries and citizens.

Keywords: electronic identification, e-card, biometric technologies

⁹⁴ Egor Efremov, student, Informatics and Control systems department Bauman Moscow State Technical University, BMSTU, Moscow, e.efremov2014@gmail.com

⁹⁵ Yulia Ershova, student, School of public administration Lomonosov Moscow State University, Moscow, ErshovaIA@spa.msu.ru

⁹⁶ Alexander Chufistov, student, Informatics and Control systems department Bauman Moscow State Technical University, BMSTU, Moscow, mega.loool@inbox.ru

Анализ методов сбора событий информационной безопасности при использовании систем мониторинга событий информационной безопасности с применением технологий SIEM

Жиров П.В.⁹⁷

Проведен анализ существующих методов сбора событий информационной безопасности при использовании систем мониторинга событий информационной безопасности. Проведена оценка методов сбора событий информационной безопасности и выявлены их недостатки.

Ключевые слова: мониторинг, события информационной безопасности, SIEM-системы.

Введение

В настоящее время в организациях для автоматизации процессов, необходимых для выполнения поставленных задач, используются информационные системы. Их количество, а также качество ежегодно растет.

В информационных системах хранится, обрабатывается, а также циркулирует информация, нарушение свойств которой может нанести ущерб организации.

Правильный подход к реализации мероприятий, направленных на обеспечение конфиденциальности, доступности, а также целостности является важной составляющей в работе организации. При работе сотрудники организации часто не выполняют свои обязанности, в части выполнения регламентов по обращению с конфиденциальной информацией, тем самым создавая предпосылки для реализации угроз безопасности информации.

Таким образом, возникает необходимость контролировать действия сотрудников, в части выполнения регламентов по обращению с конфиденциальной информацией.

На сегодняшний день разработаны технические решения, направленные на мониторинг событий информационной безопасности, позволяющие выявлять, а также реагировать на инциденты информационной безопасности. Наиболее развивающимися являются системы мониторинга с применением технологий управления событиями и информационной безопасностью (Security In Information and Events Management – SIEM) [1-7]. Указанные системы обладают достаточно большим потенциалом по обнаружению угроз безопасности информации, а также выработке набора мер, позволяющего обеспечить требуемый уровень информационной безопасности.

Функционирование указанных систем заключается в оперативном сборе, хранении и аналитической обработке данных о событиях безопасности при помощи так называемых «агентов», которые в свою очередь формируются и фиксируются в системных журналах аппаратных, а также программных блоках информационной системы таких, как серверы, маршрутизаторы, межсетевые экраны, системы управления базами данных, системы обнаружения вторжений, антивирусы.

Объектом исследований является система мониторинга событий информационной безопасности с применением технологий SIEM. Данный выбор обусловлен тем, что использование данных систем является неотъемлемой частью мероприятий, направленных на обеспечение информационной безопасности. Применение систем мониторинга в международной практике не является новым направлением в области обеспечения

⁹⁷ Жиров Павел Валентинович, аспирант, ФГБОУ ВПО «МГТУ им. Н.Э. Баумана», Москва, Российская Федерация

информационной безопасности. Как показывает международный опыт порядок применения таких систем стандартизировано, так, например существует международный стандарт ИСО/МЭК ТО 18044:2004 «Информационные технологии. Финансовые услуги. Рекомендации по информационной безопасности» (ISO/IEC TR 18044:2004 «Information technology - Security techniques - Information security incident management»), который регламентирует управление инцидентами информационной безопасности в организациях [8, 9].

На сегодняшний день при мониторинге угроз безопасности информации становится все более актуальной задача выявления атак, уязвимостей и прочих действия нарушителя, направленных на нарушение работоспособности организации. Необходимо выявлять угрозы безопасности информации, не только на основе анализа событий безопасности, полученных с сетевой инфраструктуры информационной системы, но и на основании полученных данных из сети «Интернет». Выявление и реагирование на появление новых угроз безопасности информации на ранних этапах поможет снизить ущерб, нанесенный организации, в следствии их появления и реализации.

SIEM-системы на сегодняшний день имеют большое количество коммерческих реализаций. Для сравнения было решено проанализировать рынок SIEM-систем с целью определения их функциональных возможностей в области методов сбора событий информационной безопасности, необходимых для оценки инцидентов информационной безопасности. Анализ будет проводится для следующих систем мониторинга IBM Qradar, Security Capsule SIEM, HP ArcSight, MaxPatrol SIEM, КОМПАД.

Рассмотрим каждую из систем мониторинга.

IBM Qradar модульная система мониторинга угроз безопасности включающая в себе программные продукты, в том числе такие как IBM QRadar Advisor with Watson, IBM QRadar Log Manager, IBM QRadar Incident Forensics. IBM QRadar является инструментом по анализу безопасности информации, позволяет анализировать атаки по модели MITRE ATT&CK, поэтапно расследовать инциденты, анализируя локальную среду, анализировать для идентификации вероятных угроз и интеграции угроз, связанных с исходным инцидентом, включая вредоносные файлы, в том числе анализируя внешние неструктурированные данные, включая источники информации об угрозах, веб-сайты, форумы и многое другое, с применением технологий искусственного интеллекта. Принцип работы указанной системы заключается в «сниффинге» анализе трафика, циркулирующего в сети, что является недостатком при представлении отчетов, так как трафик, передаваемый в информационно-телекоммуникационной системе, не отражает в полной мере события информационной безопасности, по результатам которых можно оценить состояние информационной безопасности⁹⁸.

Security Capsule SIEM является отечественной программно-аппаратной системой мониторинга и корреляции событий информационной безопасности. Она представляет собой систему с модульной архитектурой, включающую в себя сервер сбора событий, сервер нормализации, сервер корреляции, сервер агрегации, консоль, агенты, тем самым мониторинг событий может осуществляться локально в территориально удаленных подразделениях, филиалах, дочерних и зависимых организациях. Указанная система позволяет анализировать события безопасности операционных систем, сетевых устройств, средств защиты информации, систем управления базами данных, антивирусных средств, а также прикладных программ и систем. Данная система построена на клиент-серверной архитектуре, а принцип работы системы заключается в опросе узлов сети при помощи протокола SNMP, а также собственного протокола, в том числе уже разработанных коннекторов для специализированных устройств, находящихся в системе [10]. Недостатком указанной системы является то, что при появлении новых программных и аппаратных

⁹⁸ <https://www.ibm.com>

устройств, которые необходимо будет внедрить в информационно-телекоммуникационную инфраструктуру, появляется необходимость в разработке новых коннекторов для полноценного функционирования системы мониторинга⁹⁹.

HP ArcSight модульная система мониторинга событий информационной безопасности, обеспечивающая сбор, обработку и хранение событий безопасности, которые могут поступать от различных источников. Данная информация собирается в едином центре, обрабатывается и подвергается анализу в соответствии с заданными правилами по обработке событий, связанных с информационной безопасностью. Результаты анализа в режиме реального времени предоставляются администраторам безопасности в удобном виде для принятия решений по реагированию на инциденты безопасности. Данная система поддерживает интеграцию с большим количеством программных и аппаратных решений, посредством уникального агента. Принцип работы, данной системы заключается в опросе коннекторов, установленных на узлах информационно-телекоммуникационной инфраструктуры. Учитывая изложенное, использование коннекторов в системе мониторинга является недостатком при сборе системой мониторинга событий информационной безопасности¹⁰⁰.

MaxPatrol SIEM является отечественной программно-аппаратной системой сбора, анализа и мониторинга событий безопасности из различных источников для защиты информационно-телекоммуникационной-инфраструктуры малого и среднего масштаба. Имеет предустановленные правила корреляции событий. На основании полной модели инфраструктуры выполняется автоматическое построение топологии сети, учитывающей конфигурации сетевых устройств вне зависимости от производителя. Принцип работы указанной системы заключается в установке агентов на узлы информационно-телекоммуникационной инфраструктуры и дальнейшем их опросе¹⁰¹.

КОМРАД является отечественной системой управления событиями информационной безопасности, которая позволяет выявлять и реагировать на события информационной безопасности. Данная система имеет возможность интеграции в информационную систему любого масштаба [6]. Принцип работы указанной системы заключается в установке на отдельные узлы в информационно-телекоммуникационной системе коннекторов, при помощи которых, осуществляется сбор событий информационной безопасности. Анализ этих событий осуществляется при помощи корреляционных правил, которые предустановлены в системе мониторинга¹⁰².

Особенности каждой из систем представлены в таблице 1.

Таблица 1.

Сравнение SIEM систем					
Критерии оценки	IBM Qradar	Security Capsule SIEM	HP ArcSight	MaxPatrol SIEM	КОМРАД
Метод сбора событий	Анализ трафика	Сетевые агенты	Коннекторы	Коннекторы	Коннекторы
Масштабируемость	Масштабируемые	Масштабируемые	Масштабируемые	Масштабируемые	Масштабируемые

⁹⁹ https://www.itb.spb.ru/products/Security_Capsule_SIEM/

¹⁰⁰ <http://arcsight-russia.ru/products-hp-arcsight/products-hp-arcsight>

¹⁰¹ <https://www.ptsecurity.com/ru-ru/products/mpsiem>

¹⁰² <https://npo-echelon.ru/production/65/11174>

Критерии оценки	IBM Qradar	Security Capsule SIEM	HP ArcSight	MaxPatrol SIEM	КОМРАД
Правила оценки событий	Применение технологий искусственного интеллекта	Настраиваемые правила	Настраиваемые правила	База правил	Предусмотренные правила

Учитывая изложенное, существующие на данный момент системы мониторинга событий безопасности с применением технологий SIEM имеют ряд недостатков.

В первую очередь это использование коннекторов для опроса узлов информационно-телекоммуникационной инфраструктуры ввиду того, что с каждым годом появляется всё более технологически развитое оборудование, вследствие чего возникнет необходимость разработки новых коннекторов.

В тоже время, существующие системы мониторинга используют для анализа событий информационной безопасности, только те события, которые происходят в информационно-телекоммуникационной инфраструктуре, что не позволяет своевременно реагировать на новые уязвимости, а также угрозы безопасности информации. Также недостатком системы мониторинга событий информационной безопасности являются методы оценки событий с помощью корреляционных правил, которые не всегда предустановлены в системе мониторинга, и для корректной работы системы их необходимо настроить, вследствие чего возникает необходимость иметь в организации квалифицированного специалиста для определения, указанных правил.

Литература

1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий. М.: ДМК Пресс, 2017. 224 с.
2. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. № 5 (24). С. 2-16.
3. Кузнецов А.В. Взаимосвязь процесса управления событиями с другими процессами управления предприятия // Вопросы кибербезопасности. 2017. № 5 (24). С. 17-22.
4. Кузнецов А.В., Ненашев С.М. Способ определения регистрируемых событий // Вопросы кибербезопасности. 2015. № 5 (13). С. 23-25.
5. Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80-81.
6. Петренко С.А., Цирлов В.Л. Импортзамещение решений IDS и SIEM // Защита информации. Инсайд. 2017. № 5 (77). С. 46-51.
7. Рыболовлев Д.А., Карасёв С.В., Поляков С.А. Классификация современных систем управления инцидентами безопасности // Вопросы кибербезопасности. 2018. № 3 (27). С. 47-53.
8. Котенко И.В., SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5 с 54-52.
9. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г // Вопросы кибербезопасности. 2013. № 1 (1). С. 61-64.
10. Графов С.А., Белявцев А.Ю., Воронов Д.А., Трофимов А.А. Грани SIEM // Защита информации. Инсайд. 2017. № 1 (73). С. 56-62.

Научный руководитель: Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н. Э. Баумана.
v.tsirlov@bmstu.ru

Analysis of Methods for Collecting Information Security Events When Using Information Security Event Monitoring Systems Using SIEM Technologies

Zhirova P.V.

The analysis of existing methods for collecting information security events using the information security event monitoring systems is carried out. The methods for collecting information security events were evaluated and their shortcomings were identified.

Keywords; monitoring, information security events, SIEM systems.

Реализация криптографических алгоритмов на ПЛИС

Жоголев Г.Д.¹⁰³

В настоящей статье рассматривается метод аппаратной реализации шифров, основанных на обобщенных клеточных автоматах. Исследуется способ реализации протокола передачи данных между ПК и ПЛИС, необходимый для приема и передачи входной и выходной последовательности шифра. Исследуются особенности реализации шифра и протокола передачи данных на ПЛИС Altera Cyclone 2 EP2C5T144C8N. Также рассматриваются некоторые публикации, исследующие реализации шифров на ПЛИС.

Ключевые слова: однородные структуры, ПЛИС, USB протокол, обобщенные клеточные автоматы

Введение

Впервые клеточные автоматы исследовались Фон Нейманом¹⁰⁴, Цузе и др. [1-3].

Клеточный автомат определяется следующим образом: некоторое пространство с ортонормированным базисом разобьем целочисленными координатными прямыми на ячейки [4].

Сопоставим каждой ячейке упорядоченное множество ячеек, которые будут считаться соседними с ней, множество будет состояться по одинаковому правилу для всех ячеек.

Сопоставим каждой ячейке множество значений (состояний), которые она может принимать, множество значений также одинаково для всех ячеек.

Одинаковым для всех ячеек будет и правило изменения состояния ячейки.

Для этой модели время будет течь дискретными шагами. Каждый такт ячейка, исходя из состояний ее соседей, будет вычислять свое значение для следующего такта работы системы.

Обобщенный КА – это ориентированный мультиграф $A = (V, E)$, здесь $V = \{v_1, \dots, v_N\}$ – множество вершин, а E – множество ребер. Каждой вершине v_i мультиграфа сопоставляется:

- 1) булева переменная m_i – ячейка
- 2) булева функция $f_i(x_1, \dots, x_n)$ – функция связи i -й вершины.

Каждой паре (v, e) , где v – вершина, e – инцидентное ей ребро, сопоставляется номер аргумента локальной функции связи.

Обобщенный клеточный автомат работает по шагам. В исходном состоянии его ячейки m_i заполнены начальными значениями. Следующее состояние вычисляется по формуле (1)

$$m_i(t) = f_i(m_{\mu(i,1)}(t-1), \dots, m_{\mu(i,n)}(t-1)) \quad (1)$$

где $m_{\mu(i,1)}$ – значение ячейки вершины $\mu(i, j)$, соседней данной вершине. $\mu(i, j)$ это номер вершины, из которой исходит ребро, входящее в вершину i , ребро имеет относительно этой вершины номер j .

Блочный шифр, основанный на обобщенных клеточных автоматах

Блочные шифры реализуются как схема Фейстеля, функция (2) реализует S-блоки.

$$S_c^A(key_i, x) = pr_m(F_A(x \parallel key \parallel c, r)), \quad (2)$$

Где $pr_m: B^* \rightarrow B^m$ функция, возвращающая младшие m элементов аргумента

$\parallel$ символ конкатенации,

r число шагов клеточного автомата,

A обобщенный клеточный автомат, c некоторая константа.

¹⁰³ Жоголев Глеб Денисович, студент, МГТУ им. Н.Э. Баумана, г. Москва, zhogolevg@mail.ru

¹⁰⁴ Дж. Фон. Нейман. Теория самовоспроизводящихся автоматов. Пер. с англ. М.: Мир, 1971. 326 с.

Раундовое преобразование блочного шифра определяется функциями (3), (4).

$$L_i = R_{i-1} \quad (3)$$

$$R_i = L_{i-1} \oplus S_{c_i}^A(key_i, R_{i-1}) \quad (4)$$

Где L_0 левая половина блока открытого текста,

i номер раунда,

R_0 правая,

соответственно L_i и R_i заполнения блоков после i -го раунда,

key_i раундовый ключ,

c_i константа.

Для реализации блочного шифра на ПЛИС выбран язык описания Verilog.

Особенности реализации протокола USB на ПЛИС

В данной статье исследуется аппаратная реализация данного протокола передачи данных на ПЛИС Altera Cyclone 2 EP2C5T144C8N. Необходимо обратить внимание, что на самых широко распространенных протоколах USB, таких, как 2.0, 3.0 и их модификациях, уровень сигнала может достигать 5 В, в то время, как максимальный сигнал, воспринимаемый входами данной ПЛИС, может достигать 3,3 В. Исходя из этого необходимо реализовать схему согласования уровней.

Реализована аппаратная часть протокола USB, схема согласования уровней. Остальная часть протокола, такая как кодирование NRZI, описаны на языке Verilog.

Выводы

Попытки исследования применимости клеточных автоматов в криптографии (в ГПСП) проводились еще в 80-х годах прошлого века Стивеном Вольфрамом [9-12], с теоретической точки зрения иностранные источники не предложили новых подходов к исследованию криптографических свойств КА, автор статьи [9] реализовал ГПСП на ПЛИС и провел анализ выходных последовательностей тестами NIST., в нашей стране дело обстоит лучше [5,6,8].

Реализация клеточных автоматов на процессорах затруднена, так как используется другая модель вычислений. Рассматривалась реализация блочных шифров, основанных на КА [8], производительность оказалась сравнимой с производительностью AES, DES и др. В работах [5, 6] изучается реализация ГПСП на ПЛИС. Алгоритмы, реализованные на ПЛИС, имеют высокое быстродействие.

Таким образом можно заключить, что реализация криптографических алгоритмов, основанных на КА, на ПЛИС имеет перспективы.

В данной статье исследованы особенности реализации алгоритма блочного шифрования на ПЛИС и протокола, осуществляющего передачу данных, поступающих на вход алгоритма шифрования и снимаемых с его выхода, на ПК.

Литература

1. Жоголев Г.Д. Клеточные автоматы в криптографии. В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 81-85.
2. Жуков А.Е. Клеточные автоматы в криптографии. Часть 1. //Вопросы кибербезопасности. 2017. № 3 (21). С. 70-76. DOI: 10.21681/2311-3456-2017-3-70-76
3. Жуков А.Е. Клеточные автоматы в криптографии. Часть 2. //Вопросы кибербезопасности. 2017. № 4 (22). С. 47-66. DOI: 10.21681/2311-3456-2017-4-47-66
4. Кудрявцев В.Б., Подколзин А.С., Болотов А.А. Основы теории однородных структур. - М.: Наука. Гл.ред. физ.-мат.лит., 1990. – 296 с. ISBN 5-02-01426602.
5. Сухинин Б.М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование, № 9, 2010. С. 34–41.

6. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. – 2010. – №2. – С. 34–41.
7. Richardson D. Tessellations with local transformations. Journal of Computer and System Sciences. – 1972, No 6, pp. 373–388.
8. Ключарёв П. Г. О производительности блочных шифров, основанных на клеточных автоматах, при их реализации на графических процессорах // Радиооптика. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 06. С. 24–34.
9. Wolfram S. Cryptography with Cellular Automata // Lecture Notes in Computer Science, vol. 218, 1986. Pp. 429–432.
10. Wolfram, S. (1983): Statistical mechanics of cellular automata. // Review of Modern Physics, 55, 601–644.
11. Wolfram S. Random Sequence Generation by Cellular Automata // Advances in Applied Mathematics, vol. 7, 1986. Pp. 429–432.
12. Wolfram S. Computation theory of cellular automata // Comm. Math. Phys., vol 96, 1984, pp 15–57.

Научный консультант - Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lebedevan@bmstu.ru

Implementation of cryptographic algorithms on FPGAs **Zhogolev G. D.**¹⁰⁵

This article considers the method of hardware implementation of ciphers based on generalized cellular automata. A method of implementing a data transfer Protocol between a PC and a FPGA, necessary for receiving and transmitting the input and output sequence of the cipher, is investigated. Features of implementation of the cipher and data transfer Protocol on FPGAs Altera Cyclone 2 EP2C5T144C8N are investigated some publications investigating implementations of ciphers on FPGAs are also considered.

Keywords: *homogeneous structures, FPGA, USB Protocol, generalized cellular automata*

¹⁰⁵ Gleb Zhogolev, student, Bauman Moscow State Technical University, Moscow, zhogolevg@mail.ru

О порядке одной перестановки на элементах квадратной матрицы

Жуков Д.А.¹⁰⁶

В работе исследуется перестановка элементов матрицы, обладающая специальным свойством локальности и вследствие этого достаточно просто реализуемая в таких распространенных параллельных архитектурах, как матричные сети процессоров, систолические массивы, ПЛИС и пр. Найдено точное аналитическое выражение длины ее периода. Показано, что асимптотически этот период отличается от периода наилучшей возможной перестановки относительно медленно растущим множителем.

Ключевые слова: период перестановки, клеточный автомат, вторая функция Чебышева, функция Ландау.

Введение

Среди современных тенденций развития как общей теории вычислений, так и стойких генераторов ключевого потока в частности [1], есть стремление к увеличению скорости работы устройства путем все большей и большей его параллелизации без увеличения тактовой частоты, что актуально и для низкоресурсной криптографии [2]. Одним из активно развивающихся направлений в этой области является использование в комбинирующем генераторе таких структур с локально-распределенной памятью, как клеточные автоматы [3,4] – как классических [5,6,7], так и обобщенных [8,9]. Двумерный клеточный автомат обычно описывается матрицей с функциями локальной связи ячеек.

Специальная перестановка элементов матрицы и ее свойства. Пусть a – матрица размера $n \times n$ с элементами $a[i][j]$, и пусть $a_0 = a$. Автор работы [10] предложил следующее преобразование элементов матрицы a :

$$a_{t+1}[i][j] = a_t \left[i + (-1)^j \cos \frac{\pi t}{2} \right] \left[j + (-1)^i \sin \frac{\pi t}{2} \right], \quad (1)$$

где строки и столбцы нумеруются вычетами от нуля до $n - 1$, сложение в индексах i, j также осуществляется по модулю n . Преобразование (1) выполняется за четыре раунда $t = 0, 1, 2, 3$ и переводит матрицу a_0 в некоторую матрицу a_4 , которая является перестановкой (см., напр., [11]) элементов исходной матрицы a_0 . Обозначим полученную перестановку на n^2 -элементном множестве через M .

Отметим, что каждый раунд преобразования (1) является локальным преобразованием, т.к. задает циклический сдвиг строк или столбцов матрицы a_t . В силу этого перестановка M особенно эффективно реализуется во всех моделях параллельных вычислений с локально-распределенной памятью [12,13], например, на матричной сети процессоров.

Возникает естественный вопрос о длине периода преобразования (1) по окончании раундов $t = 0, 1, 2, 3$, то есть о порядке перестановки M . Обозначим через $K(m)$ наименьшее общее кратное (НОК) всех первых натуральных чисел от 1 до m , а через $K_1(m)$ – НОК всех нечетных чисел из того же промежутка.

Теорема 1. Пусть n нечетно, тогда перестановка M разлагается в произведение простых независимых циклов длины $1, 3, 5, \dots, 2n - 1$, следовательно, ее порядок $\text{ord } M$ равен $K_1(2n - 1)$.

¹⁰⁶ Жуков Дмитрий Александрович, к.ф.-м.н., МГТУ им. Н. Э. Баумана, Москва, dzh05@inbox.ru

При нечетном n справедливы равенства $\sum_{i=1}^n (2i-1) = n^2$ и $K(n) = 2^s K_1(n)$, где $s = [\log_2 n]$, поэтому

$$\frac{K(2n-1)}{2n} < K_1(2n-1) < \frac{K(2n-1)}{n}. \quad (2)$$

Заметим, что $\ln K(m)$ – это вторая функция Чебышева. По теореме Валле-Пуссена (см., напр., [14])

$$\ln K(m) = m + O\left(e^{-c\sqrt{\ln m}}\right), \quad (3)$$

откуда с учетом неравенств (2) и теоремы 1 получаем

$$\ln \text{ord } M = \ln K_1(2n-1) \sim 2n \text{ при } n \rightarrow \infty. \quad (4)$$

Сравним теперь порядок нашей перестановки M с наибольшим возможным порядком перестановки из симметрической группы S_n . Обозначим через $l(m)$ максимальный порядок элементов группы S_m . Как известно [15], при растущем m выполнено асимптотическое равенство $\ln l(m) \sim \sqrt{m \ln m}$ (теорема Э.Ландау, 1902 г.), поэтому

$$\ln l(n^2) \sim n \sqrt{2 \ln n}. \quad (5)$$

Из сравнения асимптотик (4) и (5) вытекает, что $\ln \text{ord } M$ отличается от $\ln \text{ord } N$, где N – наилучшая возможная перестановка на элементах матрицы размера $n \times n$, лишь относительно небольшим множителем $\sqrt{\frac{\ln n}{2}}$.

Для проверки результатов данной работы была написана программа на C++ и проведены численные эксперименты, полностью подтвердившие теоретические выкладки.

Выводы

Перестановка, предложенная И. В. Матюшкиным на заседании общемосковского научного семинара «Математические методы обеспечения безопасности информации» в МГТУ им. Н. Э. Баумана в декабре 2018 г., имеет доказуемо большой порядок и при этом эффективную параллельную схемную реализацию, что позволяет использовать ее при подходящей фильтрующей функции для увеличения скорости работы генераторов ключей.

Литература

1. Zhukov A.E. Cryptographic primitives. – в кн. «Mathematical Foundations of Information Security» (ред. В.А. Матвеев). – М.: НИИ радиоэлектроники и лазерной техники МГТУ им. Н.Э. Баумана, 2014. – с. 145-194.
2. Zhukov A.E. Lightweight Cryptography: Modern Development Paradigms // Proceedings of the 8th International Conference on Security of Information and Networks, ACM Pub., 2015. – p. 7.
3. Жуков А.Е. Клеточные автоматы в криптографии. Часть 1 // Вопросы кибербезопасности, № 3 (21), 2017. – с. 70-76.
4. Жуков А.Е. Клеточные автоматы в криптографии. Часть 2 // Вопросы кибербезопасности, № 4 (22), 2017. – с. 47-66.
5. Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. № 2. С. 34-41.
6. Сухинин Б. М. О некоторых свойствах клеточных автоматов и их применении в структуре генераторов псевдослучайных последовательностей // Вестник МГТУ им. Н.Э. Баумана. Серия: Приборостроение. 2011. № 2. С. 68-76.
7. Матюшкин И.В., Жемерикин А.В., Заплетина М.А. Клеточно-автоматные алгоритмы сортировки строк и умножения целых чисел по схеме Атрубина. Известия вузов. Электроника, том 21, № 6, 2016, с.557-565.
8. Ключарёв П.Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 12. Режим доступа: <http://technomag.edu.ru/doc/517543.html>
9. Ключарёв П.Г. Об анализе блочных шифров, основанных на обобщенных клеточных автоматах // Сборник трудов Восьмой всероссийской научно-технической конференции «Безопасные информационные технологии» под ред. М.А.Басараба, 2017, с. 237-240.

10. Matyushkin I.V. Bridged quantum cellular automata based on Si/SiO₂ superlattices // World Academy of Science, Engineering and Technology. 2011. Т. 74. С. 329-334.
11. Чашкин А.В., Жуков Д.А. Элементы конечной алгебры: группы, кольца, поля, линейные пространства. М.: Изд-во МГТУ им. Н.Э.Баумана, 2016. - 368 с.
12. Воеводин В.В., Воеводин Вл.В. Параллельные вычисления. СПб.: БХВ-Петербург, 2002. - 608 с.
13. Миллер Р., Боксер Л. Последовательные и параллельные алгоритмы: общий подход. М.: БИНОМ. Лаборатория знаний, 2006. - 406 с.
14. Прахар К. Распределение простых чисел. М.: Мир, 1967. - 512 с.
15. Miller W. The maximum order of an element of a finite symmetric group // American Mathematical Monthly, vol.94, 1987, pp.497-506.

On the order of some matrix permutation

Dmitry A. Zhukov¹⁰⁷

Abstract. *In this work we find the exact formula and asymptotic behavior for order of some permutation on square matrix elements. This permutation has local property, which usefull in applications for parallel models, as FPGA and meshes.*

Keywords: *permutation order, cellular automata, second Chebyshev function, Landau function*

¹⁰⁷ Dmitry A. Zhukov, Ph.D., BMSTU, Moscow, dzh05@inbox.ru

Изучение булевых функций, имеющих аффинные аннигиляторы

Зеленецкий А.С.¹⁰⁸

Представлен новый алгоритм поиска аффинных аннигиляторов для заданной булевой функции. Введен новый класс булевых функций - функции, имеющие аффинные аннигиляторы, выведены верхняя и нижняя оценки мощности введенного класса. Получена связь минимальной степени ненулевого аннигилятора булевой функции от n переменных с минимальными степенями ненулевых аннигиляторов ее подфункций от $n-1$ переменной. Представлен алгоритм поиска расстояния от заданной функции до введенного класса, также находящий ближайшую функцию из класса. Выведена зависимость спектра булевой функции от ее расстояния до функций, которые аннигилируются аффинными функциями. Предложена модификация алгебраической атаки.

Ключевые слова: булева функция, аннигилятор, порядок алгебраической иммунности, аффинные функции, бент-функции, преобразование Уолша-Адамара.

Введение

В 2001 году Николя Куртуа (Nicolas T. Courtois) и Юзефом Пепшиком (Josef Pieprzyk) была предложена XSL-атака (алгебраическая атака)[1], суть этой атаки сводилась к поиску ненулевых аннигиляторов как можно более низкой степени для атакующей функции, либо для ее инверсии. Порядком алгебраической иммунности называется минимальная степень ненулевого аннигилятора функции, либо ее инверсии [2], [3].

В статьях [4], [5] были представлены и оценены некоторые алгоритмы поиска аннигиляторов булевой функции низкой степени. Асимптотическая сложность этих алгоритмов для поиска базиса пространства аннигиляторов, степень которых не превосходит d , была оценена как $O(w(f)(S_n^d)^3)$, где n – число переменных булевой функции, $w(f)$ - вес функции f , а $S_n^d = \sum_{i=0}^d \binom{n}{i}$.

Предлагается алгоритм поиска базиса пространства аффинных аннигиляторов булевой функции, который работает быстрее алгоритма, представленного в статье Баева. Предлагается модификация алгебраической атаки, которая концептуально состоит в совмещении стандартной алгебраической атаки и атаки с использованием линейных аналогов [6], [7].

Алгоритм поиска аффинных аннигиляторов:

Ищется базис пространства аффинных аннигиляторов для функции f , за g обозначим один из таких аннигиляторов. Алгоритм основан на разложении булевой функции по одной переменной [8]:

$$fg \equiv 0 \leftrightarrow (x_1 f_1 \oplus \bar{x}_1 f_2)(x_1 g_1 \oplus g_2) \equiv 0 \quad (1)$$

$$(x_1 f_1 \oplus \bar{x}_1 f_2)(x_1 g_1 \oplus g_2) \equiv 0 \leftrightarrow \begin{cases} f_1(g_1 \oplus g_2) \equiv 0 \\ f_2 g_2 \equiv 0 \end{cases} \quad (2)$$

Система (2) имеет решение тогда и только тогда, когда выполнено:

$$\begin{cases} f_1 g_2 \equiv 0 \\ f_2 g_2 \equiv 0 \\ f_1 \bar{g}_2 \equiv 0 \\ f_2 g_2 \equiv 0 \end{cases} \quad (3)$$

¹⁰⁸ Зеленецкий Алексей Сергеевич, МГТУ им. Н.Э.Баумана, Москва

За $Ann_1(f)$ обозначим пространство аффинных аннигиляторов функции f .

Доказано, что из (3) следует, что

$$Ann_1(f) = \langle (h_1 \| 1 \oplus h_1), (e_1 \| e_1), \dots, (e_r \| e_r) \rangle, \quad (4)$$

где h_1 – частное решение нижней системы из (3),

$$\langle e_1, \dots, e_r \rangle = Ann_1(f_1) \cap Ann_1(f_2), \quad (5)$$

под $(f_1 \| f_2)$, где $f_1, f_2 \in P_2(n-1)$, будем понимать функцию $f \in P_2(n)$, такую что $f(1, x_2, \dots, x_n) = f_2$, $f(0, x_2, \dots, x_n) = f_1$.

Как видно, можно найти базис пространства [9], [10] аффинных аннигиляторов функции, опираясь на знание базиса аффинных аннигиляторов для ее двух подфункций. Поэтому можно составить рекурсивный алгоритм поиска аффинных аннигиляторов.

Для того, чтобы нижняя система имела хотя бы одно решение, необходимо выполнение следующего условия:

$$f_1 f_2 \equiv 0. \quad (6)$$

Поэтому перед решением этой самой системы будет производиться проверка выполнения данного условия, что позволит во многих случаях даже не приступать к ее решению. Это связано с тем, что вероятность выполнения такого тождества при независимом выборе функций $f_1, f_2 \in P_2(n-1)$ равна $(0.75)^{2^{n-1}}$.

Ниже приведена таблица, в которой приведено среднее время работы представленного алгоритма и алгоритма, описанного в [4], на одних и тех же функциях от 8, 9, 10, 11, 12 переменных:

Число переменных:	Среднее время работы представленного алгоритма (сек.):	Среднее время работы классического алгоритма (сек.):	Число функций в выборке:
8	0.216433067321777	6.81829040288925	100
9	0.529947795867920	31.8801433897018	50
10	1.36027010917664	134.243654890060	25
11	4.0239213644	662.6623238325	15
12	20.2074489594	3829.13532495	5

Табл. 1 Сравнение времени работы алгоритмов.

Класс функций, имеющих аффинные аннигиляторы:

Введем класс функций от n -переменных, имеющих аффинные аннигиляторы, обозначим его как AA_n .

Справедлива оценка снизу его мощности:

$$|AA_n| \geq 2^{2^{n-1}} \quad (7)$$

также выведена нижняя граница мощности множества функций, НЕ имеющих аффинные аннигиляторы. Обозначим эту мощность за $|NA_n|$, тогда:

$$|NA_n| \geq 2|NA_{n-1}|(2^{2^{n-1}} - 1) - |NA_{n-1}|^2 \quad (8)$$

Отсюда следует верхняя оценка мощности класса AA_n .

Связь минимальной степени ненулевого аннигилятора функции с минимальными степенями ненулевых аннигиляторов ее подфункций:

Было доказано, что если k, d_1, d_2 – степень минимальных ненулевых аннигиляторов функций $f(x_1, x_2, \dots, x_n)$, $f(0, x_2, \dots, x_n)$, $f(1, x_2, \dots, x_n)$ соответственно, то справедливо следующее двойное неравенство:

$$\min\{d_1, d_2\} \leq k \leq \min\{d_1, d_2\} + 1 \quad (9)$$

Поиск расстояния от функции до AA_n и функции из AA_n , которая на этом минимальном расстоянии находится:

Представлен алгоритм решения данной задачи, основанный на полном переборе всех аффинных функций и побитовом умножении их на представленную функцию. После каждого такого умножения вычисляется вес произведения, происходит отбор по весу, ищется результат с наименьшим весом, его вес и будет искомым расстоянием, а сам результат, соответствующий минимальному весу, по координатно сложенный с заданной функцией, дает функцию из AA_n , которая находится на этом расстоянии. Сложность алгоритма асимптотически стремится к мощности множества аффинных функций. Таким образом, она равна $O(2^{n+1})$

Модификация алгебраической атаки:

Предлагается заменить анализируемую функцию на ближайшую к ней функцию из класса AA_n . Исходя из анализа предыдущего алгоритма, очевидно, что данная функция, назовем ее аналогом, будет отличаться от заданной функции только на тех наборах, на которых сама функция обращается в 1. Таким образом, из всех $\|f\|$ единиц будет ровно $d(f, AA_n)$ единиц, на которых функция f будет отличаться от своего аналога из AA_n , при “малом” $d(f, AA_n)/\|f\|$ уравнения вида $f(x) = 1$ заменяются на уравнения $g(x) = 0$, где $g \in A_n$ и аннигилирует аналог функции f .

Также предлагается искать аналог инверсии функции, в случае

$d(f + 1, AA_n)/\|f + 1\| < d(f, AA_n)/\|f\|$ вероятность успешного проведения атаки выше, чем в случае замены самой функции на ее аналог, в этой ситуации уравнения вида $f(x) = 0$ заменяются на уравнения вида $h(x) = 0$, где h аннигилирует аналог $f + 1$.

Связь спектра булевой функции и ее расстояния до класса AA_n :

Пусть дана линейная функция l степени 1, тогда расстояние между функцией f и ближайшим аннигилятором функции l будет высчитываться как:

$$d(f, Ann(l)) = \frac{\|f\| + W(l)/2}{2} \quad (10)$$

здесь $W(l)$ – преобразование Уолша-Адамара на векторе l . Также доказано:

$$d(f, Ann(l + 1)) = \frac{\|f\| - W(l)/2}{2} \quad (11)$$

Отсюда легко следует, что любая функция, имеющая аффинный аннигилятор, должна иметь в своем спектре коэффициент $2\|f\|$ или $-2\|f\|$.

Было доказано, что для любой бент-функции $\lim_{n \rightarrow \infty} \left(\frac{d(f, AA_n)}{\|f\|} \right) = 0.5$.

То есть никакая бент-функция не поддается модифицированной алгебраической атаке.

Вывод

Был разработан алгоритм, рассчитанный на поиск аффинных аннигиляторов, время работы которого меньше, чем классический способ поиска аннигиляторов низкой степени. Выведены оценки мощности класса функций, имеющих аффинные аннигиляторы. Предложена модификация алгебраической атаки на булевы функции. Доказано, что никакая бент-функция не поддается модифицированной алгебраической атаке.

Литература

1. Nicolas T. Courtois, Willi Meier Algebraic Attacks on Stream Ciphers with Linear Feedback. Extended Version of the Eurocrypt 2003 paper, August 24, 2003.
2. Логачев О.А., Сальников А.А., Смышляев С.В., Яценко В.В. Булевы функции в теории кодирования и криптологии. М.:ЛЕНАНД, 2015. с. 405 – 412
3. Таранников Ю.В. Комбинаторные свойства дискретных структур и приложения к криптологии. М.:МЦНМО, 2011. с. 129 – 136
4. Баев В.В. О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций, Дискрет. матем., 2006, том 18, выпуск 3, 138–151
5. Баев В.В. О сложности поиска аннигиляторов низкой степени для булевых функций. Материалы международной научной конференции по проблемам безопасности и противодействия терроризму, МГУ имени М.В.Ломоносова, 2-3 ноября 2005 г. М.: МЦНМО, 2006. с.198-204
6. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. М. : Изд-во ПАИМС, 2000.
7. Городилова А.А. От криптоанализа шифра к криптографическому свойству булевой функции. ПДМ 2016, № 3(33), 16–44
8. Пакратова И.А. Булевы функции в криптографии: учеб.пособие. – Томск: Издательский Дом Томского государственного университета, 2014.
9. Чашкин А.В., Жуков Д.А. Элементы конечной алгебры: группы, кольца, поля, линейные пространства. Москва: Издательство МГТУ им. Н.Э.Баумана, 2016.
10. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х томах. Том 1. М., 1998.

Научный руководитель: Жуков Дмитрий Александрович, доцент, кандидат физико-математических наук, МГТУ им. Н.Э.Баумана.

О вероятности одновременного осуществления нескольких событий при отсутствии условия независимости

Зуев Ю.А.¹⁰⁹

В вероятностном пространстве заданы n событий, имеющих одинаковую вероятность p . Какая-либо информация о корреляционных связях между событиями отсутствует, т.е. события рассматриваются как подмножества меры p в пространстве единичной меры. Рассматриваются вероятности одновременного осуществления всевозможных k событий из этих n . Среди всех C_n^k подмножеств мощности k выбираются подмножество, имеющее минимальную вероятность, и подмножество, имеющее максимальную вероятность. Найдены интервалы, в которых может находиться каждая из этих вероятностей.

Ключевые слова: событие, вероятность, линейное программирование.

Введение

Частотный анализ всегда был и продолжает оставаться одним из важнейших приёмов взлома шифров [1,2,3]. Вероятность его успеха зависит от вероятности событий, частота которых определяется. Слишком малая вероятность может потребовать для анализа недопустимо большого объёма доступного шифртекста. Анализируемые события зачастую нельзя считать независимыми, что не позволяет находить вероятность осуществления нескольких событий, перемножая соответствующие вероятности, как в случае независимости [4]. Это приводит к задаче оценки вероятности совместного осуществления заданного числа событий, отдельные вероятности которых известны, но которые нельзя считать независимыми.

Известным подходом к оценке вероятностей в этом случае являются неравенства Бонферрони [5]. Значительное число работ посвящено уточнению неравенств Бонферрони [6,7]. Однако для использования этих методов необходима информация о вероятностях совместного осуществления событий, т.е. знание корреляций между событиями, оценить которые на практике может оказаться затруднительно.

В настоящей работе эти вероятности оцениваются в достаточно общей постановке задачи, без использования какой-либо информации о корреляциях между событиями. Основным инструментом в получении оценок является теория линейного программирования [8]. Для того, чтобы не перегружать изложение слишком сложными формулами, получаемые в качестве оценок, вероятности событий выбраны равными, но используемые методы применимы и в общем случае.

Математическая постановка задачи

Дано, что в некотором вероятностном пространстве заданы n событий. Все события имеют одну и ту же вероятность p . Хорошо известно, что в том случае, когда события независимы, вероятность осуществления любых k из них одинакова и равна p^k . Условие независимости является в теории вероятностей стандартным и кладётся в основу большинства вероятностных моделей [9]. Однако во многих практических задач, при решении которых используются вероятностные модели, условия независимости в лучшем случае выполняются лишь приближённо. Если условия независимости не выполняются и

¹⁰⁹Зуев Юрий Анатольевич, д.ф.-м.н., профессор МГТУ им. Н.Э. Баумана, Москва, 79851965730@yandex.ru

между событиями допускаются корреляционные связи, то вероятности совместного осуществления для различных групп из k событий могут оказаться различными. В этом случае может возникнуть задача выбора k событий с максимальной вероятностью совместного осуществления или задача выбора k событий с минимальной вероятностью совместного осуществления. Тогда можно поставить вопрос о том, в каком диапазоне могут лежать данные вероятности. Разумеется, ответ на этот вопрос зависит от тех корреляционных связей, которые имеются между событиями. Обосновать наложение определённых связей достаточно трудно. Однако можно пойти по другому пути, не накладывая фиксированных корреляционных связей.

Если не накладывать каких-либо фиксированных корреляционных связей, то события следует рассматривать как произвольные подмножества меры p в множестве единичной меры, задающем вероятностное пространство. В этих условиях можно поставить задачу выбора группы из k событий с максимальной вероятностью совместного осуществления и из k событий с минимальной вероятностью совместного осуществления. Рассматриваемая мощность групп k может быть при этом любым числом от 2 до n .

Если X – произвольное подмножество из k событий, то через $\mathbf{P}(X)$ обозначим вероятность того, что все события из X осуществляются. Рассматриваемые экстремальные вероятности выразятся при этом как $\max_{X:|X|=k} \mathbf{P}(X)$ и $\min_{X:|X|=k} \mathbf{P}(X)$.

Основные результаты

Приведём основные результаты, полученные автором в [10].

Границы для $\min_{X:|X|=k} \mathbf{P}(X)$ задаются теоремой 1.

Теорема 1. Если в вероятностном пространстве задано множество из n событий, имеющих одинаковую вероятность p , то минимальная по всем C_n^k подмножествам X из k событий ($2 \leq k \leq n$) вероятность $\min_{X:|X|=k} \mathbf{P}(X)$ совместного осуществления всех событий из X лежит внутри следующих интервалов:

- 1) если $kp \leq k-1$, то $0 \leq \min_{X:|X|=k} \mathbf{P}(X) \leq p$;
- 2) если $kp > k-1$, то $kp - k + 1 \leq \min_{X:|X|=k} \mathbf{P}(X) \leq p$.

Границы для $\max_{X:|X|=k} \mathbf{P}(X)$ задаются теоремой 2.

Теорема 2. Если в вероятностном пространстве задано множество из n событий, имеющих одинаковую вероятность p , то максимальная по всем C_n^k подмножествам X из k событий ($2 \leq k \leq n$) вероятность $\max_{X:|X|=k} \mathbf{P}(X)$ совместного осуществления всех событий из X лежит внутри следующих интервалов:

- 1) если $np \leq k-1$, то $0 \leq \max_{X:|X|=k} \mathbf{P}(X) \leq p$;
- 2) если $k-1 \leq np < k$, то $\frac{np - \lfloor np \rfloor}{C_n^k} \leq \max_{X:|X|=k} \mathbf{P}(X) \leq p$;
- 3) если $k \leq np$, то $\frac{(\lfloor np \rfloor + 1 - np)C_{\lfloor np \rfloor}^k + (np - \lfloor np \rfloor)C_{\lfloor np \rfloor + 1}^k}{C_n^k} \leq \max_{X:|X|=k} \mathbf{P}(X) \leq p$.

Выводы

Автором впервые получены интервалы для возможных значений вероятностей совместного осуществления нескольких равновероятных событий при отсутствии какой-либо информации об их корреляции.

Эти оценки строго доказаны.

Методы их получения, основанные на теории линейного программирования, также, по-видимому, являются новыми и ранее в теории вероятностей не использовались. Полученные оценки справедливы для любых распределений, как дискретных, так и непрерывных, и являются точными, т.е. при выборе соответствующих распределений могут достигаться.

Приведённые оценки могут оказаться полезными в прикладных задачах, использующих вероятностные модели, в которых корреляционные связи между событиями неизвестны. А использованные при их получении методы могут быть применены и в других подобного рода задачах.

Литература

1. Kahn D. The codebreakers. NewYork: Scribner, 1996. 1151 p.
2. Шнайер Б. Прикладная криптография. М.: Триумф, 2003. 815 с.
3. Сمارт Н. Криптография. М.: Техносфера, 2005. 523 с.
4. Гнеденко Б.В. Курс теории вероятностей. 11-е изд. М.: URSS, 2015. 448 с.
5. Феллер В. Введение в теорию вероятностей и её приложения. Т. 1. М.: Мир, 1984. 448 с.
6. Зубков А.М. Неравенства для распределения числа одновременно происходящих событий // Обзорение прикладной и промышленной математики. 1994. Т. 1. Вып. 4. С. 638-666.
7. Фролов А.Н. Об оценивании вероятностей объединений событий с приложениями к лемме Бореля-Кантелли. // Вестник СПбГУ. Сер. 1. 2015. Т. 2(60). Вып. 3. С. 387-392.
8. Данциг Дж. Линейное программирование, его применения и обобщения. М.: Прогресс, 1966. 600 с.
9. Колмогоров А.Н. Основные понятия теории вероятностей. 5-е изд. М.: URSS. 2016. 120 с.
10. Зуев Ю.А. Об экстремальных вероятностях осуществления k из n событий // Прикладная дискретная математика. 2018. № 39. С. 5-12.

On joint probabilities of several events when independent conditions are absent

Zuev Yu. A.¹¹⁰

In probability space n events with the same probability p are determined. There is no information about correlations between the events and all events are considered simply as arbitrary subsets of measure p in the probability space of unit measure. For each subset X of of the set of n events such that $|X| = k$ the probability $P(X)$ of joint implementations of its k events is considered and extreme probabilities $\min_{X:|X|=k} P(X)$ and $\max_{X:|X|=k} P(X)$ are selected. In the paper the intervals for both probabilities $\min_{X:|X|=k} P(X)$ and $\max_{X:|X|=k} P(X)$ are obtained.

Keywords: event, probability, linear programming.

¹¹⁰ Yury Zuev, Dr.Sc., Professor of Bauman State Technical University, Moscow, 79851965730@yandex.ru

Протокол динамического управления маскированными каналами связи

Иванов И.И.¹¹¹

Аннотация: Разработан протокол динамического управления маскированными каналами связи, который предназначен для унификации метода передачи пакетов сообщений и динамического согласования параметров соединений в сетях связи, построенных на стеке протоколов TCP/IP с использованием Ethernet. Протокол обеспечивает формирование (установление, поддержание, управление и разрыв соединения) маскированного канала связи, по которому передается истинный (конструктивный) и ложный (маскирующий) трафик. Протокол разработан для двухточечных каналов связи, по которым передаются пакеты сообщений между двумя абонентами. Абоненты осуществляют равноправное информационное взаимодействие. Каждое двухточечное соединение обеспечивает одновременную двунаправленную работу в полнодуплексном режиме. Предполагается, что протокол динамического управления маскированными каналами связи будет использоваться для организации наложенной маскированной сети передачи данных поверх сети оператора связи. **Цель** исследования – определить способ формирования маскированных каналов связи и передачи служебных пакетов сообщений по ним. **Метод** исследования – обфускация состава, структуры и алгоритмов функционирования распределенных информационных систем в киберпространстве. **Результат** исследования – техническое решение по маскированию информационных систем, интегрированных с сетью связи общего пользования. Полученные результаты позволяют явно реализовывать меры защиты, направленные на формирование у нарушителей устойчивых ложных стереотипов об информационных системах и процессах управления, реализуемых с их помощью.

Ключевые слова: информационная безопасность, сетевая разведка, защита движущейся цели, динамическая структура, сетевые угрозы, маскирование, виртуальные частные сети.

1. Постановка задачи

В условиях ведения злоумышленником сетевой разведки (СР) и проведения компьютерных атак (КА) защита информационных систем (ИС) должна основываться не на обнаружении, а на предотвращении несанкционированных (деструктивных) воздействий [1–2]. Такой подход может быть реализован методом маскирования информационных направлений [3–8].

Разработан ряд способов маскирования структуры сети связи [9–15], которые реализуют метод маскирования и обеспечивают повышение защищенности информационных направлений информационных систем от СР и КА. Способы реализованы в виде программного средства MadNet – маскиратора информационных направлений ИС, который расширяет возможности сетевого стека операционных систем семейства GNU/Linux (например, VyOS). Маскиратор позволяет обеспечить защиту функционально-логической структуры ИС при передаче информации по каналам связи, имеющим выход за пределы контролируемой зоны, путем сокрытия реальных направлений информационного обмена в общем объеме трафика, циркулирующего между распределенными сегментами ИС [5, 16]. В результате сетевые идентификаторы (IP- и MAC-адреса) в перехваченных пакетах сообщений нельзя поставить в соответствие конкретному коммуникационному узлу защищаемой ИС, что снижает возможности СР по реконструкции структуры и КА на элементы ИС [8].

¹¹¹ Иванов Илья Игоревич, Краснодарское высшее военное училище, Краснодар, 7570745@mail.ru

Учитывая известные недостатки виртуальных частных сетей [18] и необходимость обеспечения масштабирования маскированных каналов связи [5, 7], в работе предлагается протокол динамического управления маскированными каналами связи, который позволит:

- использовать децентрализованное управление маскированными каналами связи для повышения отказоустойчивости информационного взаимодействия в ИС;
- обеспечить динамическое членство абонентов в маскированном канале связи для повышения масштабируемости ИС;
- снизить ресурсоемкость системы защиты.

Поэтому необходимо определить спецификацию протокола динамического управления маскированными каналами связи. Протокол позволит обеспечить формирование (установление, поддержание, управление и разрыв соединения) маскированного канала связи, по которому передается истинный (конструктивный) и ложный (маскирующий) трафик.

2. Описание протокола

Инкапсуляция протокола динамического управления маскированными каналами (Multi-Link Masked Topology Protocol, MMTP) требует кадрирования, чтобы ограничить начало и конец передаваемых блоков данных. Схема инкапсуляции данных протокола MMTP показана на рис.1, поля передаются слева направо. MMTP-сообщения инкапсулируются в Ethernet-кадр со специальным значением поля EtherType.

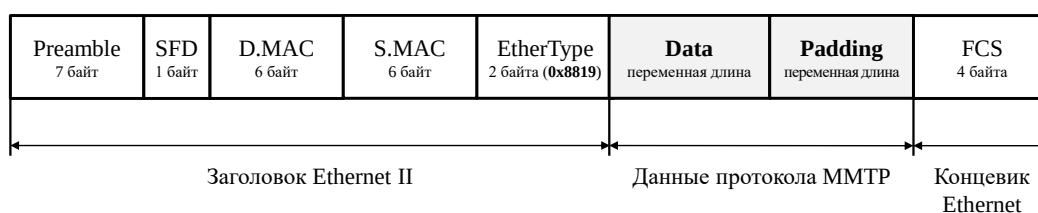


Рис.1. Схема инкапсуляции данных протокола MMTP

Поле Data может содержать один или более октетов с данными протокола MMTP. Максимальная длина поля Data (Maximum Receive Unit, MRU) составляет 1500 октетов. Допускается изменять MRU по согласованию на обоих концах двухточечного соединения. Поле Padding содержит произвольное число октетов для приведения (заполнения) длины данных протокола MMTP к MRU, если это необходимо (если размер передаваемых данных меньше, чем MRU).

3. Принцип работы протокола

Чтобы установить маскированное соединение стороны должны сначала обменяться MMTP-пакетами, чтобы согласовать параметры соединения (формат MMTP-пакета представлен на рис.2). После того как маскированное соединение установлено, стороны могут быть аутентифицированы.

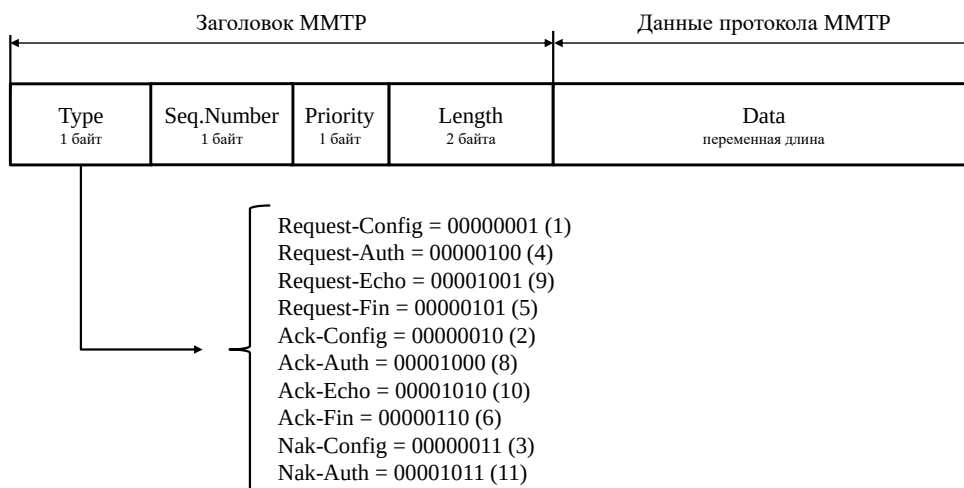


Рис.2. Формат MMTP-пакета

Маскированное соединение остается сконфигурированным до тех пор, пока не придет заключительный пакет Request-Fin или пока не произойдет какое-нибудь внешнее событие (отработает таймер неактивности или не вмешается администратор).

В процессе конфигурирования, удержания и завершения маскированного MMTP-соединения проходит через несколько определенных фаз, которые описывает схема, представленная на рис.3.

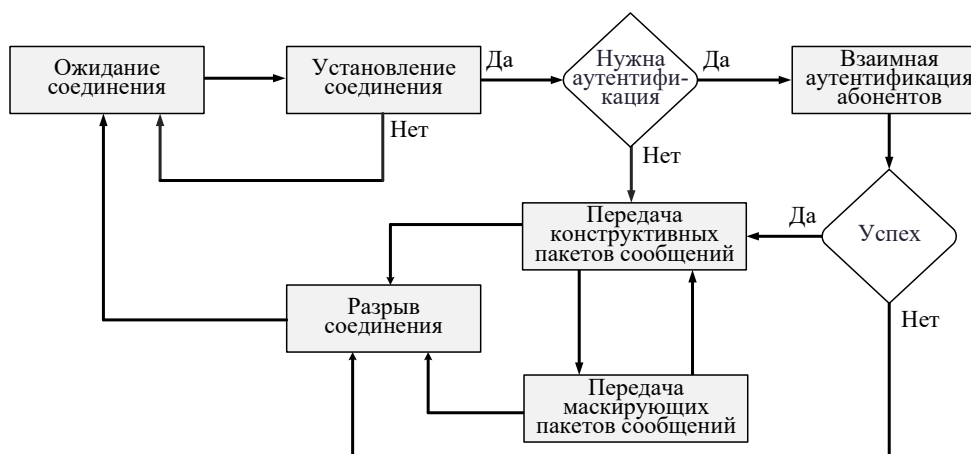


Рис.3. Схема перехода между фазами протокола MMTP

Рассмотрим фазы протокола MMTP.

3.1. Ожидание соединения

Телекоммуникационные узлы находятся в состоянии простоя, не принимают и не передают пакеты сообщений. Функции физического уровня маскирующего интерфейса отключены.

Соединение всегда начинается и кончается этой фазой. После инициализации функций физического уровня маскирующего интерфейса администратором для локального и удаленного телекоммуникационного узла они переходят в фазу установления соединения.

3.2. Установление соединения

Телекоммуникационные узлы обмениваются служебными пакетами сообщений для инициализации и согласования параметров маскированного канала (рис.4).

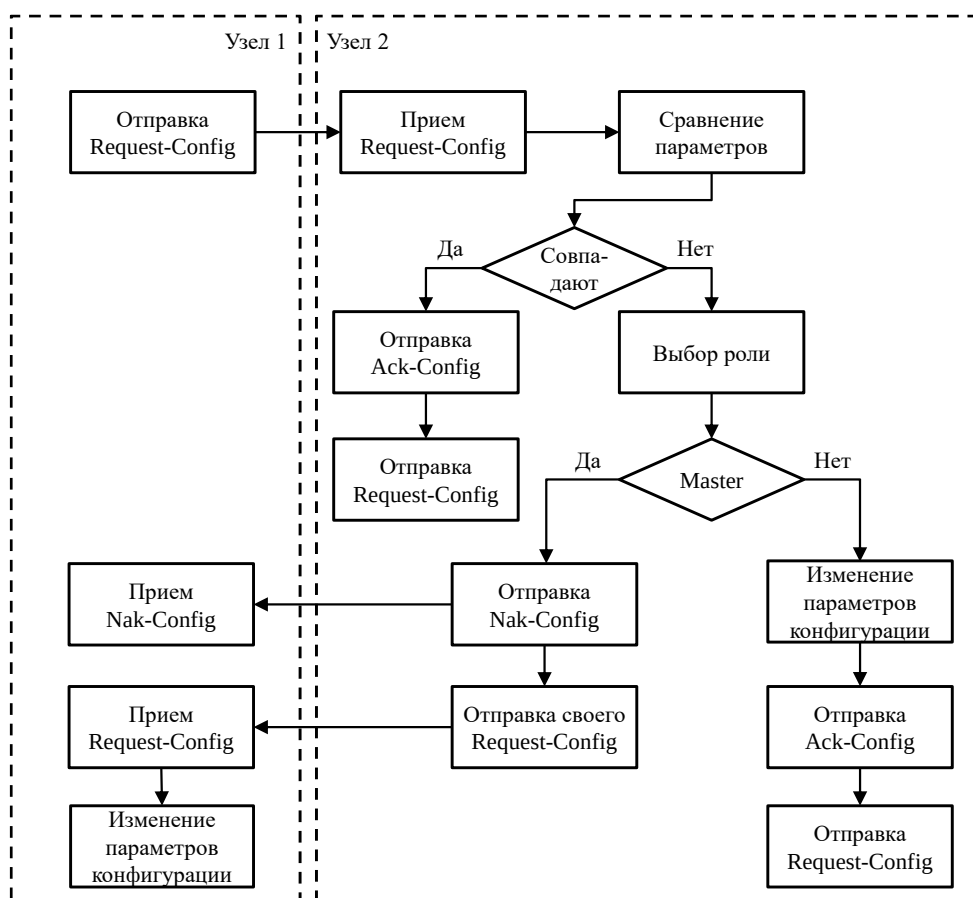


Рис.4. Схема согласования топологии при установлении соединения

Для установления маскированного соединения производится обмен пакетами Request-Config, Ack-Config, Nak-Config. Все конфигурационные параметры, передаваемые в пакетах Request-Config, Ack-Config, Nak-Config, должны устанавливаться сетевым администратором. Любые типы MMTP-пакетов, кроме Request-Config, Ack-Config, Nak-Config, полученные в течение фазы установления соединения должны быть отброшены.

3.3. Взаимная аутентификация абонентов

Телекоммуникационные узлы обмениваются служебными пакетами сообщений для согласования параметров аутентификации.

В некоторых случаях желательно запросить удаленный узел аутентифицировать себя. По умолчанию, аутентификация не обязательна. Аутентификацию следует проводить сразу после установления маскированного соединения. Если аутентификация неудачна, следует перейти к фазе разрыва соединения. В фазе взаимной аутентификации может происходить обмен следующими MMTP-пакетами: Request-Auth, Ack-Auth, Nak-Auth. Любые типы MMTP-пакетов, кроме Request-Auth, Ack-Auth, Nak-Auth, полученные в течение этой фазы

должны быть отброшены. Фазу взаимная аутентификация абонентов следует считать неудачной и выполнять переход в фазу разрыв соединения только при превышении некоторого числа попыток.

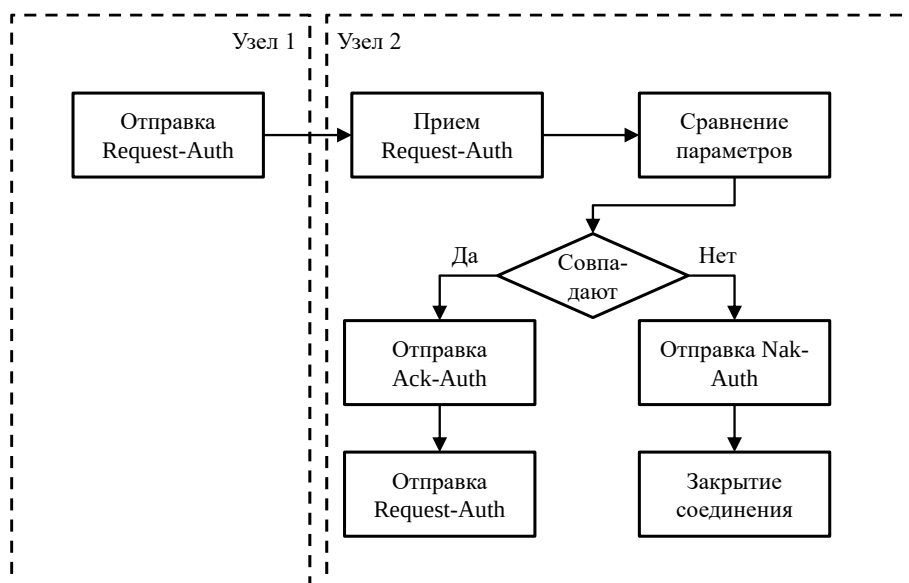


Рис.5. Схема взаимной аутентификации абонентов

3.4. Передача пакетов сообщений

Телекоммуникационные узлы выполняют формирование, передачу и прием потоков данных конструктивного трафика по установленному маскированному каналу связи. При отсутствии конструктивного трафика телекоммуникационные узлы выполняют формирование, передачу и прием потоков данных маскирующего трафика по установленному маскированному каналу связи.

3.5. Разрыв соединения

Телекоммуникационные узлы обмениваются служебными пакетами сообщений для разрыва соединения. Разрыв соединения происходит под воздействием ошибок канала связи либо инициируется администратором.

ММТР может завершить маскированное соединение в любое время. Это может произойти потому, что потеряна связь, произошел сбой аутентификации, ухудшилось качество соединения, истек период бездействия или маскированное соединение закрыто администратором.

Для закрытия ММТР-соединения использует обмен пакетами Request-Fin и Ack-Fin. Когда маскированное соединение закрыто, ММТР должен сообщить сетевому уровню операционной системы, что необходимо вернуться к штатному функционированию телекоммуникационного узла.

Отправителю пакета Request-Fin следует отключиться после получения пакета Ack-Fin или по истечении таймера Restart. Получателю пакета Request-Fin следует ждать отключения удаленной стороны и он не должен отключаться пока не пройдет как минимум один интервал таймера Restart после отправки Ack-Fin.

После закрытия MMTP-соединения следует перейти в фазу ожидания соединения. Любые типы MMTP-пакетов, кроме Request-Fin и Ack-Fin, полученные в течение фазы закрытия соединения должны быть отброшены.

4. Форматы служебных пакетов

Существует три типа служебных пакетов, используемых MMTP:

конфигурационные пакеты, которые используются для установления соединения и согласования параметров аутентификации (Request-Config, Ack-Config, Nak-Config, Request-Auth, Ack-Auth, Nak-Auth);

пакеты завершения соединения (Request-Fin и Ack-Fin);

пакеты обслуживания соединения (Request-Echo, Ack-Echo).

Формат MMTP-пакета представлен на рис.2. Принадлежность MMTP-пакета к одному из указанных типов определяется значением поля Type. Поле Type имеет длину один октет и идентифицирует тип MMTP пакета (рис.2).

Поле Sequence Number имеет длину один октет и используется для согласования номеров запросов и ответов. Когда получен пакет с неверным полем Sequence Number, пакет должен отбрасываться.

Поле Priority используется при выборе роли узла в информационном взаимодействии. Доступные в MMTP роли телекоммуникационных узлов: Master (ведущий) или Slave (ведомый). Роль узла выбирается на основе сравнения поля Priority: узел с большим значением в поле становится ведущим.

Поле Length состоит из двух октетов и показывает длину MMTP-пакета. Значение поля Length не должно превышать установленное значение MRU. Октеды за пределами диапазона, заданного полем Length трактуются как заполнение (padding) и игнорируются при приеме пакета. Если поступает пакет с неверным значением поля Length, то он должен отбрасываться.

Поле Data имеет один или большее число октетов, в соответствии со значением поля Length. Формат поля Data зависит от типа MMTP-пакета (значения в поле Type).

Выводы

Для противодействия несанкционированным (деструктивным) воздействиям злоумышленника разработан метод маскирования информационных направлений информационных, который позволяет добиться защищенного функционирования ИС. При маскированном информационном обмене злоумышленник будет принимать решения в условиях неопределенности обстановки, а планы управления и технологические процессы будут искажены либо скрыты. Это позволяет существенно повысить безопасность функционирования ИС путем введения в заблуждение злоумышленника относительно ее структуры: количество хостов, версии программного обеспечения и службы.

В работе представлен новый подход к построению маскированных каналов связи, который позволит исключить недостатки традиционных сервисов виртуальных частных сетей: повысить отказоустойчивость, гибкость и масштабируемость. Первоначальная реализация представленной в работе системы демонстрирует низкие требования к аппаратной составляющей коммуникационного оборудования и требует незначительных изменений в структуре операционных систем семейства GNU/Linux [19, 20].

В работе представлена спецификация протокола динамического управления маскированными каналами связи. Практическое подтверждение и достоверность предлагаемого решения подтверждается патентами РФ на изобретения [9–15].

Литература

1. Выговский Л.С., Максимов Р.В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости СПбГПУ. 2009. № 1 (72). С. 181-187.
2. Максимов Р.В., Савинов Е.А. Оценка живучести распределенных интегрированных информационных систем / В сборнике: Информационные технологии и нанотехнологии (ИТНТ-2016). Материалы Международной конференции и молодежной школы. Самарский государственный аэрокосмический университет имени академика С.П. Королева (национальный исследовательский университет); Институт систем обработки изображений РАН. 2016. С. 431-438.
3. Максимов Р. В., Соколовский С. П., Шарифуллин С. Р., Чернолес В. П. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. № 3 (233). С. 28-35.
4. Ворончихин И. С., Иванов И. И., Максимов Р. В., Соколовский С. П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 92–101. DOI: 10.21681/2311-3456-2019-6-92-101.
5. Maximov R. V., Ivanov I. I., Sharifullin S. R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). (Moscow, 6-7 December 2017) – Moscow, Bauman Moscow Technical University, 2017. P. 83-87.
6. Максимов Р. В., Соколовский С. П., Орехов Д. Н. Особенности детектирования и способы маскирования демаскирующих признаков средств проактивной защиты вычислительных сетей // Радиолокация, навигация, связь: Сборник трудов XXIV Международной научно-технической конференции. Том 2. – Воронеж: ООО «Вэлборн», 2018. С. 169-179.
7. Максимов Р.В., Иванов И.И. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях / Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 11-12 октября 2017 года, – СПб.: ВАС, 2017 – 357 с.
8. Шерстобитов Р. С., Шарифуллин С. Р., Максимов Р. В. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 136-175. URL: <http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf> (дата обращения 14.10.2019).
9. Максимов Р.В., Иванов И.И., Лыков Н.Ю., Шарифуллин С.Р. Способ маскирования структуры сети связи // Патент на изобретение RU 2656839, опубл. 06.06.2018, Бюл. № 16.
10. Максимов Р.В., Голуб Б.В., Лыков Н.Ю., Краснов В.А. Способ маскирования структуры сети связи // Патент на изобретение RU 2017110366, опубл. 28.09.2018, Бюл. № 28.
11. Максимов Р.В., Иванов И.И., Шарифуллин С.Р., Мирошниченко Е.Л. Способ маскирования структуры сети связи // Патент на изобретение RU 2016124953, опубл. 26.12.2017, Бюл. № 36.
12. Максимов Р. В., Кожевников Д. А., Павловский А. В., Юрьев Д. Ю. Способ выбора безопасного маршрута в сети связи (варианты) // Патент на изобретение RU 2331158, опубл. 10.08.2008, Бюл. № 22, 34 с.
13. Максимов Р. В., Берест П. А., Богачев К. Г., Выговский Л. С., Игнатенко А. В., Кожевников Д. А., Краснов В. А., Кузнецов В. Е. Способ сравнительной оценки структур информационно-вычислительной сети // Патент на изобретение RU 2408928, опубл. 10.01.2011, Бюл. № 1, 16 с.
14. Максимов Р. В., Андриенко А. А., Куликов О. Е., Костырев А. Л., Павловский А. В., Лебедев А. Ю. Способ контроля информационных потоков в цифровых сетях связи // Патент на изобретение RU 2267154, опубл. 27.12.2005, бюл. № 36, 16 с.
15. Максимов Р. В., Андриенко А. А., Кожевников Д. А., Колбасова Г. С., Павловский А. В., Стародубцев Ю. И. Способ (варианты) и устройство (варианты) защиты канала связи вычислительной сети // Патент на изобретение RU 2306599, опубл. 20.09.2007, Бюл. № 26, 56 с.
16. Iskolnyy B. B., Maximov R. V., Sharifullin S. R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). (Moscow, 6-7 December 2017) – Moscow, Bauman Moscow Technical University, 2017. P. 59-65.

17. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50-99. DOI: 10.24411/2410-9916-2019-10403.

18. Марков А.С., Горшков Ю.Г., Матвеев В.А., Цирлов В.Л. Современные тренды в области кибербезопасности / Безопасные информационные технологии. Сборник трудов Седьмой всероссийской научно-технической конференции / под. ред. В.А. Матвеева. – М.: МГТУ им. Н.Э. Баумана. – С. 138-142.

19. Лыков Н.Ю., Шарифуллин С.Р., Иванов И.И. Результаты экспериментов по управлению демаскирующими признаками виртуальных частных сетей / Технические и технологические системы: Материалы девятой Международной научной конференции «ТТС-17» (22–24 ноября 2017 года) / ФГБОУ ВО «КубГТУ», КВВАУЛ им. А.К. Серова; под общей редакцией Б.Х. Гайтова. – Краснодар: издательский Дом – Юг, 2017. – 250с.

20. Лазарев А.А., Лыков Н.Ю., Иванов И.И. Результаты эксперимента по тестированию функциональных возможностей макета маскировщика информационной системы / Информатика: проблемы, методология, технологии: сборник материалов XVIII международной научно-методической конференции: в 7 т. / под редакцией Н. А. Тюкачева; Воронеж, Воронежский государственный университет, 8–9 февраля 2018 г. – Воронеж: Издательство «Научно-исследовательские публикации» (ООО «Вэлборн»), 2018. – Т. 4. – 268 с.

Научный руководитель: Максимов Роман Викторович, д.т.н., профессор, профессор Краснодарского высшего военного училища имени генерала армии С.М. Штеменко, Краснодар, rvmxim@yandex.ru.

Multi-Link Masked Topology Protocol

Ivanov I.I.¹¹²

Abstract. *Multi-Link Masked Topology Protocol is developed. The protocol is used for defining transmission method and dynamic negotiation method of masked link parameters in TCP/IP networks. The protocol provides establishment of a masked links for transmission true (constructive) and false (masking) traffic. The protocol is developed for point-to-point links. The protocol is used for dynamic control of masked links and overlay network secure interconnection. The purpose of the study is to define the method for establishing masked links and the method for transmitting service packets over this links. The research method is network structure obfuscation in cyberspace. The result of the study is a software solution for masking information system interconnection.*

Keywords: *cyber-security; security threats; obfuscation; network intelligence; dynamic topology; software-defined networks; network security management; secure interconnection, virtual private network.*

¹¹² Ivanov Ilya Igorevich, Krasnodar Higher Military School, Krasnodar, Russia, 7570745@mail.ru

Симметричный блочный алгоритм шифрования данных «ВС-2» Капалова Н.А.¹¹³, Хаумен А.¹¹⁴

Аннотация. В статье речь идет об алгоритме шифрования данных, основанном на SP - сети. Описаны основные свойства алгоритма шифрования ВС-2 и преобразования, которые входят в состав алгоритма. Представлены основные дифференциальные свойства, выявленные для S-блок алгоритма а. Эти свойства могут быть использованы для анализа с помощью таких методов, как дифференциальный криптоанализ и метод невозможных дифференциалов.

Ключевые слова: схема алгоритма шифрования, линейное преобразование, SP-сеть, S-блок подстановок, дифференциальные свойства.

Введение

В институте информационных и вычислительных технологий по руководством Р.Бияшева создан симметричный блочный алгоритм шифрования данных. Алгоритм был назван «ВС-2» (сокращенное от слова BlockCipher).

Алгоритм шифрует данные блоками по 256 бит, длина ключа составляет 512 бит. Структура алгоритма приведены в следующем рисунке (Рис.1).

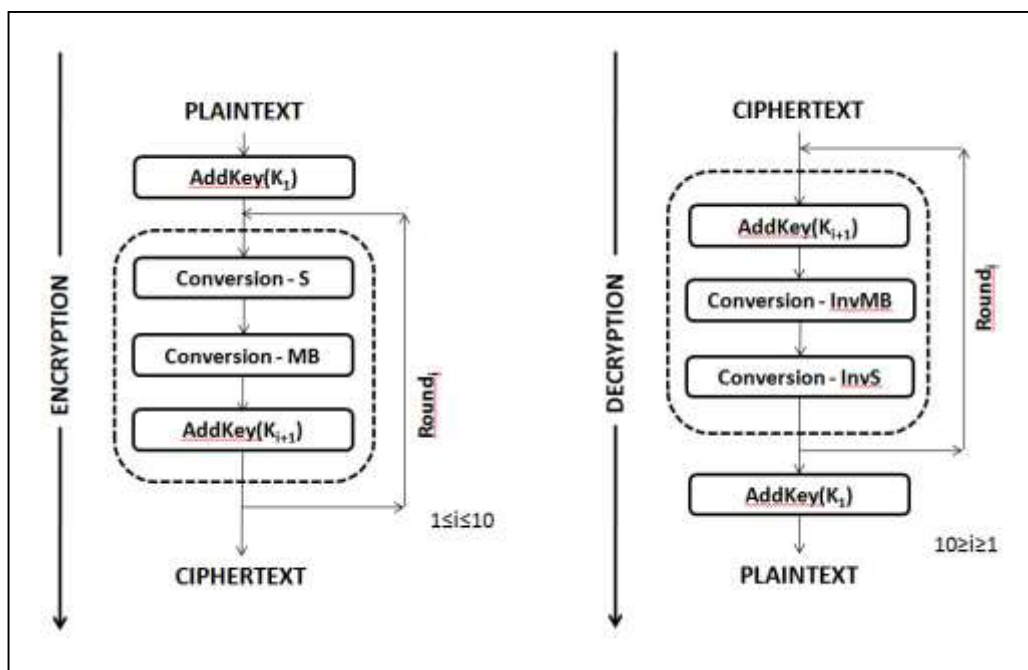


Рис.1. Общая схема алгоритма ВС-2

Алгоритм ВС-2 разработан на основе SP-сети. Использование SP-сети позволяет выполнить преобразования над всем входным блоком целиком, а не только над его половиной [1].

Процесс шифрования состоит из нескольких раундов, каждый из которых включает в себя несколько преобразований, а именно три:

¹¹³ Капалова Нурсулу Алдажаровна, к.т.н., Институт информационных и вычислительных технологий КН МОН РК, г.Алматы, nkaralova@mail.ru.

¹¹⁴ Хаумен Арманбек, Институт информационных и вычислительных технологий КН МОН РК, г.Алматы, haumen.armanbek@mail.ru.

- *AddKey* – сложение по модулю 2 (xor) с раундовым ключом;
- *Conversion-S* – замена с помощью таблиц подстановок;
- *Conversion-MB* (MixBlock) – линейное преобразование.

Количество раундов шифрования 10. В каждом раунде над шифруемыми данными поочередно выполняются перечисленные выше преобразования (рис. 1).

Процесс шифрования

Алгебраически шифротекст C зависит от открытого текста A следующим образом:

$$C = X(MB(S(A))).$$

Входной 256-битовый блок алгоритма шифрования представляется в виде последовательности 32 байтов, как элементы поля Галуа $F=GF(2^8)$, которые нумеруются справа налево, начиная с нуля:

$$A = a_{31}, a_{30}, a_{29}, \dots, a_1, a_0.$$

Раундовый ключ для шифрования состоит из 256 битов, которые тоже представляются в виде последовательности 32 байтов:

$$K_j = k_{j31}, k_{j30}, k_{j29}, \dots, k_{j1}, k_{j0}, \text{ где } j - \text{номер раунда.}$$

Первым выполняется операция наложения первого раундового ключа на входной блок с помощью операции *побитового сложения* (xor).

$$b_i = a_i \text{ xor } k_i, \quad i = \overline{0, 31}$$

Затем идут раундовые преобразования, состоящих из трех преобразований.

Преобразование S

Нелинейное преобразование алгоритма BC-2 использует операции с байтами. К каждому байту применяется нелинейная, биективная *подстановка*, задаваемая одномерным массивом, состоящих из 256 элементов.

256-битный блок данных поступает на вход преобразования S, и разбивается на 32 байтов. Каждый байт входного блока – это индекс значения, находящегося в таблице подстановок. Таким образом, на выходе преобразования S будет набор байтов, находящихся по соответствующим индексам в заданной таблице подстановок.

$$c_i = S[b_i], \quad i = \overline{0, 31}$$

Для выходного блока в целом нелинейная *подстановка* может быть определена как

$$S(B) = S(b_{31} || \dots || b_0) = S(b_{31}) || \dots || S(b_0).$$

Далее этот блок подается на вход линейного преобразования MB, в котором блок разбивается на 32 байта.

Преобразование MB

Это линейное преобразование алгоритма BC-2. Преобразование **MB** (MixBlock) перемешивает байты в блоке.

Преобразование **MB** осуществляется следующим образом:

1. Каждый байт в блоке умножается на соответствующий ему коэффициент на поле $GF(2^8)$ по модулю $x^8 + x^4 + x^3 + x^2 + 1$. Коэффициенты являются элементами блока-констант C . После операции умножения выполняется операция сложения всех 32-х байтов между собой по модулю 2 (битовое сложение).

2. Полученное число записывается 32-ым байтом, а все остальные байты сдвигаются на один байт вправо, тем самым вытесняя самый крайний правый байт. Подобные расчеты проводятся 32 раза, в результате получаем новое 32-х байтное значение(Рис. 2).

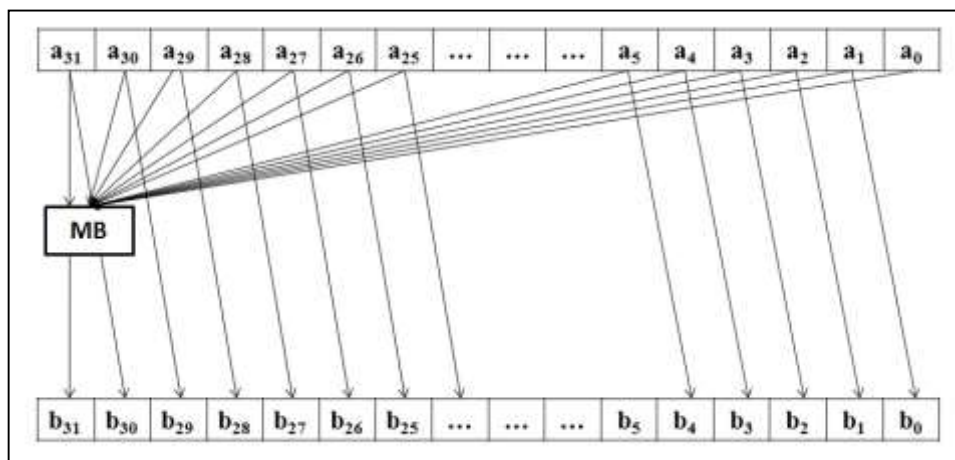


Рис.2. Схема линейного преобразования MB

Блок-констант **C** состоит из 32 элементов.

$C(32) = (17, 39, 191, 203, 67, 173, 43, 197, 61, 13, 59, 131, 227, 7, 101, 83, 41, 149, 71, 127, 19, 137, 113, 53, 157, 241, 73, 181, 223, 109, 157, 23)$.

Преобразование X (AddKey)

Это преобразование добавляет раундовые ключи входной блок с помощью операции побитового сложения.

Так выполняется один раунд зашифрования. Остальные 9 раундов выполняются абсолютно аналогично. После сложения по модулю два с последним раундовым ключом мы получаем шифртекст.

Генерация раундовых ключей

Раундовые ключи получаются путем определенных преобразований на основе мастер-ключа, длина которого, составляет 512 бит. Этот процесс начинается с разбиения мастер-ключа пополам, так получается первая пара раундовых ключей. Для генерации каждой последующей пары раундовых ключей применяется десять итераций сети Фейстеля, в каждой итерации используется функции преобразования **S**, **MB** и **ROL**. Преобразование **S** и **MB** использовались для шифрования байтов блока и преобразование **ROL**—есть циклический сдвиг битов блока налево на одну позицию.

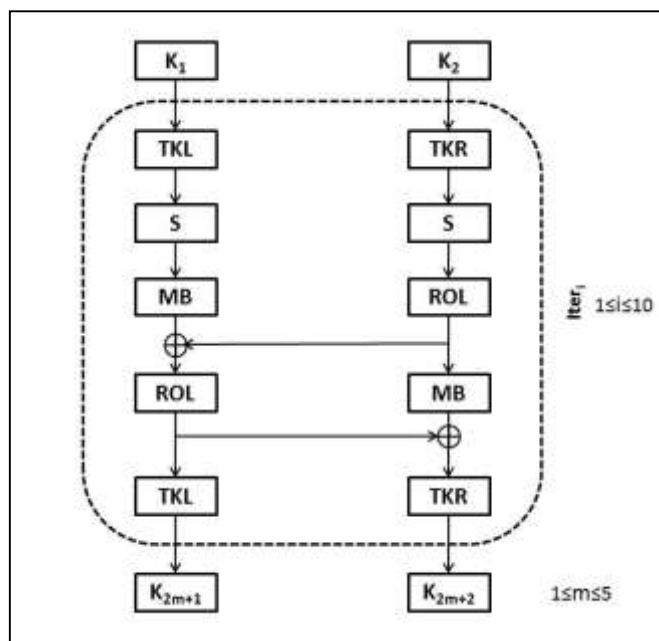


Рис.3. Схема генерации раундовых ключей

Процесс расшифрования

Операция расшифрования выполняется по такому же принципу, но в обратном порядке и с использованием раундовых преобразований, инверсных к тем, что использовались при зашифровании.

Алгебраически открытый текст A зависит от шифротекста C следующим образом:

$$A = \text{InvS}(\text{InvMB}(X(C))).$$

Conversion $\text{InvMB} = \text{MB}^{-1}$ – это обратное к линейному преобразованию для блока.

Conversion $\text{InvS} = S^{-1}$ – это обратная таблица подстановок байтов в блоке.

Дифференциальные свойства S-блока

В ходе разработки алгоритма BC-2 были исследованы дифференциальные свойства S-блока подстановок данного алгоритма. Для анализа использован алгоритм анализа S-блока ГОСТ 28147-89 [2].

Сначала нам необходимо составить таблицу для блока подстановок S , строки которой содержат входные значения ΔA в блок подстановок, а столбцы – соответствующие значения ΔC , получаемые на выходе из блока подстановок. На пересечении строк и столбцов отображается количество пар дифференциалов $\Delta A/\Delta C$ имеющих данные входную и выходную разности. Иными словами, мы получим значение, которое покажет, с какой вероятностью при заданном дифференциале ΔA на выходе из блока подстановок S будет получен конкретный дифференциал ΔC [1-2]. Часть таблицы вероятностей отображена в таблице 1.

В общем случае показано, что если входная разность в блок замены имеет нулевую разность (то есть тексты, которые образуют данную разность, равны), то на выходе такого преобразования разность также будет иметь нулевое значение (несмотря на то, что она будет образована новыми значениями, полученными в результате применения преобразования замены). Если же входная разность имеет ненулевое значение, то она может быть преобразована в различные значения с некоторыми вероятностями (вне которых случаях даже в значение, равное 0) [2-3].

В результате применения алгоритма анализа S-блоков, было получено таблица, отражающих дифференциальные зависимости для S-блока (таблице 1).

Анализ построенной таблицы позволил выявить следующие закономерности:

1. Сумма всех значений одной горизонтальной линии, то есть количества различных значений выходных разностей ΔC , соответствующих одному и тому же значению входной разности ΔA всегда равна 2^8 .
2. Ненулевое значение входной разности ΔA ни в одном из блоков не может быть заменено на значение $\Delta C = 0$.
3. В таблице анализа нет пар разностей $(\Delta A, \Delta C)$ с вероятностью больше, чем $3/64$.
4. Таблица №2 свидетельствует о том, что в данном случае вероятность может быть равна $1/256$, $2/256$, $4/256$, $6/256$, $8/256$ и $12/256$, а также может быть равной нулю.

Таблица 1.

Фрагмент таблицы со значениями вероятностей, построенной для блока подстановок S

		ΔA							
		0	1	2	3	...	253	254	255
ΔC	0	256/256	0/256	0/256	0/256	...	0/256	0/256	0/256
	1	0/256	0/256	0/256	0/256	...	0/256	2/256	2/256
	2	0/256	0/256	2/256	0/256	...	0/256	0/256	0/256
	3	0/256	0/256	2/256	0/256	...	0/256	0/256	4/256
	...	...	...	...	...	...	...	...	...
	253	0/256	0/256	0/256	0/256	...	2/256	0/256	0/256
	254	0/256	0/256	6/256	4/256	...	2/256	0/256	2/256
	255	0/256	4/256	2/256	2/256	...	0/256	0/256	0/256

Заключение

Выявленные закономерности представляют собой большой интерес и будут использованы в дальнейшем при разработке алгоритма дифференциального криптоанализа.

Алгоритм ВС-2 программно реализован на языке Delphi. Ведутся работы по криптоанализу алгоритма шифрования ВС-2 и в дальнейшем планируется тестирования алгоритма с помощью различных тестов, исследование полученных результатов для выявления недостатков реализации алгоритма.

Благодарность

Научно-исследовательская работа выполнена в рамках проекта BR05236757-«Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» в Институте информационных и вычислительных технологий.

Литература

1. Бабенко Л.К., Ищукова Е.А., Толоманенко Е.А. Дифференциальный анализ шифра «Кузнечик» // Изв. ЮФУ. Технические науки. – Таганрог: Изд-во ЮФУ, 2017. – №5. – С. 25–37.
2. Ищукова Е.А., Калмыков И.А. Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147–89 // Инженерный вестник Дона. – 2015. – №4. – URL: <https://cyberleninka.ru/article/n/differentsialnyesvoystva-s-blokov-zameny-dlya-algoritma-gost-28147-89>).
3. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.
4. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2002. – 648 с.
5. Капалова Н.А., Хаумен А. Алгоритм шифрования на SP-сети // Материалы научной конференции Института информационных и вычислительных технологий МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2017. – С. 113–118.
6. N. Kapalova, A. Haumen. The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network. // Open Engineering, formerly Central European Journal of Engineering. De Gruyter. 2018; 8: –P. 140–146.

Symmetric block data encryption algorithm «BC-2»

Kapalova N.A.¹¹⁵, Haumen A.¹¹⁶

Abstract. *The article deals with the data encryption algorithm based on an SP-network. The basic properties of the BC-2 encryption algorithm and the transformations that are part of the algorithm are described. The main differential properties revealed for the S-box of the algorithm are presented. These properties can be used for analysis using methods such as differential cryptanalysis and the impossible differential method.*

Keywords: *scheme of encryption algorithm, linear conversion, SP-network, S-substitution block, differential properties.*

¹¹⁵ Nursulu Kapalova: candidate of engineering science, Institute Information and Computational Technologies Almaty, Kazakhstan, nkapalova@mail.ru.

¹¹⁶ Armanbek Haumen, Institute Information and Computational Technologies Almaty, Kazakhstan, haumen.armanbek@gmail.com

Правовые аспекты статуса и рисков искусственного интеллекта**Карцхия А. А.,¹¹⁷ Макаренко Д. Г.¹¹⁸****Аннотация**

Статья посвящена анализу особенностей рисков применения технологий искусственного интеллекта с точки зрения права в условиях формирования новой технологической среды, цифровых прав и цифровых активов в виде новых объектов правового регулирования, создаваемых с применением современных цифровых технологий (криптовалюты и токены, виртуальное имущество, искусственный интеллект и роботизированные устройства, цифровые двойники, большие данные, облачные сервисы и др.) Авторы обосновывают необходимость создания законодательной базы для практического использования и применения технологий искусственного интеллекта, предлагают построение комплексной модели правового регулирования, включающей формирование универсальных стандартов и правил применения ИИ в имущественном обороте и цифровой виртуальной технологической среде.

Ключевые слова: субъекты права, искусственный интеллект, цифровые технологии, цифровые права, смарт-контракты, интеллектуальная собственность, интеллектуальные права, патенты и товарные знаки, риск-менеджмент

Введение

Современные цифровые технологии упраздняют традиционные границы между областями знаний и технологий, способствуют проникновению инноваций в новые, более сложные области техники. Под воздействием цифровых технологий создаются новые цифровые объекты (криптовалюты и токены, виртуальное имущество, искусственный интеллект и роботизированные устройства, цифровые двойники, большие данные и др.), которые способны участвовать в имущественном коммерческом обороте, появляются новые виды услуг (сервисов) (компьютерные облачные вычисления и сервисы, разнообразные «умные» устройства, технологические цифровые платформы, смарт-контракты и др.), формируется новая среда виртуального общения в виде социальных сетей, цифровых технологических платформ-агрегаторов [1-3]. Формирование новой технологической среды обуславливает практическую необходимость создания специального систематизированного законодательства по искусственному интеллекту, включая вопросы правового статуса искусственного интеллекта, правовые способы использования технологий ИИ, основания и пределы ответственности ИИ.

1. Постановка задачи: актуализация новой сферы правового регулирования

Влияние цифровых технологий определяет потребность развития современного правового регулирования с использованием цифровых объектов, технологий искусственного интеллекта, цифровых технологических платформ, новых видов цифровых услуг, субъектов имущественного гражданского оборота. Использование современных цифровых технологий способствует формированию новой технологической среды для правового регулирования и, одновременно, актуализирует проблему адаптации права к возможностям современных цифровых технологий, правовой охраны и использования интеллектуальной собственности, защиты интеллектуальных прав. Цифровые технологии оказывают существенное влияние на развитие традиционных отраслей экономики и стали составной

¹¹⁷ Карцхия Александр Амиранович, профессор РГУ нефти и газа (НИУ) имени И.М. Губкина, кандидат юридических наук, доцент, г. Москва, Россия. E-mail: arhz50@mail.ru.

¹¹⁸ Макаренко Дмитрий Григорьевич, Генеральный директор ООО «Национальная юридическая служба», г. Москва, Россия. E-mail: m54321@ya.com

частью современных управленческих систем в предпринимательстве, государственном управлении, в сферах обороны страны, безопасности государства и обеспечения правопорядка, создают новые бизнес-модели [4-6].

В условиях широкого применения технологий искусственного интеллекта в различных сферах, применения новых цифровых объектов, изменения действующего гражданского законодательства и введения правовых институтов цифровых прав, цифровых активов формируется новая область имущественного гражданского оборота – цифровой гражданский оборот, центральное место в котором отводится цифровым правам на новые объекты, создаваемые современными цифровыми технологиями.

В совокупности факторов формирования новой технологической среды правового регулирования и отсутствия законодательного регулирования искусственного интеллекта практика использования технологий искусственного интеллекта свидетельствует о необходимости создания системного массива законодательства, включая вопроса правового статуса искусственного интеллекта, способов использования технологий ИИ, оснований и пределов ответственности ИИ.

2. Особенности объекта исследования: феномен искусственного интеллекта в праве

Искусственный интеллект в правовом регулировании, рассматривается как новый вызов для правовой системы, новое явление, имеющее мультипликационный эффект, правовой феномен в структуре правоотношений, новый объект для правового регулирования.

Искусственный интеллект (ИИ) все чаще становится движущей силой важных разработок в области технологий и бизнеса, от автономных транспортных средств до медицинской диагностики и передового производства. В наши дни ИИ стал объектом не только теоретических исследований, но вышел на глобальный рынок, его рост стимулируется обилием оцифрованных данных и быстро развивающимися вычислительными мощностями обработки таких данных¹¹⁹.

Феномен ИИ проявляется в следующих факторах влияния:

- Способы использования ИИ: продвинутые формы статистических и математических моделей (машинное обучение, нечеткая логика и экспертные системы), позволяющие вычислять задачи, обычно выполняемые людьми. Способы использования ИИ служат в качестве средства реализации различных функций ИИ.

- Функциональные возможности ИИ такие функции, как: предиктивная аналитика, методы контроля, планирование и диспетчеризация, роботы, хранение, обработка и представление знаний и обоснований; распределенный ИИ; речь и компьютерное зрение; речевые функции (включая общую обработку речи, распознавание речи, фонология, синтез речи, речевой диалог, распознавание диктора), а также компьютерное зрение (включая дополненную реальность, биометрию, сегментацию изображений и видео, распознавание символов, слежение за объектом, понимание сцены, общее зрение); обработка естественного языка (включая извлечение информации, машинный перевод, диалог). Эти функции используются как самостоятельно, или могут быть реализованы в совокупности нескольких функций.

- Сферы применения ИИ: различные области (промышленность, транспорт, сельское хозяйство, медицина, образование, госуправление и др.) или дисциплины, где способы ИИ или функциональные его приложения могут найти применение, включая аффективные вычисления, персональные компьютеры и приложения для ПК; Интернет вещей (IoT), компьютерные сети/Интернет; аэрокосмическая отрасль и авионика, автономные транспортные средства и управление ими; радиовещание и телевидение, все виды связи; обнаружение аномалий/наблюдение, идентификация, криптография и компьютерная

¹¹⁹ WIPO Technology Trends 2019: Artificial Intelligence.URL: <http://www.wipo.int>

безопасность; «умные» города и иные «умные» объекты; социальные связи; обслуживание клиентов и электронная коммерция; право, социальные и поведенческие науки.

Разновидности (приложения) искусственного интеллекта быстро осваиваются в ряде секторов, где возможно обнаружение закономерности в больших объемах данных и моделирование сложных, взаимозависимых системы для улучшения принятия решений изготoвление и экономия затрат¹²⁰, включая автономные транспортные средства, НИОКР с обработкой крупномасштабных данных, интеллектуальная медицина и здравоохранение, финансы и расчеты, маркетинг и реклама, сельское хозяйство; прогнозирование полицейской деятельности и оценки риска повторных правонарушений, прогнозирование законотворчества и правоприменения, а также автоматизация обнаружения и реагирования на угрозы в режиме реального времени.

Искусственный интеллект с точки зрения права и способности участия в имущественном обороте представляет собой компьютерную систему, действующая на основе определенных принципов, которая может для заданного набора целей, определенных человеком, делать прогнозы, рекомендации или решения, влияющие на реальную или виртуальную среду, и предназначена для работы с различными уровнями автономности.

ИИ стал инструментом правового регулирования, но, тем не менее, с точки зрения современного права ИИ не обладает самостоятельной правосубъектностью и рассматривается как объект правового регулирования, т.е. имущество, подконтрольное физическому или юридическому лицу.

В этом смысле ИИ выступает как программно-аппаратный комплекс. Разновидности ИИ: слабый ИИ, способный решать только узкоспециализированные задачи и универсальный (сильный) ИИ, способный подобно человеку решать комплексные задачи, самостоятельно мыслить, взаимодействовать и адаптироваться к изменяющимся условиям, использовать большие данные.

Используемый в современном праве режим правовой охраны искусственного интеллекта только с позиций защиты интеллектуальных прав (прав интеллектуальной собственности) на компьютерные программ (их комплекс) явно не достаточен. Правовые дискуссии о возможности защиты прав искусственного интеллекта на создаваемые им самостоятельно произведения в сфере авторского права лишь частично решают вопросы использования технологий искусственного интеллекта и в полной мере не отвечают перспективным возможностям их применения, что создает препятствия к расширению внедрения таких технологий.

Новые достижения в области искусственного интеллекта вызваны взаимодействием информатики и когнитивной наукой. Идея глубокой нейронной сети (используемой для применения искусственного интеллекта в автономных транспортных средствах, создание новых лекарств и генетических объектов и др.) базируется на механизмах работы человеческого мозга, применении машинного обучения на базе множества вычислительных систем, организованных по принципу нейронных сетей.

Искусственный интеллект рассматривается и как комплекс технологических решений, имитирующий когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и способный получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Такой комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение, процессы и сервисы по обработке данных и поиску решений, что позволяет

¹²⁰ OECD Recommendation of the Council on Artificial Intelligence. OECD. 2019
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

рассматривать его в качестве объекта регулирования в сфере интеллектуальной собственности и возможности защиты интеллектуальных прав.

3. Направленность исследования: правовые риски искусственного интеллекта, их оценка и управление

Безопасность как один из основных принципов использования ИИ представляет собой «недопустимость использования искусственного интеллекта в целях умышленного причинения вреда гражданам и юридическим лицам, а также предупреждение и минимизация рисков возникновения негативных последствий использования технологий искусственного интеллекта», как отмечается в Национальной стратегии развития искусственного интеллекта.

Это предполагает, в том числе, прогнозирование рисков и неблагоприятных событий, снижение уровня непосредственного участия человека в процессах, связанных с повышенным риском для его жизни и здоровья. Таки образом, ИИ становится фактором информационной безопасности [7].

Оценка риска, в соответствии с ГОСТ РФ, включает в себя процесс идентификации внутренних и внешних угроз уязвимостей, идентификацию вероятности опасного события, возникшего при реализации этих угроз или уязвимостей, определение критических видов деятельности, для которых необходимо обеспечение бесперебойной работы, определение средств управления на местах, необходимых для снижения распространения последствий опасного события, и оценка стоимости таких средств управления [8-10].

Участие в имущественном обороте предполагает у его участников навыки идентификации угроз и опасностей, оценку риска, уязвимостей и опасностей, анализ воздействий на деятельность. В этом смысле ИИ может найти широкое применение, включая разработку различных бизнес моделей предпринимательской деятельности, в том числе и в виртуальном мире сети Интернет [11-15].

Развитие внедрения ИИ связано с разработкой (а) стандартов и эталонов безопасности функционирования ИИ, (б) комплексной системы безопасности использования технологий ИИ, (в) этических правил взаимодействия человека с искусственным интеллектом.

Отсюда необходимость выявления и систематизация рисков при использовании ИИ, включая правовые аспекты таких рисков, к которым можно отнести основания, формы и пределы ответственности ИИ, объем правосубъектности для каждой технологии ИИ, формирование специальных норм законодательства по созданию и использованию ИИ в рамках института интеллектуальной собственности и имущественного гражданского оборота, создание эталонной классификации технологий ИИ для определения режима правовой охраны и способов использования ИИ в имущественном обороте для каждой группы классификатора.

4. Выводы и рекомендации

Расширение использования ИИ в гражданском обороте, в коммерческих отношениях и предпринимательской деятельности формирует запрос на создание специальных правовых норм, регулирующих сферу использования технологий искусственного интеллекта, включая нормы, определяющие правосубъектность и режимы правовой охраны, использования и защиты технологий ИИ, формы и виды ответственности при использовании технологий ИИ, создание эталонной классификации технологий ИИ.

Объективно необходима не только законодательная база для практического использования и применения технологий искусственного интеллекта, но и построение комплексной модели правового регулирования, включающей в том числе формирование универсальных стандартов и правил применения ИИ в имущественном обороте и цифровой виртуальной технологической среде, регулирование способов и форм применения

технологий ИИ, использования имущественных прав на технологии ИИ, особенностей правовых режимов регулирования в зависимости от вида технологии ИИ.

Литература

1. Карцхия А.А. Кибербезопасность и интеллектуальная собственность. Часть 1 // Вопросы кибербезопасности. 2014. № 1 (2). С. 61-66.
2. Карцхия А.А. Кибербезопасность и интеллектуальная собственность. Часть 2 // Вопросы кибербезопасности. 2014. № 2 (3). С. 46-50.
3. Карцхия А.А. Кибербезопасность и интеллектуальная собственность. Часть 3 // Вопросы кибербезопасности. 2014. № 3 (4). С. 42-49.
4. Гущина Е.А., Макаренко Г.И., Сергин М.Ю. Обеспечение информационно-технологического суверенитета государства в условиях развития цифровой экономики // Право.by. 2018. № 6 (56). С. 59-63.
5. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. №3 (31). С.18-23. DOI: 10.21681/2311-3456-2019-2-18-23.
6. Bliznets I., Kartskhiya A., Smirnov M. Technology Transfer in Digital Era: Legal Environment// Tarih Kültür ve Sanat Araştırmaları. 2018. V.7. N 1. P.354-363. DOI: <http://dx.doi.org/10.7596/taksad.v7i1.1466>.
7. Карцхия А.А. Промышленная собственность как фактор информационной безопасности // Правовая информатика. 2017. №2. С. 55-58. DOI: 10.21681/1994-1404-2017-2-55-58.
8. Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. -London: IntechOpen, 2018. 278 p.
9. Александров А.А., Ларионов В.И., Суцев С.П. Анализ и управление техногенными и природными рисками. – М.: МГТУ им.Н.Э. Баумана, 2019, 357 с.
10. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
11. Карцхия А.А. Интеллектуальная собственность в киберпространстве: новые условия правоприменения // Мониторинг правоприменения. 2017. № 1(22). С.50-52. DOI: 10.21681/2412-8163-2017-1-53-61.
12. Abbott R. I Think, Therefore I Invent: Creative Computers and the Future of Patent Law // Boston College Law Review. 2016. Vol. 57.
13. DeCosta F.A., Carrano A.G. Intellectual property protection for artificial intelligence // Westlaw journal intellectual property. 2017. 30 (August). URL:https://www.finnegan.com/print/content/46173/Intellectual-Property_Protection-for-Artificial-Intelligence.pdf?q=
14. McCarthy J. What is Artificial Intelligence?/ URL: <http://www-formal.s.tanford.edu/jmc/whatisai>.
15. Yanisky S. and Moorhead S. Generating Rembrandt: Artificial Intelligence, Accountability and Copyright. The Human-Like Workers Are Already Here - A New Model. URL: <https://ssrn.com/abstract=2957722>

Legal Aspects of the Status and Risks of Artificial Intelligence

Kartskhia A., Makarenko D.

Annotation

The article is devoted to the analysis of the use of artificial intelligence technologies and virtual property, virtual property, artificial intelligence and robotic technologies. devices, digital doubles, big data, cloud services, etc.) the actual use and application of artificial intelligence technologies, offers the construction of a comprehensive model of legal regulation, including the formation of universal standards and rules for the use of AI in property circulation and digital virtual technological environment.

Keywords: subjects of law, artificial intelligence, digital technologies, digital rights, intellectual contracts, intellectual property, patents and trademarks, risk management.

Локализация сбоев при дифференциальном криптоанализе по ошибкам вычислений поточных шифров, основанных на нелинейных регистрах сдвига

Климцов В.Е.¹²¹, Чиликов А.А.¹²²

Аннотация. Мы рассматриваем возможность применения алгоритма локализации сбоев, основанного на построении таблиц распространения ошибок, к криптосистемам, использующим регистры с нелинейной функцией обратной связи. В Grain-128 сбои вносились только в LFSR, что позволяло избежать влияние нелинейности на распространение ошибок. Однако в Trivium не используются регистры с линейной функцией обратной связи. В ходе анализа было установлено, что данный метод локализации сбоев применим к шифрам, основанным на NFSR, но требует адаптации, усложняющей его программную реализацию.

Ключевые слова: eSTREAM, Grain-128, Trivium, fault-атаки, криптоанализ.

Введение

Дифференциальный криптоанализ по ошибкам вычислений является одним из подвидов анализа по сторонним каналам^[1]. В нем используется оказание воздействия на схему алгоритма с целью внесения сбоя в работу криптосистемы и последующее сравнение полученного «сбойного» ключевого потока с изначальным, с целью полного или частичного получения ключа и вектора инициализации, используемых в системе^[2].

В настоящее время fault-атаки считаются одним из наиболее эффективных методов анализа современных шифров, как поточных, так и блочных. Принципы проектирования криптоалгоритмов делают их изначально стойкими к классическим «математическим» атакам, однако учесть все аспекты атак по сторонним каналам удастся далеко не всегда. В тоже время успех side-channel анализа зависит не только от структуры алгоритма, но и от того, на каком устройстве он реализуется.

При рассмотрении криптоанализа по ошибкам вычислений поточных аппаратно-реализуемых шифров прослеживается возможность автоматизации некоторых этапов работы для конкретной модели сбоя. Классический метод проведения fault-атак на LFSR-based шифры был описан Хоком и Шамиром^[3]. В нем было выделено пять этапов анализа, однако в целом их можно обобщить в два – локализации сбоя и получение секретной информации.

При fault-анализе Grain-128 локализация сбоя производилась посредством построения таблиц распространения ошибок и выделения уникальных сигнатур для каждого из диапазонов начального расположения сбоя. Потенциально данный метод может быть применен к широкому классу криптоалгоритмов. Однако анализ Trivium показывает, что при работе с нелинейными регистрами построение таблиц затрудняется возникновением «вероятных» сбоя не только на выходе криптосистемы, но и в столбцах таблицы.

¹²¹ Климцов Владимир Евгеньевич, аспирант кафедры ИУ-8 МГТУ им. Н.Э. Баумана, Москва, sentlabs@bk.ru

¹²² Чиликов Алексей Анатольевич, кандидат физико-математических наук, доцент кафедры ИУ-8 МГТУ им. Н.Э. Баумана, Москва, chilikov@passware.com

Анализ Grain-128

В ходе проекта eSTREAM были предложены три новых поточных поточных шифра, предназначенных для аппаратной реализации – Trivium, Grain и MIKEY.

В основе шифра Grain-128 лежат три основных блока: регистр сдвига с линейной обратной связью (далее – LFSR), регистр сдвига с нелинейной обратной функцией связи (далее – NFSR) и выходная функция. Выходная функция определена как нелинейная комбинация значений определенных ячеек обоих регистров, каждый из которых имеет длину 128^[4].

Для начала работы шифр необходимо проинициализировать. В Grain-128 используются 128-битный ключ и 96-битный вектор инициализации. Все ячейки NFSR заполняются битами ключа, а IV помещается в LFSR с нулевой ячейки, оставшиеся заполняются единицами. После чего шифр обрабатывает 256 тактов, не подавая ключевой поток на выход, вместо этого каждый бит гаммы складывается с функциями обратной связи как LFSR, так и NFSR.

При анализе использовалась модель сбоя, предполагающая инверсию значения одной из ячеек регистра. Ошибки вносились в LFSR. После анализа выходной функции криптосистемы, стало известно, что сбой, попав в ячейки $s_{93}, b_{89}, b_{73}, b_{64}, b_{45}, b_{36}, b_{15}, b_2$ – с вероятностью 100% изменяет значение выходной функции шифра, попав в $s_{79}, s_{60}, s_{42}, s_{20}, s_{13}, s_8, b_{73}, b_{12}$ – с вероятностью 50%, а в s_{95} – с вероятностью в 25%. При этом для локализации сбоя можно использовать следующие признаки: сбой, попавший в диапазон $s_{93} - s_{127}$, можно идентифицировать по следующему признаку – после первого появления в различий в выходном потоке двух криптосистем, ошибка также появится и спустя 132 сдвига (расстояние между s_{93} и b_{89}), а для остальной части LFSR можно использовать разницу в 16 сдвигов (расстояние между b_{89} и b_{73}).

Дальнейший анализ показал несостоятельность такого метода ввиду того, что он позволяет определить позицию ошибки, только если в обоих регистрах одновременно находится лишь один инвертированный бит, а при работе шифра, такие биты распространяются и множатся. После чего были построены таблицы распространения сбоя для каждого из возможных положений ошибки. Пример такой таблицы приведен на рисунке 1.

125	b98	s2	s17	s28	s34	s60	s64	s66	s81	s86	s91	s92	s96	s97	s98	s111
126	b97	s1	s16	s27	s33	s59	s63	s65	s80	s85	s90	s91	s95	s96	s97	s110
127	b96	s0	s15	s26	s32	s58	s62	s64	s79	s84	s89	s90	s94	s95	s96	s109
128	b95	b127	s14	s25	s31	s57	s61	s63	s78	s83	s88	s89	s93	s94	s95	s108
129	b94	b126	s13	s24	s30	s56	s60	s62	s77	s82	s87	s88	s92	s93	s94	s107
130	b93	b125	s12	s23	s29	s55	s59	s61	s76	s81	s86	s87	s91	s92	s93	s106
131	b92	b124	s11	s22	s28	s54	s58	s60	s75	s80	s85	s86	s90	s91	s92	s105
132	b91	b123	s10	s21	s27	s53	s57	s59	s74	s79	s84	s85	s89	s90	s91	s104
133	b90	b122	s9	s20	s26	s52	s56	s58	s73	s78	s83	s84	s88	s89	s90	s103
134	b89	b121	s8	s19	s25	s51	s55	s57	s72	s77	s82	s83	s87	s88	s89	s102
135	b88	b120	s7	s18	s24	s50	s54	s56	s71	s76	s81	s82	s86	s87	s88	s101
136	b87	b119	s6	s17	s23	s49	s53	s55	s70	s75	s80	s81	s85	s86	s87	s100
137	b86	b118	s5	s16	s22	s48	s52	s54	s69	s74	s79	s80	s84	s85	s86	s99
138	b85	b117	s4	s15	s21	s47	s51	s53	s68	s73	s78	s79	s83	s84	s85	s98
139	b84	b116	s3	s14	s20	s46	s50	s52	s67	s72	s77	s78	s82	s83	s84	s97
140	b83	b115	s2	s13	s19	s45	s49	s51	s66	s71	s76	s77	s81	s82	s83	s96
141	b82	b114	s1	s12	s18	s44	s48	s50	s65	s70	s75	s76	s80	s81	s82	s95
142	b81	b113	s0	s11	s17	s43	s47	s49	s64	s69	s74	s75	s79	s80	s81	s94
143	b80	b112	b127	s10	s16	s42	s46	s48	s63	s68	s73	s74	s78	s79	s80	s93
144	b79	b111	b126	s9	s15	s41	s45	s47	s62	s67	s72	s73	s77	s78	s79	s92
145	b78	b110	b125	s8	s14	s40	s44	s46	s61	s66	s71	s72	s76	s77	s78	s91
146	b77	b109	b124	s7	s13	s39	s43	s45	s60	s65	s70	s71	s75	s76	s77	s90
147	b76	b108	b123	s6	s12	s38	s42	s44	s59	s64	s69	s70	s74	s75	s76	s89
148	b75	b107	b122	s5	s11	s37	s41	s43	s58	s63	s68	s69	s73	s74	s75	s88
149	b74	b106	b121	s4	s10	s36	s40	s42	s57	s62	s67	s68	s72	s73	s74	s87
150	b73	b105	b120	s3	s9	s35	s39	s41	s56	s61	s66	s67	s71	s72	s73	s86

Рисунок 1 – Распространения сбоя при его изначальном попадании в диапазон $s_{93} - s_{127}$

Красным обозначены ячейки, которые используются для расчета функции обратной связи LFSR, а синим – NFSR, попадание сбоя в них, приводит к появлению нового столбца

в таблице. Ячейка s_0 выделена желтым, так как используется и в обоих регистрах. Зеленым помечены ячейки, изменение значений в которых приводит к изменению значения z_i , а салатовым те, для которых вероятность этого события не равна 100%.

Диапазоны начального положения сбоя были получены на основе функции обратной связи LFSR, далее для каждого из них выделена уникальная сигнатура и общий алгоритм локализации сбоя для шифра Grain-128.

Анализ Trivium

Trivium – синхронный поточный шифр, который может генерировать вплоть до 2^{64} бит ключевого потока на основе 80-битного секретного ключа (Key) и 80-битного вектора инициализации (IV)^[5]. Как и в большинстве проточных шифров этот процесс делится на две стадии – инициализация и непосредственно генерация гаммы.

Изначальное состояние Trivium представляет собой 3 сдвиговых регистра суммарной длины в 288 бит. Каждый такт происходит изменение битов в регистрах сдвига путём нелинейной комбинации прямой и обратной связи.

При анализе алгоритма было выявлено следующее – Trivium является диаметральной противоположностью Grain-128. LFSR имеет линейную функцию обратной связи, а ключевой поток z_i нелинейно зависит от значений ячеек LFSR и NFSR в момент времени t . В Trivium все три регистра имеют нелинейную функцию обратной связи, а z_i линейно зависит от значений их ячеек в момент времени t .

Такая структура алгоритма позволяет упростить построение таблиц распространения сбоя, так как исчезают ячейки, изменения значений которых приводят к изменению z_i с вероятностью не равной 100%. Однако при этом нелинейная функция обратной связи приводит к появлению в таблице столбцов, существующих лишь для некоторых пар (Key, IV).

Методы решения этой проблемы можно разделить на два типа - специфичный для алгоритма и общие. В случае первого типа необходимо проанализировать схему шифра и определить, можно ли построить сигнатуры до появления вероятных столбцов, или же вообще использовать другой алгоритм локализации сбоя. Общие методы основаны либо на устранении подобных столбцов, либо на их анализе. Во втором случае необходимо оценить возможность влияния вероятных распространявшихся сбоя на получаемые сигнатуры. В первом же рассмотреть все возможные варианты увеличения количества сбоя. При этом если для каждого из вариантов будет получена уникальная сигнатура, то можно будет уже на стадии локализации ошибок определить некоторые изначальные значения ячеек регистров. Если же все вероятные столбцы приведут к одинаковым сигнатурам, то они будут совпадать с теми, что получены методом анализа.

Использование специфичных для алгоритма подходов исключает возможность автоматизации этого этапа анализа и применение таблиц распространения сбоя в качестве универсального алгоритма локализации ошибок. Общие методы лишены этого недостатка, однако существенно увеличивают объем информации, необходимой для построения и дальнейшего анализа таблиц сбоя.

Заключение

Автоматизация некоторых этапов дифференциального криптоанализа по ошибкам вычислений позволит сократить время работы криптоаналитика. Основной сложностью при этом является поиск универсальных алгоритмов, позволяющих локализовать ошибку или получить изначальное значение регистра для широкого класса криптосистем.

Работа с Grain-128 и Trivium показала, что потенциально универсальные методы локализации сбоя, например построение таблиц распространения ошибок, испытывают некоторые трудности при работе с нелинейными регистрами. Если для линейных регистров

параметры функции обратной связи влияют на объем вычислений, то в случае с нелинейными регистрами увеличивается объем контролируемых в ходе работы алгоритма параметров.

Таким образом при проектировании программного обеспечения для автоматизации анализа придётся разделять модули, предназначенные для работы с шифрами, основанными на линейных и нелинейных регистрах соответственно. Что ставит вопрос о поиске других, более эффективных в реализации, алгоритмов локализации сбоя.

Литература

1. Introduction to Side-Channel Attacks [Электронный ресурс]. – Режим доступа: https://www.springer.com/cda/content/document/cda_downloaddocument/9780387718279-c1.pdf, свободный – (08.11.2019).
2. On the importance of Checking Cryptographic Protocols for Faults [Электронный ресурс]. – Режим доступа: https://link.springer.com/content/pdf/10.1007%2F3-540-69053-0_4.pdf, свободный – (08.11.2019).
3. Fault Analysis of Stream Ciphers [Электронный ресурс]. – Режим доступа: https://link.springer.com/content/pdf/10.1007%2F978-3-540-28632-5_18.pdf, свободный – (08.11.2019).
4. Trivium Specifications [Электронный ресурс]. – Режим доступа: http://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf, свободный – (21.11.2019).
5. A Stream Cipher Proposal: Grain-128 [Электронный ресурс]. – Режим доступа: http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain128_p3.pdf, свободный – (21.11.2019).

Графы Пайзера в задачах криптографии и обработки информации

Ключарёв П.Г.¹²³

Статья посвящена обзору применения в криптографии графов Пайзера, представляющих собой графы, вершинами которых являются классы изоморфизма суперсингулярных эллиптических кривых, а ребрами – изогениями между представителями этих классов. Такие графы являются графами Рамануджана и применяются, в частности, для построения как постквантовых асимметричных криптосистем, так и криптографических хэш-функций, основанных на блужданиях по расширяющему графу, а также, в качестве графов обобщенных клеточных автоматов, предназначенных для криптографических применений. Тот факт, что графы из одного и того же семейства применяются для решения столь разных задач, представляется весьма интересным.

Ключевые слова: граф Рамануджана, изогения, эллиптические кривые, криптография

Введение

Расширяющие графы, которые последние годы активно исследуются, весьма интересны не только своим глубоким теоретическим значением, но и возможностью использования в различных прикладных областях. В данной статье дается краткий обзор приложений семейства графов Пайзера в задачах криптографии (подобные задачи часто возникают в различных областях, связанных с обработкой информации). Такие графы являются так называемыми графами Рамануджана – в определенном смысле асимптотически наилучшим видом расширяющих графов.

Термины и определения.

Напомним, что расширяющим графом (expander graph) [1] называется неориентированный регулярный граф G , имеющий достаточно большой коэффициент реберного расширения $h(G)$ (здесь и далее мы используем термин «граф», допуская наличие петель и кратных ребер). Задача вычисления коэффициента реберного расширения является вычислительно трудной, однако его можно оценить исходя из связи с компонентами спектра графа. Напомним, что спектром неориентированного графа называется набор собственных значений его матрицы смежности, отсортированный по невозрастанию: $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_N$, где N – число вершин графа. Известно, что для d -регулярных графов $\lambda_1 = d$ и справедливо неравенство Чигера:

$$\frac{1}{2}(d - \lambda_2) \leq h(G) \leq \sqrt{2d(d - \lambda_2)}.$$

Теперь введем обозначение: $\lambda = \lambda(G) = \max_{|\lambda_i| < d} |\lambda_i|$. Графом Рамануджана [2] называется связный d -регулярный неориентированный граф G , для которого выполняется: $\lambda(G) \leq 2\sqrt{d-1}$. У таких графов маленький диаметр: $D(G) \leq 2\log_{d-1} N + O(1)$.

Графы Пайзера

Существуют явные семейства графов Рамануджана [3]. В том числе, два семейства графов Любоцкого-Филипса-Сарнака [4,5]: LPS-X и LPS-Y, семейство графов Пайзера [6,7]

¹²³ Ключарёв Петр Георгиевич, к.т.н., МГТУ им. Н.Э. Баумана, Москва, pk.iu8@yandex.ru

и семейство графов Моргенштерна [8]. Здесь приведем краткую информацию о семействе графов Пайзера [6,7]. Граф из этого семейства может быть описан различными способами. Здесь мы приведем наиболее часто употребляемое его описание – на основе изогений. Пусть p и l – простые числа, причем $p \equiv 1 \pmod{12}$, а l является квадратичным вычетом по модулю p . Вершинами графа Пайзера являются классы изоморфизма суперсингулярных эллиптических кривых [9] над полем F_{p^2} . Вершины такого графа можно задавать с помощью j -инвариантов соответствующих эллиптических кривых. То есть, будем писать «вершина j », имея в виду вершину, соответствующую классу изоморфизма эллиптических кривых с j -инвариантом j . Представителя такого класса будем обозначать как E_j .

Вершины j_1 и j_2 являются смежными, если существует l -изогения между E_{j_1} и E_{j_2} . Построенный таким образом граф Пайзера имеет $N = \lfloor p/12 \rfloor$ вершин. Он является двудольным $(l+1)$ -регулярным неориентированным графом и является графом Рамануджана.

Применения графов Пайзера

Графы Пайзера интересны тем, что они находят применения в различных областях криптографии. В частности, такие графы небольшого размера (от нескольких сотен до нескольких тысяч вершин) применяются в качестве графов обобщенных клеточных автоматов в некоторых симметричных криптографических алгоритмах, предложенных автором. Кроме того, они используются в некоторых специальных конструкциях криптографических хэш-функций, которые основаны на блужданиях по таким графам. Наиболее интересны применения таких графов в асимметричных криптосистемах, основанных на изогениях. В таких криптосистемах стойкость обеспечивается высокой вычислительной сложностью некоторых задач на таких графах. Причем для таких криптосистем не известно эффективного квантового алгоритмов взлома, поэтому их относят к постквантовым.

В статье [10] был предложен метод построения криптографических хэш-функций, основанных на блуждании по графу Пайзера большого размера. Сообщение делится на блоки длины s , где $2^s \leq l$. Блуждание начинается в некоторой фиксированной вершине этого графа. На каждом шаге в соответствии с очередным блоком хэшируемого сообщения выбирается ребро, инцидентное текущей вершине (кроме предыдущего ребра на пути), и производится переход по выбранному ребру в вершину ему инцидентную. Результатом является j -инвариант вершины, в которой блуждание остановится.

В ряде работ автора, в том числе [11,12], разрабатывались симметричные криптографические алгоритмы, основанные на обобщенных клеточных автоматах. Они интересны тем, что обладают высокой производительностью при аппаратной реализации. Обобщенный клеточный автомат представляет собой граф, с каждой вершиной которого ассоциирована ячейка памяти. На каждом шаге значение каждой ячейки вычисляется как некоторая булева функция (называемая локальной функцией связи) от значений смежных с ней ячеек на предыдущем шаге (ячейки будем называть смежными, если ассоциированные с ними вершины графа смежны). Такой граф (граф обобщенного клеточного автомата) должен обладать рядом свойств [3], в том числе, его диаметр должен быть как можно меньше, он не должен быть двудольным, он должен иметь маленькую степень (но не меньшую четырех) и в семействе графов должно существовать достаточно много графов с количеством вершин от нескольких десятков до нескольких тысяч. Оказывается, всеми этими свойствами обладают в том числе графы Пайзера.

Еще одно важное применение графов Пайзера – в постквантовой криптографии. В частности, в работе [13] предложен протокол распространения ключа, основанный на

изогениях суперсингулярных эллиптических кривых (идея использования изогений для построения таких протоколов, по-видимому, впервые предложена в работе [14]). Протокол этот состоит в следующем.

Пусть E – суперсингулярная эллиптическая кривая над полем F_{p^2} , где $p = s_A^n s_B^m k \pm 1$, s_A и s_B – простые числа, k – коэффициент, такой, что p – простое число. Алиса и Боб выбирают точки P_A, Q_A, P_B, Q_B таким образом, что точки P_A, Q_A порождают группу s_A^n -кручения, а точки P_B, Q_B – группу s_B^m -кручения эллиптической кривой E . Параметры p, E, P_A, Q_A, P_B, Q_B являются открытыми.

Теперь Алиса случайно выбирает секретные неотрицательные целые числа m_A, n_A , меньшие s_A^n , не кратные s_A одновременно. Боб случайно выбирает секретные неотрицательные целые числа m_B, n_B , меньшие s_B^m , не кратные s_B одновременно.

Алиса вычисляет изогению $\alpha: E \rightarrow E_A$ с ядром $\langle m_A P_A + n_A Q_A \rangle$, а Боб вычисляет изогению $\beta: E \rightarrow E_B$ с ядром $\langle m_B P_B + n_B Q_B \rangle$.

Боб передает Алисе $E_B, \beta(P_A), \beta(Q_A)$.

Алиса передает Бобу $E_A, \alpha(P_B), \alpha(Q_B)$.

Алиса вычисляет изогению $\alpha': E_B \rightarrow E_{AB}$ с ядром $\langle m_A \beta(P_A) + n_A \beta(Q_A) \rangle$, а Боб – изогению $\beta': E_A \rightarrow E_{AB}$ с ядром $\langle m_B \alpha(P_B) + n_B \alpha(Q_B) \rangle$.

Теперь и Алиса и Боб обладают общей эллиптической кривой $E_{AB} = \alpha'(\beta(E)) = \beta'(\alpha(E))$. В качестве общего ключа, сгенерированного в результате выполнения протокола, выступает j -инвариант эллиптической кривой E_{AB} .

Очевидно, что описанный протокол, являющийся постквантовым аналогом протокола Диффи-Хеллмана, напрямую связан с графами Пайзера [14,15].

Выводы

Таким образом, графы Пайзера находят применение в различных задачах криптографии. Тот факт, что три весьма разных задачи – построение графов обобщенных клеточных автоматов, предназначенных для применения в криптографии, построение криптографических хэш-функций и разработка методов постквантовой криптографии – привели к использованию графов одного и того же семейства, наводит на мысль о глубоких аналогиях между этими задачами.

Литература

1. Hoory S., Linial N., and Wigderson A. Expander graphs and their applications // Bull. Amer. Math. Soc. 2006. V. 43. No. 4. P. 439–562.
2. Davidoff G., Sarnak P., and Valette A. Elementary Number Theory, Group Theory and Ramanujan Graphs. Cambridge: Cambridge University Press, 2003. V. 55. 144 p.
3. Ключарёв П.Г. Детерминированные методы построения графов Рамануджана, предназначенных для применения в криптографических алгоритмах, основанных на обобщённых клеточных автоматах. // Прикладная дискретная математика, 2018, № 42, С. 76–93
4. Lubotzky A., Phillips R., and Sarnak P. Explicit expanders and the Ramanujan conjectures // Proc. 18th Ann. ACM Symp. on Theory of Computing. ACM, 1986. P. 240–246.
5. Sarnak P. Some Applications of Modular Forms. Cambridge: Cambridge University Press, 1990. V. 99. 111 p.
6. Pizer A. K. Ramanujan graphs and Hecke operators // Bull. Amer. Math. Soc. 1990. V. 23. No.1. P. 127–137.
7. Charles D. X., Goren E. Z. and Lauter K. E. Families of Ramanujan graphs and quaternion algebras // Groups and symmetries, CRM Proc. Lecture Notes, vol. 47, Amer. Math. Soc., Providence, RI, 2009, P. 53–80
8. Morgenstern M. Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q // J. Combinatorial Theory. Ser. B. 1994. V. 62. No. 1. P. 44–62.
9. Silverman J. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. N.Y.: Springer, 2009. 402 p.
10. Charles D. X., Lauter K. E., and Goren E. Z. Cryptographic hash functions from expander graphs // J. Cryptology. 2009. V. 22. No. 1. P. 93–113.
11. Ключарёв П. Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2012. № 12. С. 361–374.
12. Ключарёв П. Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности, 2017, №1(19). С. 45-50.
13. De Feo L., Jao D, Plut J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies //Journal of Mathematical Cryptology. – 2014. –V. 8. – №. 3. – P. 209-247.
14. Rostovtsev A., Stolbunov A. Public-Key Cryptosystem Based on Isogenies //IACR Cryptology ePrint Archive. 2006. P. 145.
15. Costache A. et al. Ramanujan graphs in cryptography //Research Directions in Number Theory. – Springer, 2019. – P. 1-40.

Pizer graphs in cryptography and in information processing

Klyucharev P.G.¹²⁴

Abstract. *In this article we briefly review some applications of Pizer graphs in cryptography. The Pizer graphs are graphs whose vertices are isomorphism classes of supersingular elliptic curves, and edges are the isogenies between representatives of these classes. Such graphs are Ramanujan graphs. They are used to construct post-quantum asymmetric cryptosystems, cryptographic hash functions based on walks on the expander graph, and also as graphs of generalized cellular automata intended for cryptographic applications. The fact that graphs from the same family are used to solve such different problems is appeared to be very interesting.*

Keywords: *Ramanujan graph, isogeny, elliptic curve, cryptography*

¹²⁴ Petr Klyucharev, Ph.D., Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

Проблема информационной безопасности в сфере авионики

Козарь А.А.¹²⁵

Аннотация

В статье рассматриваются теоретические вопросы обеспечения информационной безопасности бортового оборудования летательных аппаратов. Подробно описаны существующие проблемы и способы их решения в сфере защиты авионики. Кратко представлены актуальные задачи и требуемые направления исследований для решения поставленных задач. Обозначена актуальность проблемы информационной безопасности в сфере авионики и авиации в целом, приведены примеры серьезных угроз безопасности и последствия успешной компрометации информационной целостности систем летательных аппаратов.

Ключевые слова: авиация, авионика, кибербезопасность, летательный аппарат, бортовые системы.

Введение

В настоящее время летательные аппараты все шире применяются в различных сферах деятельности человека. Это и гражданская авиация, и грузовые перевозки, военная сфера, а также беспилотные летательные аппараты (далее ЛА) различного применения [4]. Поскольку летательные аппараты полагаются на сложные электронные системы, а также являются одной из самых серьезных сфер, требующих обеспечения надежности и отказоустойчивости, соблюдение информационной безопасности на всех этапах проектирования и эксплуатации является важнейшим требованием. При этом в настоящий момент комплексного решения проблемы информационной безопасности не предложено. Развитие технологий и усложнение техники позволяет злоумышленникам осуществлять взлом и подавление электронных систем летательного аппарата без использования каких-либо сложных технических средств [14-16]. Существующих стандартов недостаточно для того, чтобы говорить о полной информационной защищенности жизненно важных систем ЛА[5].

Для решения задачи обеспечения информационной безопасности необходимо решить несколько подзадач. В частности, актуальным является исследование такого понятия, как сами информационные угрозы, типы и причины их возникновения. Актуальным представляется построение некой обобщенной модели угрозы для дальнейшего анализа и тестирования. Помимо этого, необходимо детальное изучение жизненного цикла ЛА, процесса проектирования и основных его этапов для выявления уязвимых моментов. Необходимы также пересмотр и модификация стандартов обеспечения информационной безопасности, и разработка новых рекомендаций и методов контроля информационной целостности бортовых систем.

Проблема информационной безопасности и ее актуальность в настоящее время

В настоящий момент современные технологии направлены на поддержание эффективной работы практически любой сферы деятельности человека. Один из наиболее

¹²⁵Козарь Анастасия Андреевна, аспирант второго года обучения МГТУ им. Н.Э. Баумана кафедры РК6, kozar.a.a.rk6@yandex.ru

актуальных вопросов - насколько безопасно использование воздушного транспорта. Воздушный транспорт справедливо считается наиболее безопасным видом транспорта, поскольку специалистами постоянно проводится огромная работа по поддержанию целостности, высокой отказоустойчивости как воздушной, так и наземной составляющей авиации. Однако, с возрастанием сложности информационных технологий, все более остро встает вопрос соблюдения кибербезопасности, чему, по мнению экспертов, по-прежнему не уделяется должного внимания.

Будучи крайне сложной информационной системой, самолет является также наиболее уязвимой системой для злоумышленников. Благодаря повышению уровня автоматизации, современные летательные аппараты являются, по сути, полноценными компьютерами. Несмотря на то, что вероятность кибератаки рассматривается как крайне низкая, в контексте развития информационных технологий можно с уверенностью прогнозировать рост числа кибератак как в наземной сфере, так и на борту летательных аппаратов.

Конечно, современные летательные аппараты оснащены средствами для повышения надежности и защиты от атак потенциальных злоумышленников. Так, например, основные бортовые системы воздушных судов разделены с помощью файерволла на две части: систему управления самолетом, которой пользуются пилоты в кабине, и общую сеть салона[3]. Однако, при подключении к локальной сети, потенциальные хакеры способны взять под контроль и системы управления летательным аппаратом. Помимо этого, в процессе эксплуатации воздушного судна происходит постоянное обновление программного обеспечения, а также загрузка базы данных полетов и профилактическое обслуживание, что, потенциально, также может привести к нарушению информационной целостности и появлению уязвимостей. Наконец, не стоит исключать и случаи закладки различных «жучков» во время обслуживания летательного аппарата.

За последние 10 лет подтвержден целый ряд уязвимостей в информационных системах воздушного судна. Некоторые примеры приведены в таблице 1.

Таблица 1 – Нарушения информационной безопасности ЛА за последние 10 лет

Год	Выявленная уязвимость
2008	FAA заявила, что архитектура Boeing 787 позволяет создавать новые виды подключений к ранее изолированным сетям передачи данных, которые подключены к системам, выполняющие критически важные операции, необходимые для обеспечения безопасности полета самолета.
2010	FAA заявила, что некоторые компьютерные системы Boeing 747-8 и Boeing 747-8F могут быть уязвимы для внешних атак из-за интерфейсов их подключения.
2012	Хакер продемонстрировал уязвимость в управлении воздушным движением. Без использования дорогостоящей техники ему удалось обмануть сигналы АЗН-В так, что на экране диспетчера появился несуществующий самолет.
2013	Хакер продемонстрировал теоретическую возможность использовать Android для удаленной атаки и захвата самолета.

2014	Потенциальной уязвимостью в программировании электронных бортовых журналов могут воспользоваться киберпреступники при подключении их к внешним сетям для обновлений.
2015	Эксперт по вопросам информационной безопасности заявил, что он смог взломать и изменить направление движения воздушного судна в середине полета, вторгнувшись в систему развлечений пассажиров.
2018	Самолет WestJet передал код 7500, что обозначает угон. Возможно, данное сообщение было передано киберпреступником.

Предложенные на данный момент способы решения проблемы информационной безопасности

В настоящий момент существует несколько стандартов информационной безопасности в авионике[1]. Наиболее известными являются стандарты американской компании ARINC (Aeronautical Radio, Incorporated). Основные стандарты приведены в таблице 2.

Таблица 2 – Основные стандарты информационной безопасности в авиации

Стандарт и год принятия	Название	Описание
ARINC 811 2005	Commercial aircraft information security concepts of operation and process framework	Приведены терминологические основы информационной безопасности бортовых сетей, описан подход к оценке состояния информационной безопасности
ARINC 664 2005-2009	Aircraft data network	Приведены методы построения детерминированной бортовой сети Ethernet. Определены домены информационной безопасности на борту воздушного судна.
ED-202 DO-326 2014	Airworthiness security process specification	Приведены руководящие принципы процесса обеспечения информационной безопасности
ED-202A DO-326A 2018		
ED-203 DO-356 2014	Airworthiness security methods and considerations	Приведены методы и инструменты для достижения целей процесса обеспечения безопасности
ED-203A DO-356A 2018		
ED-204 DO-355 2014	Information Security Guidance for Continuing Airworthiness	Приведено руководство по обеспечению информационной безопасности для поддержания летной годности
ATA Spec 42 2017	Aviation industry standards for digital information security	Приведены требования к взаимной идентификации и управлению доступом между отдельными узлами и агрегатами самолета

Стандарты ARINC предлагают концепции и рекомендации для построения защищенного канала обмена информацией, стандарты серии ED предлагают рекомендации для устранения и минимизацию попыток несанкционированного доступа.

Крупнейшими компаниями, занимающимися проектированием, разработкой и исследованиями в сфере авиации, на данный момент признается необходимость некоего автоматизированного средства для контроля информационной безопасности на этапе проектирования и в течение всего жизненного цикла ЛА. На данный момент разрабатывается концепция разделения внутреннего информационного пространства летательного аппарата на домены различного уровня доступа для обеспечения информационной целостности бортовых систем, однако пока подобная схема существует только на уровне концепции и требует большого количества доработок и дополнительных исследований.

Решение проблемы информационной безопасности летательных аппаратов

К сожалению, на данный момент исследований, проводимых в этой области, недостаточно для решения этой проблемы. Актуальность проблемы информационной безопасности очевидна как для специалистов в этой области, так и для сторонних наблюдателей. В настоящее время в России разрабатывается несколько концепций систем защиты информационной безопасности летательных аппаратов, однако до полноценного комплексного решения еще далеко.

Вывод

Несмотря на то, что информационная безопасность в авиации признала одной из наиболее актуальных проблем, решений на настоящий момент предложено немного. Большинство решений сводятся к набору концепций, терминов и рекомендаций, призванных обеспечить надежную передачу информации между воздушными судами, их системами и наземными подразделениями. Для решения данного вопроса активно проводятся разработки и исследования, но пока вопрос создания централизованного решения для обеспечения информационной безопасности на протяжении жизненного цикла ЛА остается открытым.

Литература

Научный руководитель: Волосатова Тамара Михайловна, к.т.н., доцент, МГТУ им. Н.Э.Баумана, кафедра РК6, tamaravol@gmail.com

The problem of information security in the field of avionics

Kozar A.A.¹²⁶

Abstract

The article discusses theoretical issues of ensuring information security of aircraft onboard equipment. The existing problems and their solutions in the field of avionics protection are described in detail. The current tasks and the required areas of research to solve the tasks are briefly presented. The urgency of the problem of information security in the field of avionics and aviation is indicated, examples of serious security threats and the consequences of successfully compromising the information integrity of aircraft systems are given.

Keywords: aviation, avionics, cybersecurity, aircraft, airborne systems.

¹²⁶Kozar Anastasia Andreevna, graduate student of the second year of study, MSTU. N.E. Bauman Department of RK6, kozar.a.a.rk6@yandex.ru

Аналитическая модель оценки предельно достижимой емкости встраивания робастного водяного знака

Козачок А.В.,¹²⁷ Копылов С.А.,¹²⁸ Нгуен М.Т.¹²⁹

В статье представлена аналитическая модель оценки предельно достижимой емкости встраивания робастного водяного знака, основанного на подходе к внедрению информации в текстовые данные за счет изменения величины межстрочного интервала. Разработанная модель позволяет осуществить количественную оценку граничных значений объема информации, которые может содержать водяной знак, встраиваемый в текстовые данные, выводимые на печать. В ходе разработки аналитической модели установлена зависимость величины предельно достижимой емкости встраивания от количества строк текстового документа и используемых параметров встраивания водяного знака. Осуществлена оценка соответствия полученных результатов моделирования параметрам напечатанных на бумаге текстов. Получены аналитические выражения, позволяющие количественно оценить величину предельно достижимой емкости встраивания разработанного робастного водяного знака. Определены направления дальнейших исследований.

Ключевые слова: цифровой водяной знак, математическое моделирование, аппроксимация, метод наименьших квадратов.

Введение

Защита авторских прав владельцев текстовой информации является одним из наиболее актуальных направлений исследований. Анализ инцидентов нарушения безопасности, связанных с утечкой персональных данных и информации, содержащей коммерческую тайну, проведенный аналитическим центром InfoWatch, показал, что доля утечек информации, представленной в напечатанном виде, в 2018 г. возросла с 8,2% до 11%. При этом, в распределении утечек количество инцидентов, связанных с утечкой бумажных текстовых документов увеличилось до 17% [1]. Высокий процент утечек бумажной информации обусловлен наличием недостатков в существующих средствах защиты. Для устранения указанного недостатка разработан подход к маркированию текстовых электронных документов, основанный на внедрении робастного водяного знака (РВЗ) в текстовые данные [2-4].

Разработанный подход позволяет осуществить перцептивно невидимое внедрение идентификационной информации в текстовые документы в процессе вывода их на печать. Робастность разработанного подхода состоит в обеспечении инвариантности встроенных данных к преобразованию формата текстового документа в изображение посредством применения операции "печать-сканирование". Обеспечение робастности и невидимости встроенных данных разработанного РВЗ накладывает ограничение на величину емкости встраивания. Для оценки емкости встраивания необходимо разработать аналитическую модель, позволяющую количественно оценить граничные значения объема встраиваемой информации (полезной нагрузки), который может содержать разработанный РВЗ.

¹²⁷Козачок Александр Васильевич, к.т.н., Академия ФСО России, Орёл, a.kozachok@academ.msk.rsnet.ru

¹²⁸Копылов Сергей Александрович, Академия ФСО России, Орёл, gremlin.kop@mail.ru

¹²⁹Нгуен Мань Тханг, Академия ФСО России, Орёл, chieumatxcova@gmail.com

1. Зависимость количества строк текста от параметров текстового документа

Под емкостью встраивания понимается количество информации, которое может быть внедрено в текстовый документ [5-7]. В качестве количественной оценки граничного значения величины емкости встраивания выступает величина предельно достижимой емкости встраивания η подхода внедрения информации. Исходя из особенностей разработанного подхода к внедрению информации, основанного на изменении величины межстрочного интервала (положения строки текста), установлено, что η зависит от количества строк N текстового документа.

Количество строк текстового документа N , в свою очередь, зависит от таких параметров как формат бумаги текстового документа, гарнитура и размер кегля шрифта, величины интервалов и отступов текстового документа. При этом, экспериментально установлено, что наиболее близким аналитическим выражением, позволяющим рассчитать количество строк N страницы текстового документа, является выражение:

$$N = \left\lfloor \frac{H - (m_t + m_b)}{\gamma + \beta \gamma} \right\rfloor, \quad (1)$$

где H – высота текстового документа, m_t , m_b – размер верхнего и нижнего поля текстового документа, γ – размер кегля шрифта, β – величина множителя межстрочного интервала.

Для определения достоверности полученных значений количества строк текстовой информации, вычисленных посредством выражения (1), необходимо провести их сравнение со значениями количества строк, содержащихся в напечатанном на бумаге текстовом документе.

В качестве напечатанных на бумаге текстовых документов использованы официальные электронные текстовые документы, подготовленные в системе компьютерной верстки LaTeX. Под официальным документом понимается документ, созданный организацией, должностным лицом или гражданином, оформленный в установленном порядке [8]. Текстовые документы оформлены в соответствии с ГОСТ Р 7.0.97-2016 со следующими параметрами [9]:

- 1) формат бумаги – A4 (210 × 297 мм);
- 2) кегль шрифта – 10, 12, 14 пт;
- 3) межстрочный интервал – 1, 1,25, 1,5;
- 4) поля текстового документа: левое: 20 мм, правое: 10 мм, верхнее: 20 мм, нижнее: 20 мм.

В процессе формирования официального текстового документа осуществлено полное заполнение страницы текстовой информации в соответствии с указанными параметрами и гарнитурой шрифта Computer Modern Roman (свободно распространяемый шрифт, аналог Times New Roman).

Для количественной оценки количества строк официального текстового документа посредством выражения (1), использованы следующие значения:

- $H = 297$ мм (для формата бумаги A4);
- $m_t = m_b = 20$ мм;
- 1 пт = 0,376 мм (согласно типометрической системе Дидо [10]).

В ходе оценки значений количества строк получено точное соответствие количества строк, содержащихся в напечатанных текстовых документах значениям, вычисленным аналитическим методом. Результат зависимости количества строк страницы текстового документа от требований, предъявляемых к оформлению официальных документов, представлен в таблице 1.

Таблица 1.

Количество строк текстового документа		
Кегль шрифта γ (пт)	Величина межстрочного интервала β (множитель)	Количество строк текстового документа
10	1	63
10	1,25	50
10	1,5	42
12	1	52
12	1,25	42
12	1,5	35
14	1	45
14	1,25	36
14	1,5	30

Анализ полученных значений позволяет определить граничные значения количества строк страницы текстового документа. Для текстового документа формата А4 максимальное число строк полностью заполненной текстом страницы ограничено значением в 63 строки, при использовании текста с кеглем шрифта 10 пт и величиной межстрочного интервала 1. Полученные пороговые значения количества строк страницы текстового документа позволяют оценить граничные значения емкости встраивания разработанного РВЗ. Для решения данной задачи разработана аналитическая модель оценки величины предельно достижимой емкости встраивания РВЗ.

2. Аналитическая модель оценки величины предельно достижимой емкости встраивания

Исследование емкости встраивания разработанного подхода показало, что величина предельно достижимой емкости встраивания разработанного подхода зависит не только от количества строк текстового документа, но и от параметров встраивания. В подходе внедрения информации, основанном на изменении величины межстрочного интервала, в качестве параметра встраивания выступает величина изменения межстрочного интервала Δ . Число возможных изменений параметра встраивания представляет собой количество компонент встраивания λ разработанного подхода внедрения информации.

Исходя из указанных особенностей, зависимость величины предельно достижимой емкости встраивания η разработанного РВЗ может быть описана следующим образом:

$$\eta = F(N, \lambda), \quad (2)$$

где λ – количество компонент встраивания.

В процессе внедрения РВЗ реализована схема многокомпонентного встраивания. Для реализации схемы многокомпонентного встраивания использована процедура кодирования встраиваемой информации в систему счисления по основанию λ . В процессе кодирования на количество компонент λ накладывается ограничение:

$$\begin{cases} \lambda \leq (N - 1) \\ \lambda \leq 8 \\ \lambda \geq 2 \end{cases}. \quad (3)$$

Исходя из особенностей многокомпонентной схемы встраивания РВЗ, конечная формула расчета величины предельно достижимой емкости встраивания η может быть представлена в следующем виде:

$$\eta = \left\lfloor \log_2 f_{\lambda \rightarrow 2}(\lambda^{N-1} - 1) \right\rfloor, \quad (4)$$

где $f_{\lambda \rightarrow 2}$ – функция перевода числа из системы счисления λ в двоичную систему счисления.

Выражение (4) представляет собой аналитическую модель оценки величины предельно достижимой емкости встраивания РВЗ, основанного на подходе к встраиванию за счет изменения величины межстрочного интервала.

Разработанная аналитическая модель позволяет осуществить количественную оценку граничных значений емкости встраивания разработанного РВЗ. Результаты зависимости величины предельной емкости встраивания η от количества строк текста N и количества компонент встраивания λ представлены в таблице 2.

Таблица 2.

Количество строк текста N	Предельно достижимая емкость встраивания η (бит)						
	$\lambda = 2$	$\lambda = 3$	$\lambda = 4$	$\lambda = 5$	$\lambda = 6$	$\lambda = 7$	$\lambda = 8$
30	29	45	58	67	75	81	87
35	34	53	68	79	87	95	102
36	35	55	70	81	91	98	105
42	41	64	82	79	87	95	102
45	44	69	88	102	114	123	132
50	49	77	98	113	127	137	147
52	51	80	102	118	132	143	153
63	62	98	124	143	161	174	186

Анализ полученных результатов показал, что предельно достижимая емкость встраивания разработанного РВЗ ограничена значением в 186 бит (для страницы текстового документа набранной с кеглем в 10 пт и величиной межстрочного интервала 1 при использовании восьмикомпонентного встраивания). При этом, стоит отметить, что параметр λ может выступать в качестве варьируемого параметра, позволяющего управлять величиной предельно достижимой емкости встраивания, при наличии достаточного количества строк текстового документа.

Полученные количественные значения зависимости величины предельно достижимой емкости встраивания могут быть использованы в процессе математического описания величины предельно достижимой емкости встраивания разработанного РВЗ для каждой компоненты встраивания λ .

В ходе решения данной задачи использован подход к аппроксимации функции основанный на методе наименьших квадратов. Величина предельно достижимой емкости встраивания для соответствующего количества строк тестового документа и используемой компоненты встраивания, характеризуется линейной зависимостью, что позволяет использовать в качестве аппроксимирующей функции уравнение прямой вида: $f(x) = a \cdot x + b$.

Решая задачу нахождения наименьшего значения суммы квадратов отклонений:

$$\sum_{i=1}^n e_i^2 = \sum_{i=1}^n (y_i - f(x_i))^2 = \sum_{i=1}^n (y_i - (a \cdot x_i + b))^2, \quad (5)$$

получаем коэффициенты a и b , характеризующие аппроксимирующие функции наиболее близко описывающие полученные зависимости:

$$\begin{aligned} f(N_{\lambda=2}) &= N - 1 & f(N_{\lambda=3}) &= 1,59 \cdot N - 2 & f(N_{\lambda=4}) &= 2 \cdot N - 2 \\ f(N_{\lambda=5}) &= 2,31 \cdot N - 2 & f(N_{\lambda=6}) &= 2,61 \cdot N - 3 & f(N_{\lambda=7}) &= 2,81 \cdot N - 3. \\ f(N_{\lambda=8}) &= 3 \cdot N - 3 \end{aligned} \quad (6)$$

Полученные значения (выражение (6)) позволяют аналитически описать зависимость величины предельно достижимой емкости встраивания от количества строк текстового документа при использовании выбранного количества компонент.

Для оценки достоверности полученных результатов использован графический метод, в рамках которого, осуществлено построение графиков зависимостей величин предельно достижимых емкостей встраивания, полученных посредством аппроксимации, и соответствующих значениям представленным в таблице 2. Результат сравнения для $\lambda = 3$ и $\lambda = 5$ представлен на рисунке 1.

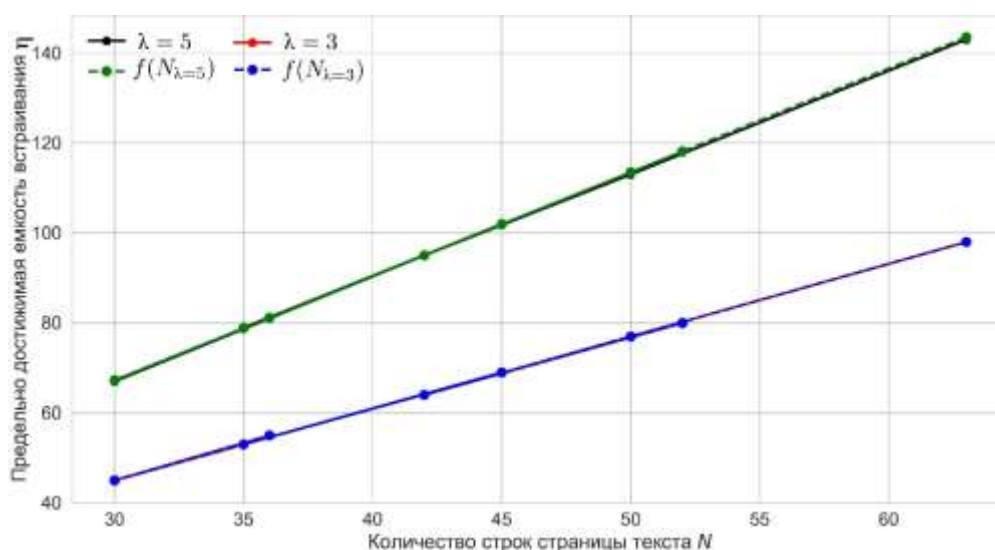


Рис. 1. Сравнение результата аппроксимации с полученными зависимостями

Проведенный анализ показал, что графики функций аппроксимации соответствуют графикам зависимостей, построенным по полученным значениям (табл. 2), что позволяет сделать вывод о возможности использования полученных аналитических выражений для определения величины предельно достижимой емкости встраивания разработанного РВЗ.

Выводы

Разработанная аналитическая модель оценки предельно достижимой емкости встраивания позволяет определить граничные значения емкости встраивания разработанного РВЗ. Полученные значения предельно достижимой емкости встраивания позволяют использовать в качестве встраиваемой информации идентификатор, который может содержать идентификационные данные пользователя, метку конфиденциальности данных и другую метаинформацию необходимую для идентификации владельца данных или источника утечки. Для повышения надежности извлечения встроенного идентификатора могут быть использованы методы помехоустойчивого кодирования. Применение данной технологии в процессе формирования РВЗ является направлением дальнейших исследований.

Литература

1. Через бумажные документы случается каждая девятая утечка конфиденциальных данных // Аналитический центр InfoWatch. 2019. URL: <https://www.infowatch.ru/analytics/digest/15511> (дата обр. 03.06.2019)
2. Kozachok A.V., Kopylov S.A., Shelupanov A. A., Evsutin O. O. Text marking approach for data leakage prevention // Journal of Computer Virology and Hacking Techniques. 2019. Vol. 15. no. 3. pp. 219-232. DOI: 10.1007/s11416-019-00336-9.
3. Подход к извлечению робастного водяного знака из изображений, содержащих текст / А. Козачок [и др.] // Труды СПИИРАН. 2018. № 5(60). С. 128-155. DOI: 10.15622/sp.60.5.

4. Козачок А.В., Копылов С.А. Подход к маркированию текстовых электронных документов и его сравнение с существующими аналогами // Доклады ТУСУР. 2019. Т. 22. № 2. С. 52-60. DOI: 10.21293/1818-0442-2019-22-2-52-60
5. Salomon D. Data privacy and security: encryption and information hiding // Springer Science & Business Media, 2003. 469 p.
6. Woo C.-S. Digital image watermarking methods for copyright protection and authentication. // Queensland University of Technology. 2007. 197 p.
7. Phadikar A. Robust Watermarking Techniques for Color Images. April. 2009. 20 p.
8. ГОСТ Р 7.0.8–2013 Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения // Москва : Стандартинформ. 2014. 32 с.
9. ГОСТ Р 7.0.97–2016: Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов // Москва : Стандартинформ. 2019. 16 с.
10. Brogain S.O. Typographic measurement: A critique and a proposal // Professional Printer: Journal of the Institute of Printing. 1983. Vol. 12. no. 5. pp. 9-14.

An Analytical Model of the Limit Achievable Embedding Capacity Evaluation for Robust Watermark

Kozachok A. V.¹³⁰, Kopylov S.A.¹³¹, Nguyen M.T.¹³²

The article describes an analytical model of the limit achievable embedding capacity evaluation for robust watermark based on the approach to information embedding in text data by line space shifting. The developed model allows to boundary values assessment of information amount that may contain a watermark embedded into text data printed. In the developing process of an analytical model, the dependence of limit achievable embedding capacity on the lines amount of a text document and the used watermark embedding parameters was established. The evaluation of obtained simulation results correspondence to the parameters of texts printed on paper is implemented. Analytical expressions that make possible to quantify the limit achievable embedding capacity value of the developed robust watermark are obtained. The further research directions are determined.

Keywords: robust watermark, mathematical modelling, approximation, least squares method.

¹³⁰Kozachok Alexander Vasilevich, Ph. D., Academy of Federal Guard Service, Oryol, a.kozachok@academ.msk.rnet.ru

¹³¹Kopylov Sergey Alexandrovich, Academy of Federal Guard Service, Oryol, gremlin.kop@mail.ru

¹³²Nguyen Manh Thang, Academy of Federal Guard Service, Oryol, chieumatxcova@gmail.com

Подходы к классификации псевдослучайных последовательностей

Козачок А.В.¹³³, Спирин А.А.¹³⁴.

Современные системы защиты информации от утечек позволяют передавать любые данные в зашифрованном или сжатом виде, что приводит к утечке конфиденциальных данных и разглашению защищаемой информации. В работе рассмотрено два подхода к классификации псевдослучайных последовательностей, сформированных алгоритмами сжатия, шифрования и генераторами псевдослучайных чисел: на основе статистических тестов NIST и на основе подсчета количества бинарных подпоследовательностей длины N бит. Предложенный подход к формированию признакового пространства и классификации псевдослучайных последовательностей позволил получить значение точности классификации равное 0.98 на указанной в работе выборке данных.

Ключевые слова: статистический анализ данных, машинное обучение, тесты NIST

Введение

В последнее время, согласно отчетам информационно-аналитических агентств, возросло количество инцидентов, связанных с утечкой информации по вине внутренних нарушителей [1].

В настоящее время применяются методы психологического диагностирования [2], которые могут выявить мотивированных на кражу конфиденциальных данных сотрудников, однако, выявить немотивированных сотрудников достаточно затруднительно.

При этом программно-аппаратные средства защиты от утечек информации не имеют механизмов анализа зашифрованных или сжатых данных, в случае отсутствия информации об алгоритме сжатия [3]. Основным направлением обнаружения последовательностей, сформированных алгоритмами шифрования или сжатия, далее – псевдослучайные последовательности (ПСП), являются методы статистического анализа.

Была выдвинута гипотеза о возможности классификации ПСП на основе их статистических свойств.

Формальная постановка задачи

В общем виде задача классификации ПСП представлена в выражении 1 и формулируется следующим образом: необходимо исходное множество битовых последовательностей X отобразить на множество классов Y на основе выбранного признакового пространства.

$$F: X \rightarrow Y, \quad (1)$$

где X – исходное множество бинарных последовательностей, подлежащих классификации, Y – множество классов.

Множество классов Y включает в себя:

1. Зашифрованные последовательности.
2. Сжатые последовательности.
3. Сжатые последовательности с паролем.
4. Последовательности, сформированные генераторами случайных чисел.

Для оценки качества классификации была использована метрика доля правильных ответов, в общем виде определяемая выражением 2:

¹³³ Козачок Александр Васильевич, к.т.н., Академия ФСО России, Орел, tottrin@list.ru

¹³⁴ Спирин Андрей Андреевич, Академия ФСО России, Орел, spirin_aa@bk.ru

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \quad (2)$$

где TP – количество объектов, верно отнесенных к классу $y_j \in Y$, TN – количество объектов, верно отнесенных не к классу $y_j \in Y$, FP – количество ложных срабатываний (ошибка первого рода), т.е. количество объектов неверно отнесенных к классу $y_j \in Y$, FN – количество пропусков цели (ошибка второго рода), т.е. количество объектов неверно не отнесенных к классу $y_j \in Y$.

Для выборки, состоящей из K классов ПСП, доля правильных ответов классификатора определяется выражением 3:

$$Accuracy_{total} = \frac{\sum_{j=1}^K Accuracy_{y_j}}{K}, \quad (3)$$

где $Accuracy_{y_j}$ – доля правильных ответов для класса y_j .

Для определения доли правильных ответов каждого класса строится матрица ошибок, представленная на рисунке 1.

		Истинный класс			
		1	2	3	4
Предсказанный класс	1	TP_1	FP_12	FP_13	FP_14
	2	FN_21	TP_2	FP_23	FP_24
	3	FN_31	FN_32	TP_3	FP_34
	4	FN_41	FN_42	FN_43	TP_4

Рис.1. Матрица ошибок при классификации 4 классов ПСП.

Значение доли правильных ответов при классификации должно удовлетворять условию, представленному в выражении 4:

$$p(F(x_i) = y_j | i = j) \rightarrow \max, \quad (4)$$

где p – вероятность верного отнесения ПСП x_i из множества X к метке классов y_j , $F(x_i)$ – функция отображения i -го файла множества X , y_j – метки класса из множества Y ; i, j – индексы во множестве X и Y соответственно.

Построение признакового пространства на основе тестов NIST

Для проверки возможности решения задачи классификации был использован пакет статистических тестов NIST SP 800-22rev1a [4], применяемый для оценки генераторов случайных и псевдослучайных последовательностей в криптографии.

Для проведения эксперимента исходное множество 1000 файлов по 600 Кбайт текста на русском языке, было преобразовано алгоритмами шифрования и сжатия. В результате была получена выборка из 4000 файлов, которая была разделена на 2 класса:

1. Зашифрованные алгоритмами AES, 3DES.
2. Архивы RAR, ZIP.

Далее файлы из выборки были обработаны пакетом статистических тестов, в результате для каждого файла было получено по 188 значений признаков, представляющих собой вычисленные значения P-value. Вычисленные значения P-value наиболее значимых тестов NIST для архивов RAR и ZIP представлены в таблице 1.

Таблица 1.

Вычисленные в результате проведения
тестов NIST средние значения P-value для архивов RAR и ZIP

	Frequency	Block Frequency	Cumulative Sums#1	Cumulative Sums#2	Runs	Longest Run
RAR	0,049	0,155	0,020	0,020	0,017	0,139
ZIP	0,032	0,207	0,021	0,017	0,042	0,429
	Rank	FFT	Serial#1	Serial#2	Linear Complexity	
RAR	0,487	0,490	0,027	0,346	0,501	
ZIP	0,491	0,484	0,344	0,486	0,509	

Для оценки случайности анализируемых тестами NIST ПСП полученные значения P-value сравнивают с пороговым значением 0.01, в случае если вычисленное значение P-value больше указанного порогового значение принимается гипотеза о случайности анализируемой ПСП, в противном случае эта гипотеза отвергается.

Для оценки применимости выбранного признакового пространства использовалась кросс-валидация алгоритмов машинного обучения с параметрами по умолчанию [5-9]: классификатор деревьев решений (КДР), классификатор на основе случайного леса (КСЛ). Результаты проведенных экспериментов представлены в таблице 2.

Таблица 2.

Доля правильных ответов при классификации сжатых и шифрованных ПСП
алгоритмами машинного обучения на основе признакового пространства по результатам
тестов NIST

№ п/п	Алгоритм	Значение доли правильных ответов
1	Дерево решений	0,58
2	Случайный лес	0,64

Из анализа значений, представленных в таблице 1 можно сделать вывод о том, что признаковое пространство на основе результатов тестов NIST не позволяет решить задачу бинарной классификации с учетом выбранных ограничений.

Построение признакового пространства на основе подсчета частоты встречаемости подпоследовательностей длины N бит

Было выдвинуто предположение о том, что в качестве признакового пространства, для решения задачи классификации ПСП, могут быть использованы результаты анализа частоты встречаемости независимых битовых подпоследовательностей различной длины N (в битах) без учета полного перекрытия каждой подпоследовательности. Например, для

последовательности S=00011011 частота вхождения подпоследовательностей длины N=2 битам представлена в таблице 2.

Таблица 2.

Пример подсчета частот битовых подпоследовательностей

Подпоследовательность	Кол-во	Частота
00	1	0,143
01	2	0,29
10	1	0,143
11	2	0,29

С целью проверки предположения о возможности построения многоклассового классификатора исходная выборка была дополнена файлами, сформированными утилитой urandom операционной системы семейства Linux [11] и разделена на 4 класса:

1. Зашифрованные алгоритмами AES, 3DES, RC4, Camellia [12].
2. Архивы RAR, ZIP [13].
3. Зашифрованные архивы RAR, ZIP [13].
4. ПСП, сформированные утилитой urandom.

Поскольку полученные значения частоты встречаемости битовых подпоследовательностей длины N бит являются достаточно малыми величинами ($\leq 10^5 \dots 10^6$), то было выдвинуто предположение о том, что переход к логарифмическому масштабу значений может повысить точность классификации (КДРЛ, КСЛЛ).

Зависимость доли правильных ответов при классификации ПСП, отнесенных к 4 классам, от длины подпоследовательности представлена на рисунке 1.

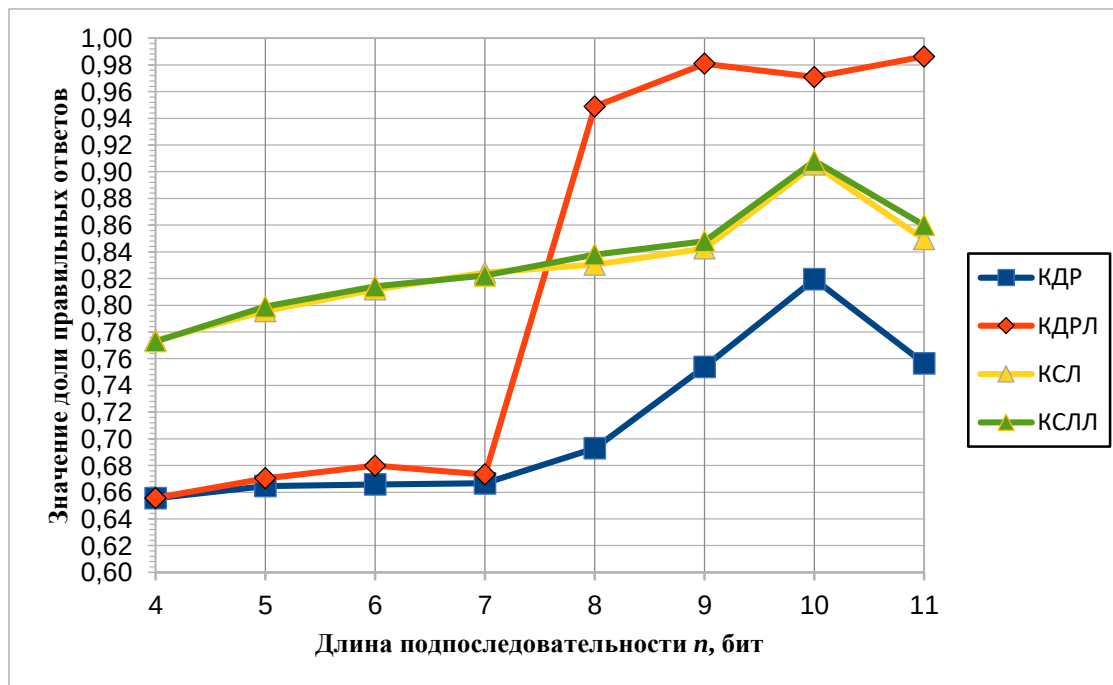


Рис. 1. Доля правильных ответов при классификации ПСП, отнесенных к 4 классам.

Из рисунка 1 видно, что применение лог-признаков дает прирост точности классификации ПСП при использовании КДР. При длине подпоследовательности N=9 бит доля правильных ответов составила 0,98.

Выводы

Для построения классификатора ПСП (4 класса) было рассмотрено два способа формирования признакового пространства: на основе тестов NIST и на основе подсчета количества подпоследовательностей длины N бит. Для формирования классификатора использовались алгоритмы машинного обучения на основе дерева решений и случайного леса. На основе полученных результатов был выбран алгоритм дерева решений, использующий в качестве признакового пространства частоты встречаемости подпоследовательностей длины N бит в логарифмическом масштабе. Точность предложенного подхода на указанных в работе данных составила 0.98.

Литература:

1. Глобальное исследование утечек конфиденциальной информации в 2018 году. Сайт группы компаний InfoWatch. URL: <https://www.infowatch.ru/analytics/reports> (дата обращения: 14.11.2019).
2. Обухов А. Н. О применении полиграфа в интересах выявления инсайдерских угроз информационной безопасности //Безопасность информационных технологий. – 2017. – Т. 24. – №. 3. – С. 60-66.
3. Huang X. et al. A novel mechanism for fast detection of transformed data leakage //IEEE Access. – 2018. – Т. 6. – С. 35926-35936.
4. NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications/ [A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo]. National Institute of Standards and Technology, 2010.
5. Pedregosa F. et al. Scikit-learn: Machine learning in Python //Journal of machine learning research. – 2011. – Т. 12. – №. Oct. – С. 2825-2830.
6. Breiman L. Classification and regression trees. – Routledge, 2017.
7. Hastie T. et al. The elements of statistical learning: data mining, inference and prediction //The Mathematical Intelligencer. – 2005. – Т. 27. – №. 2. – С. 83-85.
8. Breiman L. Random forests //Machine learning. – 2001. – Т. 45. – №. 1. – С. 5-32.
9. Рашка С. Python и машинное обучение //М.: ДМК Пресс. – 2017.
10. Linux programmer's manual. URL: <http://man7.org/linux/man-pages/man4/random.4.html> (дата обращения: 14.01.2019).
11. Toolkit for the transport layer security and secure sockets layer protocols.
12. URL: <http://openssl.org> (дата обращения: 14.01.2019).
13. Archive manager WinRAR. URL: <http://rarlab.com> (дата обращения: 14.01.2019).

Approaches to the classification of pseudo-random sequences

Kozachok A.V.¹³⁵, Spirin A.A.¹³⁶

Modern systems of information protection against leaks allow to transfer any data in encrypted or compressed form, which leads to the leakage of confidential data and disclosure of protected information. The paper considers two approaches to classification of pseudorandom sequences formed by compression, encryption algorithms and pseudorandom number generators: on the basis of NIST statistical tests and on the basis of counting the number of binary subsequences of length n bits. The proposed approach to the formation of the feature space and classification of pseudorandom sequences demonstrated a classification accuracy of 0.98 on the data sample specified in the work.

Keywords: statistical data analysis, machine learning, NIST tests

¹³⁵ Alexander Kozachok, Ph.D., Academy of Federal Guard Service, Orel, tottrin@list.ru

¹³⁶ Andrey Spirin, Academy of Federal Guard Service, Orel, spirin_aa@bk.ru

Метод представления информации об инцидентах информационной безопасности

Козлов Д.В.¹³⁷

С ростом числа информационных систем и совершенствованием информационных технологий растёт и число инцидентов информационной безопасности (ИБ), под которыми понимается любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность автоматизированной системы управления (АСУ). Международный стандарт ISO 27001:2005 обращает особое внимание на необходимость создания процедуры управления инцидентами ИБ – очевидно, что без своевременного реагирования на инциденты ИБ, устранения их последствий и возможных причин невозможно эффективное управление информационной безопасностью. В связи с этим лучшей защитой АСУ будет разработка и внедрение таких средств и мер защиты, которые позволят в лучшем случае – не допустить инцидент, в другом случае – своевременно выявить, оперативно отреагировать и провести анализ инцидента. Именно анализ инцидента поможет выявить уязвимые места системы, знание которых в свою очередь позволит усовершенствовать системы защиты и не допустить подобные инциденты в будущем.

Ключевые слова: база данных, прецедент, реагирование, автоматизированная система управления, компьютерные атаки.

Введение

Развитие информационных технологий позволяет охватывать все больше каналов цифровых коммуникаций, хранить значительные массивы информации для последующего анализа, что значительно расширяет возможности расследования нарушений, поиска косвенных признаков мошенничества, выявления закономерностей и аномалий. Обратной стороной этих возможностей становится увеличение потока событий ИБ в АСУ, требующих внимания специалиста по безопасности, поэтому современные системы реагирования должны иметь развитые средства автоматизации управления жизненным циклом инцидента, элементы базы данных, инструменты поиска и анализа информации на достаточную для проведения расследования глубину.

Основной целью метода представления информации об инцидентах ИБ является повышение эффективности автоматического расследования инцидентов ИБ и, как следствие, уменьшение времени реагирования на инциденты ИБ за счет формирования базы данных прецедентов.

Предлагаемый метод

Прецедент – это запись в базе данных (БД) прецедентов, содержащая описание инцидента и его решения. База данных прецедентов является помощником эксперта по безопасности, которому необходимо следить за безопасностью автоматизированной системы управления и принимать меры по предупреждению и предотвращению угроз и связанных с ними последствий.

Сущностью метода является накопление и повторное использование данных об инцидентах ИБ в АСУ путем создания БД прецедентов.

В основе метода представления информации об инцидентах ИБ предлагается использовать подход, основанный на анализе формальных понятий [1, 2]. Данный подход позволяет представить структуру данных как множество классов, объекты которых ссылаются друг на друга.

¹³⁷Козлов Денис Викторович, начальник отделения - инструктор практического обучения базы обеспечения учебного процесса Военной академии воздушно-космической обороны, Тверь, lujnikovo@mail.ru

Каждый прецедент описывается алгебраической системой:

$$P = (A, \sigma), \quad (1)$$

где A – основное множество алгебраической системы, а σ – её сигнатура. Сигнатура σ – это множество понятий, на языке которых описывается данная предметная область: множество различных уязвимостей, угроз, контрмер, последствий и т.п. Будем считать, что у всех прецедентов компьютерных атак сигнатура одна. Обогатим сигнатуру σ добавив для каждого элемента a константу c_a : обозначим:

$$\sigma_A = \sigma \cup \{c_a \mid a \in A\}, \quad (2)$$

Таким образом, алгебраические системы, с помощью которых мы описываем экземпляры данной предметной области, принадлежат множеству:

$$K(\sigma_A) = \{P = (\{c_a^P \mid a \in A\}, \sigma_A) \mid c_a^P \neq c_b^P \text{ при } a \neq b\} \quad (3)$$

В качестве объектов мы будем рассматривать прецеденты, а в качестве атрибутов – шесть категорий признаков: симптомы, угрозы, уязвимости, последствия, потери и контрмеры. Отношение между ними – обладание прецедента каким-либо признаком из категории.

На рис.1 показана схема системы автоматического расследования ИБ [3]. Система включает в себя: средство загрузки данных о системных событиях 1, сервер администрирования 2, средство управления событиями 3, средство поиска решений 4, аналитический модуль описания прецедентов 5 и база данных прецедентов 6.



Рис. 1. Схема системы автоматического расследования ИБ

Средство поиска решений 4 включает в себя: аналитический модуль описания прецедентов 5 и БД прецедентов 6.

Система может быть установлена на сервер администрирования 2 и вместе с ним подключена к компьютерной сети.

Основным назначением средства управления событиями 3 является: загрузка данных о системных событиях 1 с компьютерных устройств пользователей, подключенных к серверу администрирования; обнаружение и регистрация факта возникновения инцидента; анализ событий.

Начальные события определяются в качестве причин возникновения инцидента безопасности, и именно для них требуется найти решение, которое предотвратит в дальнейшем повторение инцидента и исправит его последствия.

Как уже отмечалось ранее, средство поиска решений 4 включает в себя: аналитический модуль описания прецедентов 5 и база данных прецедентов 6.

Аналитический модуль описания прецедентов 5 служит для: формализации прецедентов; поиска прецедентов в базе данных прецедентов; актуализация прецедентов; предоставление знаний.

Для организации БД прецедентов 6 и работы с ней было решено использовать технологию процесса «Описание прецедентов», формализующего процедуры накопления и использования данных об инцидентах [4, 5].

В данной технологии используется объектно-ориентированная структура данных, и основными понятиями здесь являются Класс, Объект и Свойство [4-6]. Под Классом понимается множество объектов, при этом объект имеет возможность явно принадлежать многим классам. Существует два вида Свойств: *t*-свойство и *o*-свойство. Если значением является значение типа (строка, целое число и т.п.), то свойство называется *t*-свойством. Если значением является объект, то свойство называется *o*-свойством.

Для описания прецедентов в БД создано шесть категорий признаков (Классов) – Симптомы, Угрозы, Уязвимости, Последствия, Потери и Контрмеры. Каждая из шести категорий признаков, применяемых для описания прецедентов компьютерных атак, представлена в базе знаний в виде древовидной структуры. Каждый прецедент в базе характеризуется обладанием определенных признаков из каждой категории. При обращении к конкретному прецеденту происходит считывание его базы данных множества признаков, которыми он обладает. По полученному множеству строится 3 списка признаков для прецедента:

- (+) – список всех признаков из БД, которыми обладает прецедент;
- (–) – список всех признаков из БД, которыми прецедент не обладает;
- (?) – список тех признаков из БД, обладание которыми не определено для прецедента.

Схема заполнения списков следующая. Все признаки вверх по дереву от признака, обладание которым задано в БД, заносятся в список признаков, которыми прецедент обладает. Все признаки вниз по дереву от признака, обладание которым задано в БД, заносятся в список признаков, обладание которыми для данного прецедента не определено. Остальные признаки заносятся в список тех признаков, которыми прецедент не обладает.

Для пополнения данных, хранящихся в БД, важно обнаружить связь между существующими прецедентами, исходя из сходства их признаков; предсказать обладание интересующими признаками ранее представленных прецедентов.

Обновление БД прецедентов происходит с серверов антивирусных программ, а также используются RSS каналы сайтов.

Вывод

Основываясь на описанном выше методе, разработан алгоритм анализа инцидентов ИБ в АСУ. Согласно данному алгоритму каждое действие описывается через имя и набор объектов: объект, над которым совершается действие; субъект, который его выполняет; компоненты – другие объекты, которые в нем участвуют. Описание структур действий с использованием абстрактных понятий позволяет рассмотреть не одну только ситуацию, а целый класс ситуаций. Таким образом, объединение концептуальных структур инцидентов в единое целое образует событийную концептуальную модель предметной области, которая представляется в виде БД прецедентов.

Вся исходная информация о прецедентах компьютерных атак хранится в БД системы. Более того, при пополнении БД, создаются новые прецеденты, и система в автоматическом режиме находит необходимые контрмеры для ликвидации этих нежелательных событий, что в свою очередь позволяет сократить время реакции системы на инциденты ИБ.

Литература

1. Мойсеев Н.Н. Математические задачи системного анализа. М.: Наука, 1981. 487 с.
2. Катулев А.Н., Северцев Н.А. Математические методы в системах поддержки принятия решений: Учеб. пособие. М.: Высшая школа, 2005. 311 с: ил. - ISBN5-06-004754-7.
3. Пат. 2664018. Российская Федерация, МПК G06F 21/55 (2013.01). Система и способ автоматического расследования инцидентов безопасности в автоматизированной системе / Козлов Д.В. – 2017121961, заявл. 21.06.2017, опубл. 14.08.2018, Бюл. 23.
4. Больных А.А. Построение онтологической модели компонентов информационной системы / Всероссийская науч.-практ. конф. «Технологии интернет — на службу обществу» // Сб. ст. - Саратов: СГТУ, 2004. - С. 107-110. - ISBN5-7433-1222-2.140.
5. Больных А.А., Старых В.А. Разработка методики моделирования систем управления информационными системами / Всероссийская науч.-практ. конф. «Технологии Интернет — на службу обществу»: Сб. ст. - Саратов: СГТУ, 2005. - С.136-140. - ISBN5-7433-1549-3.
6. Старых В.А., Болотова Л.С., Смолянинова В.А., Больных А.А. Обеспечение качества принятия решений в информационных системах с управлением: Тр. XIV Всероссийской науч.-метод. конф. «Телематика 2007». - Т. 2. – С-Пб.: Университетские телекоммуникации, 2007. - С. 313-315. - ISBN5-7577-0329-6.

Научный руководитель: Дроботун Евгений Борисович, д.т.н., профессор кафедры Военной академии воздушно-космической обороны, drobotun@xakep.ru

Presentation Method about information security incidents Kozlov D.V.¹³⁸

With the increase in the number of information systems and the improvement of information technologies, the number of information security (IS) incidents is also growing, which means any unforeseen or undesirable event that could violate the activities or information security of the automated control system (ACS).

International standard ISO 27001: 2005 pays special attention on the need to create a procedure for managing IS incidents - it is obvious that without a timely response to IS incidents, eliminating their consequences and possible reasons, it is impossible to effectively manage information security.

In this regard, the best protection for ACS will be the development and implementation of such means and protective measures that will allow, in the best case, to prevent an incident, in the other case, to timely identify, quickly respond and analyze the incident. It is the analysis of the incident that will help to identify vulnerabilities in the system, the knowledge of which in turn will improve security systems and prevent similar incidents in the future.

Keywords: database, precedent, response, automated control system, computer attacks.

¹³⁸ Kozlov Denis Viktorovich, head of the department – instructor of practical training for the educational process support base of the Military academy of aerospace defense, Tver, lujnikovo@mail.ru

Исследование возможностей системы Agda в создании верифицированного генератора псевдослучайных чисел

Кокорин А.О.¹³⁹

В работе сделан обзор возможностей системы Agda в верификации свойств генераторов псевдослучайных чисел. Рассмотрены способы создания алгебраических конструкций для проведения верификации в системе Agda. Были проанализированы способы задания поля, позволяющих реализовать эффективные операции поля и проводить доказательство их свойств: на основе конечного множества и с использованием отношения нестрогого частичного порядка. Были выделены свойства генераторов псевдослучайных чисел, поддающихся верификации с помощью систем доказательства. На базе этой работы возможно проведение верификации основных свойств генераторов псевдослучайных чисел.

Ключевые слова: верифицированное программное обеспечение, интерактивные системы доказательства, объединяющая теория типов Ло Чжаохуэя

Введение. Источниками случайных чисел могут служить физические явления, такие как время между последовательными событиями в процессе атомного распада, тепловой шум в полупроводниках, дробовой шум в резисторе или космическое излучение. Ключевой проблемой при создании ГСЧ с использованием физического устройства является то, что получаемые числа должны быть приближены к независимым и равномерно распределённым случайным величинам. В случае, если устройство генерирует поток бит, то каждый бит должен быть равен нулю или единице с равной вероятностью и должен быть независим от остальных битов. В общем случае, это не может быть доказано, таким образом, следует использовать эмпирические статистические тесты для того, чтобы убедиться в том, что получаемые числа имеют желаемые статистические свойства.

У физических источников случайных чисел есть ряд недостатков по сравнению с генераторами псевдослучайных чисел:

- время и трудозатраты при установке и настройке;
- высокая стоимость;
- низкая скорость получения случайных чисел;
- невозможность воспроизведения ранее сгенерированной последовательности случайных чисел [1].

На практике физические генераторы случайных чисел используются для выработки порождающего элемента для генераторов псевдослучайных чисел, которые реализуются программно.

Важность задачи обуславливает высокую цену ошибок реализации. В частности, алгоритм RANDU, долгое время использовавшийся на мейнфреймах, не удовлетворяет спектральному критерию [2], что вызвало сомнения в достоверности результатов многих исследований, использовавших этот алгоритм.

Возникает задача верификации генераторов псевдослучайных чисел. Для сведения риска возникновения недостатков реализации к минимуму следует доказать, что реализация алгоритма удовлетворяет заданным свойствам. Для решения этой задачи можно использовать системы автоматического или интерактивного доказательства, такие как Coq, Epigram или Agda. Системы доказательства успешно применяются для верификации промышленного программного обеспечения [3].

¹³⁹ Кокорин Артём Олегович, студент МГТУ им. Н.Э.Баумана, Москва, xx.artem-kokorin@mail.ru

В данной работе рассматривается интерактивная система доказательства Agda. Agda является функциональным языком программирования с развитой системой зависимых типов, который основан на Haskell. Несмотря на то, что Haskell является языком с зависимыми типами, не все программы Agda могут быть переписаны на Haskell [4]. Также Agda является интерактивной системой доказательства теорем, использующей соответствие Карри — Ховарда и базируется на *объединяющей теории типов Ло Чжаохуэя* [5].

Линейный конгруэнтный метод. Линейный конгруэнтный метод был предложен Д. Г. Лемером в 1949 году [6]. Последовательность случайных чисел $\langle X_n \rangle$ задаётся следующим образом:

$$X_{n+1} = (aX_n + c) \bmod m, n \geq 0 \quad (1)$$

где:

- m , модуль; $0 < m$;
- a , множитель; $0 \leq a < m$;
- c , инкремент; $0 \leq c < m$;
- X_0 , стартовое значение; $0 \leq X_0 < m$.

Эта последовательность называется линейной конгруэнтной последовательностью. Из-за простоты операций (одно умножение, одно сложение, одно взятие по модулю) этот метод является очень быстрым. Применяется в простых случаях и не обладает криптографической стойкостью. Входит в стандартные библиотеки различных компиляторов.

Метод генерации линейной конгруэнтной последовательности при $c = 0$ называют *мультипликативным конгруэнтным методом*, а при $c \neq 0$ — *смешанным конгруэнтным методом*. При $c = 0$ генерируемые числа будут иметь меньший период, чем при $c \neq 0$, но при определённых условиях можно получить период длиной $m - 1$, если m — простое число. Чтобы гарантировать максимальность цикла повторения последовательности при $c = 0$, необходимо в качестве значения параметра m выбирать простое число. Примером такого генератора является минимальный стандартный генератор случайных чисел, предложенный Стивеном Парком и Кейтом Миллером в 1988 году [7]. Для него $a = 16807$, $m = 2147483647$.

Для данной работы ключевым фактом является то, что линейный конгруэнтный метод описывается при помощи простых математических конструкций, следовательно, подходит для формального доказательства. Смешанный конгруэнтный метод основывается на поле, а мультипликативный конгруэнтный метод — на группе. Таким образом, базой для доказательства должны служить конструкции группы и поля.

Длина периода линейного конгруэнтного метода. Линейная конгруэнтная последовательность, определенная числами m , a , c и X_0 периодична с периодом, не превышающим m . При этом длина периода равна m тогда и только тогда, когда:

- числа c и m взаимно простые;
- $b = a - 1$ кратно p для каждого простого p , являющегося делителем m ;
- b кратно 4, если m кратно 4.

Наличие этого свойства для случая $m = 2^e$, где e — число битов в машинном слове, было доказано М. Гринбергом [8]. Наличие этого свойства для общего случая и достаточность условий были доказаны Т. Е. Халлом и А. Р. Добеллом [9].

Возможности системы Agda для верификации линейного конгруэнтного метода. Стандартная библиотека Agda содержит определения и теоремы (или объявления и функции), которые требуются для написания как программ, так и доказательств.

Так как конечному полю соответствуют аддитивная и мультипликативная коммутативные группы, то для верификации свойств конгруэнтного метода будет полезно определение абелевой группы из модуля Algebra.Structures:

```
record IsAbelianGroup (· : Op2 A)
  (ε : A) (⁻¹ : Op1 A) : Set (a ⊔ ℓ) where
  field
    isGroup : IsGroup · ε ⁻¹
    comm    : Commutative ·
```

В стандартной библиотеке также объявляются конечные множества в модуле Data.Fin.Base:

```
data Fin : ℕ → Set where
  zero : {n : ℕ} → Fin (suc n)
  suc   : {n : ℕ} (i : Fin n) → Fin (suc n)
```

Для конечного множества Fin в стандартной библиотеке Agda формализовано несколько базовых свойств. На основе конечного множества возможна реализация операций поля (для данной работы требуются операции умножения и сложения). Однако из-за того, что ограничивающий параметр n меняется при использовании конструктора suc, то сложность задачи прибавления единицы составит O(n):

```
try-suc : ∀ {n} → Fin n → Maybe (Fin n)
```

```
try-suc (suc x) = Maybe.map suc (try-suc x)
```

```
try-suc {suc n} zero with n
```

```
... | zero = nothing
```

```
... | suc _ = just (suc zero)
```

```
suc-flip : ∀ {n} → Fin n → Fin n × Bool
```

```
suc-flip {suc n} x = maybe (_, false) (zero , true) (try-suc x)
```

```
suc-flip {zero} ()
```

Алгоритма, реализующего операцию инкремента за меньшее асимптотическое время, найдено не было. Для обхода этой проблемы можно применить другое описание:

```
data ≥_ (m : ℕ) : ℕ → Set where
  m ≥ m : m ≥ m
  m ≥ p : ∀ {n} → m ≥ suc n → m ≥ n
```

Эта реализация конечного множества позволяет определять операции поля более эффективно. Следует учесть, что Agda позволяет создавать верифицированные структуры данных, однако для доказательства их свойств следует использовать различные приёмы, например, приём сохранения инварианта [10]. Поэтому эффективная реализация, которая к тому же позволит проводить доказательство, может отличаться от наивной реализации.

Вывод. Для реализации верифицированного генератора псевдослучайных чисел подходит линейный конгруэнтный метод. Система Agda содержит описание алгебраических структур для доказательства его свойств, таким образом, её можно использовать для верификации свойств генератора псевдослучайных чисел. Для эффективной реализации следует использовать тип неравенства, причём в этом случае эффективными получаются не только алгоритмы, но и теоремы.

Литература

1. Pierre L'Ecuyer D'epartement d'Informatique et de Recherche Op'erationnelle, Universit'e de Montr'eal, C.P. 6128, Succ. Centre-Ville, Montr'eal (Qu'ebec), H9S 5B8, Canada.
2. Marsaglia, George (1968). "[Random Numbers Fall Mainly in the Planes](#)". *Proc. Natl. Acad. Sci. U.S.A.* 61 (1): 25–28. doi:[10.1073/pnas.61.1.25](#).
3. Breitner, Joachim, Antal Spector-Zabusky, Yao Li, Christine Rizkallah, John Wiegley, and Stephanie Weirich. 2018. "Ready, Set, Verify! Applying Hs-to-coq to Real-world Haskell Code (Experience Report)." *Proc. ACM Program. Lang.* 2 (ICFP) (July): 89:1–89:16. doi:[10.1145/3236784](#).
4. Weirich, Stephanie. 2014. "Depending on Types." In *Proceedings of the 19th ACM SIGPLAN International Conference on Functional Programming*, 241–241. ICFP '14. New York, NY, USA: ACM. doi:[10.1145/2628136.2631168](#).
5. Zhaohui L. A unifying theory of dependent types: the schematic approach // *Proceedings of Logical Foundations of Computer Science – Tver '92*. 1992. Vol-620, pp. 293–304. doi:[10.1007/BFb0023883](#).
6. D. H. Lehmer, Mathematical methods in large-scale computing units, *Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery*, 1949, Harvard University Press, Cambridge, Mass., 1951, C. 141—146. MR 0044899 (13,495f).
7. Stephen K. Park and Keith W. Miller (1988). Random Number Generators: Good Ones Are Hard To Find. *Communications of the ACM* 31 (10): 1192—1201.
8. M. Greenberger, Method in randomness, *Comm. ACM* 8 (1965), 177—179.
9. T.E. Hull and A.R. Dobell «Random Number Generators», *SIAM Review* 4-3(1962), 230-254
10. McBride, Conor Thomas. 2014. "How to Keep Your Neighbours in Order." In *Proceedings of the 19th ACM SIGPLAN International Conference on Functional Programming*, 297–309. ICFP '14. New York, NY, USA: ACM. doi:[10.1145/2628136.2628163](#).

Научный руководитель: Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., доцент кафедры «Информационная безопасность», lebedevan@bmstu.ru

Research of capabilities of the Agda system in creation of a verified pseudorandom number generator

Kokorin A.O.¹⁴⁰

The paper reviews the capabilities of the Agda system in verifying the properties of pseudorandom number generators. Methods of creating algebraic constructions for verification in the Agda system were analysed. The methods of field assignment that allow to implement effective field operations and to prove their properties were analyzed: on the basis of a finite set and using a partial order relation. The properties of pseudorandom number generators that can be verified with the help of proof systems were identified. On the basis of this work it is possible to verify the basic properties of pseudorandom number generators.

Keywords: verified software, interactive proof systems, unifying Luo Zhaohui type theory.

¹⁴⁰ Artem Kokorin, BMSTU, Moscow, xx.artem-kokorin@mail.ru

К вопросу об определении «вредоносного программного обеспечения»**С.Е. Кондаков¹⁴¹, И.С. Рудь¹⁴²**

Аннотация. Бурное развитие цифровых технологий в последние два десятилетия, а также широкое распространение разнообразных вычислительных устройств стали мощным стимулом для использования этих устройств в разнообразных сферах деятельности и для решения огромного количества задач. Параллельно с ростом количества вычислительных устройств и программного обеспечения, работающего на этих устройствах, быстрыми темпами росло и количество вредоносных программ. В данной статье приведено сравнение определений вредоносного программного обеспечения (далее – ВПО) и обосновано наиболее полно раскрывающее сущность современного ВПО.

Ключевые слова: защита информации, вредоносное программное обеспечение (ВПО), компьютерная атака (КА).

Введение

Применение ВПО является одним из основных инструментов проведения целенаправленных КА на информационные системы [1].

Согласно статистике доля КА, в ходе которых использовалось вредоносное ПО, в 2018 выросло по сравнению с 2017 годом с 48 до 58 %¹⁴³.

Злоумышленниками наиболее часто как средство для проведения КА используется ВПО, чем, например, компрометация учетных данных или перехват трафика [2-7]. Данный факт показывает, что вопрос изучения технологий, применяемых в ВПО, а также способы и меры по защите информационных систем от воздействий ВПО является актуальной задачей.

Анализ понятийной базы

Для того, чтобы вырабатывать эффективные меры по противодействию ВПО, необходимо четко определить, что понимается под термином «вредоносное программное обеспечение» [8].

В табл. 1 собраны определения термина «вредоносная программа» с указанием нормативного правового акта, в котором они указаны.

Таблица 1.

Определения «вредоносного программного обеспечения»

№ п/п	Определение
1.	Вредоносная программа: созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети ¹⁴⁴ .
2.	Вредоносная компьютерная программа: компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации ¹⁴⁵ .

¹⁴¹ Кондаков Сергей Евгеньевич, кандидат технических наук, Минобороны России, г. Москва, sergeikondakov@list.ru

¹⁴² Рудь Илья Сергеевич, Минобороны России, г. Москва, rud@mil.ru

¹⁴³ <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2019-rus.pdf>

¹⁴⁴ Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (ратифицировано федеральным законом РФ от 1 октября 2008 г. № 164-ФЗ)

¹⁴⁵ Уголовный кодекс Российской Федерации (федеральный закон от 13 июня 1996 г. № 63-ФЗ)

3.	Вредоносное программное обеспечение: программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя, либо к ухудшению параметров функционирования абонентского терминала или сети связи ¹⁴⁶ .
4.	Вредоносная программа: Программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы (ГОСТ Р 51275-2006).
5.	Вредоносная программа: Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы (ГОСТ Р 50922-2006).
6.	Вредоносная программа: Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы (ГОСТ Р 53113.1-2008).
7.	Вредоносный код: компьютерная программа, предназначенная для внедрения в автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование кредитной организации и ее клиентов — пользователей систем дистанционного банковского обслуживания, приводящая к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации (в том числе защищаемой в соответствии с пунктом 2.1 Положения 382-П), а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи ¹⁴⁷ .
8.	Вредоносная программа: программа, которая скрытно вставляется в другую программу с целью уничтожения данных, запуска деструктивных или навязчивых программ или иным образом ставить под угрозу конфиденциальность, целостность или доступность данных, приложений или операционной системы жертвы (NIST Special Publication 800-83).
9.	Вредоносное программное обеспечение: любое программное обеспечение, устанавливаемое на компьютеры и устройства без разрешения пользователя, либо выполняющее заведомо вредоносные действия, а также действия, отличные от описанных в документации ¹⁴⁸ .
10.	Вредоносная программа: любая программа, преднамеренно созданная для выполнения несанкционированных, зачастую вредоносных действий ¹⁴⁹ .

Анализ определений, приведённых в (табл.1), показывает, что главным критерием отнесения ПО к ВПО является деструктивное воздействие на информацию.

При этом, как показывает реальность, осуществление деструктивного воздействия на информацию также возможно путем применения и системного ПО. Например, с помощью системной утилитой *rm*, предназначенной для удаления файлов и входящей в состав операционных систем семейства Linux, которая может быть запущена скрытно и без разрешения пользователя. Последствия работы системой утилиты *rm* для системы могут оказаться крайне негативными.

Таким образом, возможность осуществления программой деструктивного воздействия на информацию не означает, что данное ПО однозначно является ВПО. Для

¹⁴⁶ Постановление Правительства Российской Федерации от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи»

¹⁴⁷ Письмо Банка России от 24.03.2014 №49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»

¹⁴⁸ <https://vms.drweb.ru/glossary>

¹⁴⁹ <https://encyclopedia.kaspersky.ru/glossary/malware>

подтверждения данного факта необходимо убедиться, что ПО соответствует еще одному критерию отнесения его к ВПО, а именно функционирует скрытно.

Скрытый режим запуска и функционирования ПО характеризуется выполнением программы без явного отображения режима ее выполнения для пользователя (администратора).

Связка выполнения выше указанных критериев может служить при отнесении ПО к ВПО.

Формирование терминологической базы

Учитывая личный опыт авторов и проведенный анализ, предлагается программу относить к вредоносной при наличии совокупности следующих обстоятельств:

в ПО реализован «потенциально опасный» функционал, выполнение которого способно уничтожить, заблокировать, модифицировать либо несанкционированно скопировать информацию или нейтрализовать средства защиты информации [9, 10];

в ПО реализован функционал скрытного функционирования, предусматривающий выполнение данной программы без каких-либо запросов (разрешений).

Таким образом, предлагается использовать следующее определение:

Вредоносное программное обеспечение – скрытно функционирующее программное обеспечение, в котором реализован функционал, способный привести к уничтожению, блокированию, модификации либо несанкционированному копированию информации или нейтрализации средств защиты информации.

$$P_{iВПО} \rightarrow \{ I^R_{ВПО}; I^S_{ВПО} \} \quad (1)$$

где, $P_{iВПО}$ - i -ая программа из множества ВПО;

$I^R_{ВПО}$ - признак подмножества ВПО, имеющих «потенциально опасный» функционал;

$I^S_{ВПО}$ - признак подмножества ВПО с признаком скрытного функционирования.

Вышеуказанное определение (1) с учетом функциональности современного ВПО, по мнению авторов статьи, является наиболее полным.

Литература

1. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1(1). С.28-36.
2. Алешин В.А., Жилина В.С., Коршунов А.В., Работаев И.М., Работаев Н.М. О подходах к обнаружению прослушивания трафика в анонимной сети TOR // Вопросы кибербезопасности. 2013. № 2 (2). С. 2-8.
3. Еремеев М.А., Кравчук А.В. Анализ методов распознавания вредоносных программ // Вопросы защиты информации. 2014. № 3 (106). С. 44-51.
4. Ермаков А.О., Кавешников М.Б., Клянчина Е.В. Вредоносное программное обеспечение АРТ-групп и его характеристики // Вопросы кибербезопасности. 2017. № S2 (20). С. 24-29.
5. Жуковский Е.В., Зегжда Д.П. Анализ вредоносного ПО, обладающего механизмами опасного триггерного поведения // Защита информации. Инсайд. 2019. № 3 (87). С. 60-63.
6. Козачок А.В., Кочетков Е.В. Обоснование возможности применения верификации программ для обнаружения вредоносного кода // Вопросы кибербезопасности. 2016. № 3 (16). С. 25-32.
7. Комаров А.А. Вредоносный программный код в составе специального программного обеспечения электронной компонентной базы встраиваемых систем // Защита информации. Инсайд. 2011. № 4 (40). С. 59-63.
8. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. №3. С. 56-61.
9. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1 (2). С. 40-48.

10. Харжевская А.В., Ломако А.Г., Петренко С.А. Представление программ инвариантами подобия для контроля искажения вычислений // Вопросы кибербезопасности. 2017. № 2 (20). С. 9-20.

On the definition of «malware»

S.E. Kondakov¹⁵⁰, I.S. Rud¹⁵¹

Annotation. *The rapid development of computer technology in the last two decades, as well as the widespread use of various computing devices (personal computers, laptops, smartphones, etc.) have become a powerful incentive for using these devices in various fields of activity and for solving a huge number of tasks (from development of documents to decision-making systems based on artificial intelligence). In parallel with the increase in the number of computing devices and software running on these devices, the number of malicious programs has grown rapidly. This article compares the definitions of malware and substantiates the most fully revealing the essence of modern malware.*

Keywords: *information protection, malware (malicious), computer attack*

¹⁵⁰ Kondakov Sergey Yevgen'yevich, Ph.D., military unit, Moscow, sergeikondakov@list.ru

¹⁵¹ Rud' Il'ya Sergeyevich, military unit, Moscow, rud@mil.ru

Классификация компьютерных атак с использованием вредоносного программного обеспечения

С.Е. Кондаков¹⁵², И.С. Рудь¹⁵³

Аннотация. В данной статье проведен анализ существующих классификации вредоносного программного обеспечения (далее – ВПО, вредоносная программа). Учитывая современные виды ВПО авторами предложена классификация в зависимости от этапа компьютерной атаки, на котором используется ВПО, от цели, которую данное ВПО позволяет достичь, и непосредственно от способа достижения ВПО данной цели. Данный подход может быть использован при разработке системы защиты информации от воздействий ВПО или при оценке ее эффективности.

Ключевые слова: информационная безопасность, вредоносное программное обеспечение, классификация, этапы компьютерной атаки.

Введение

Целью классификации ВПО является разделение множества ВПО на группы, для которых характерны определенные свойства, с целью использования данных свойств для решения задач по предотвращению воздействия ВПО на ресурсы информационных систем.

Понимание действий злоумышленника, используемый им инструментарий и применяемые техники для достижения своих целей, позволяют разработать эффективную систему защиты информации от воздействий ВПО. Таким образом, вопрос разработки классификации, учитывающей цель использования ВПО и её способы достижения, является актуальным.

Обзор имеющихся классификаций ВПО

В зависимости от цели классификации исследователями предлагаются различные варианты разделения ВПО на категории.

Несмотря на ряд классификаций [1-7] до сих пор отсутствует единое понимание о том, какие особенности ВПО следует учитывать, какие из них являются ключевыми и наиболее значимыми для решения задачи по противодействию ВПО, а именно для создания эффективной системы защиты от воздействия ВПО.

Например, в одном случае ключевое значение будет иметь признак классификации, связанный с вектором, используемым для инициирования атаки (например, веб-сайты, локальные сети, USB-накопители или электронная почта). Или другой пример – разделение методов распространения ВПО на тех, в которых присутствует необходимость взаимодействия с пользователем и на те, в которых такой необходимости нет.

Таким образом, из проведенного анализа видно, что в настоящее время в литературе предложены различные классификации ВПО, которые могут служить основой для исследования свойств ВПО. При этом, в случае необходимости использования классификации ВПО для выбора механизмов защиты при построении системы защиты информации от ВПО или оценки эффективности применяемых для защиты от ВПО мер, ни одна из указанных не позволяет в явном виде полноценно выполнить данную задачу. Например, понимая особенности алгоритма работы нерезидентных, резидентных или полиморфных вредоносных программ, разработчику системы защиты не будет достаточно данной информации для выбора средств защиты информации.

¹⁵² Кондаков Сергей Евгеньевич, кандидат технических наук, Минобороны России, г. Москва, sergeikondakov@list.ru

¹⁵³ Рудь Илья Сергеевич, Минобороны России, г. Москва, rud@mil.ru

С учетом вышеизложенного можно сделать вывод, что существующие классификации ВПО для выбора механизмов защиты при построении системы защиты информации от ВПО или оценки эффективности применяемых для защиты от ВПО мер мало пригодны, и вопрос разработки для этих целей классификации является актуальный.

Этапы проведения компьютерных атак

Согласно отчетам по расследованию инцидентов, связанных с воздействиями ВПО на информационные системы, все современные компьютерные атаки проводятся в несколько этапов. Для достижения конечной цели злоумышленник решает ряд обязательных задач.

В современной литературе в последнее время наиболее часто и полно раскрывающей моделью проведения атаки является модель «Cyber Kill Chain» (пер. с англ. «Цепь киберубийств») [8]. В общем плане данная модель предусматривает 8 этапов, отражающих задачи злоумышленника: разведка, вооружение, доставка, проникновение, установка, управление, реализация, уничтожение следов. Данная модель является концептуальной и описывает действия злоумышленника на том или ином этапе, делая акцент прежде всего на цели, которая предполагается достичь.

В тоже время, для более развернутого понимания как действует злоумышленник на различных этапах, разработана модель «MITRE ATT&CK» [5].

Если рассматривать этапы компьютерной атаки с точки зрения использования в ходе их проведения ВПО, то можно отметить следующее:

Этап «разведка» осуществляется, как правило, без применения ВПО, так как на данном этапе осуществляется исследование, идентификация и выбор цели для атаки.

На этапе «вооружение» происходит разработка ВПО, осуществляется его тестирование, создается необходимая инфраструктура, осуществляется планирование доставки ВПО до жертвы.

Начиная с 3 этапа на всех последующих этапах основным инструментом для достижения цели является ВПО.

Так как каждый этап проведения атаки предназначен для достижения определенных целей, то соответственно общим свойством для всех ВПО, применяемых на отдельных этапах, является достигаемая этим ВПО цель.

На одном этапе злоумышленник может стремиться к достижению одной (например, на этапе «доставка» одна цель – получение первоначального доступа) или нескольких целей (например, на этапе «установка» четыре цели – «анализ инфраструктуры», «повышение привилегий», «обход защиты», «получение учетных данных»).

Кроме того, достижение цели может осуществляться различными способами.

Классификация ВПО на основе этапа компьютерной атаки, на котором применяется данное ВПО

Анализируя выше изложенное, авторы предлагают свой принцип классификации ВПО, учитывающей цель использования ВПО и способы достижения данной цели (рис. 1).

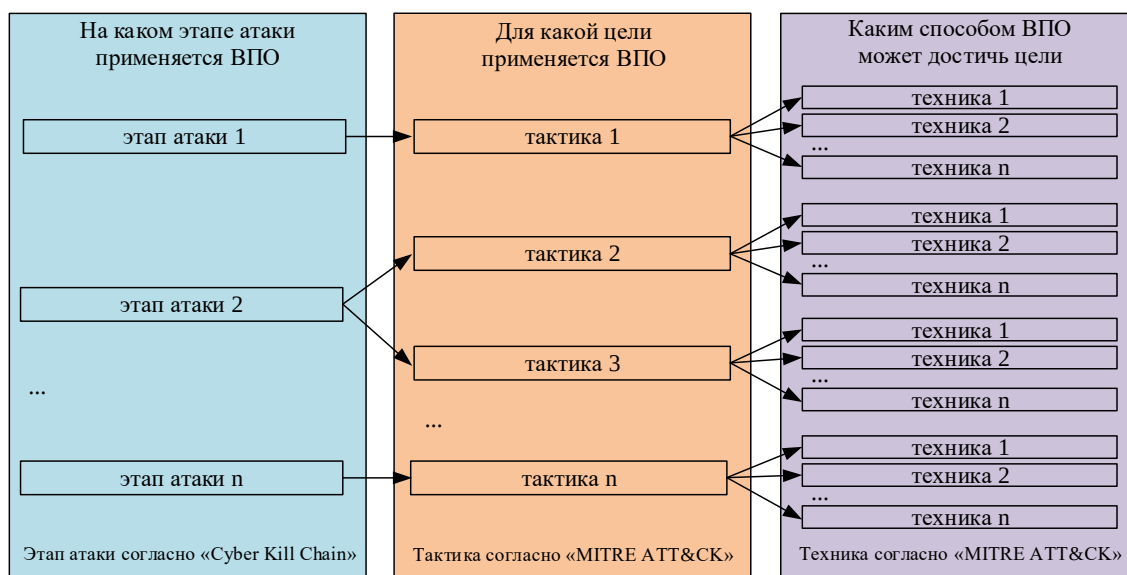


Рис.1. Классификации ВПО

Предлагается классифицировать ВПО:

по этапу, на котором оно применяется: доставка, проникновение, инсталляция, управление, реализация, уничтожение следов.

по цели, для которой оно применяется: для получения первоначального доступа, закрепления в системы, анализа инфраструктуры, повышения привилегий, обхода защиты, получения учетных данных, взаимодействия с сервером управления, бокового перемещения, сбора данных, передачи данных, воздействия на систему.

Категорию ВПО, предназначенную для достижения определенной цели, также предлагается классифицировать по технике достижения этой цели.

Вывод

Предложенную классификацию возможно использовать при разработке требований тактико-технического задания на создание системы защиты информации информационной системы или при оценке ее эффективности.

Разработанная классификация позволяет более точно понять способы проникновения ВПО в информационную систему, какие типы устройств могут быть подвержены заражению ВПО, какие цели преследуются злоумышленниками и как они реализовываются на отдельных этапах атаки.

Предлагаемая классификация ВПО была апробирована в ходе контрольно-технических мероприятий по оценки защищенности объектов информатизации воинских частей.

Литература

1. Еременко С.П., Сапелкин А.И., Хитов С.Б. Классификация вредоносных программ // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2016. №3.
2. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1 (2). С. 40-48.
3. Кондаков С.Е., Рудь И.С. К вопросу об определении «вредоносного программного обеспечения». Материалы X Международной конференции «Безопасные информационные технологии». М.: МГТУ им. Н.Э.Баумана, 2019. С.20-207.
4. Маркина Т.А. Модели и методы защиты от вредоносных программ на основе контроля доступа к файлам: диссертация ... кандидата технических наук: 05.13.19; [Место защиты: С.-Петербург. нац. исслед. ун-т информац. технологий, механики и оптики] – Санкт-Петербург, 2014. – 140 с.
5. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. №3. С. 56-61.
6. Соловьев Л.Н. Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ: диссертация ... кандидата юридических наук: 12.00.09; –Москва, 2003. – 275 с.
7. Rutkowska J. Introducing Stealth Malware Taxonomy. Technical report, COSEINC Advanced Malware Labs, November 2006. [Электронный ресурс]. – URL: https://blog.invisiblethings.org/papers/2006/rutkowska_malware_taxonomy.pdf (дата обращения: 10.11.2019).
8. Лукацкий А. Убийственная цепочка или что такое Kill Chain [Электронный ресурс]. – URL: https://www.securitylab.ru/blog/personal/Business_without_danger/320009.php (дата обращения: 7.11.2019).

Classification of computer attacks using malware

S.E. Kondakov¹⁵⁴, I.S. Rud¹⁵⁵

Annotation. *This article analyzes the existing classification of malicious software. Given the modern types of malware, the authors propose their own classification depending on the stage of the computer attack at which malware is used, on the goal that this malware allows to achieve, and directly on how the malware is achieved. This approach can be used in developing a system for protecting information from the effects of malware or in evaluating its effectiveness. The proposed classification contributes to a better understanding of how, using malware, attackers achieve the intermediate and ultimate goal of a computer attack.*

Keywords: *information security, malware, classification, stages of a computer attack*

¹⁵⁴ Kondakov Sergey Yevgen'yevich, Ph.D., military unit, Moscow, sergeikondakov@list.ru

¹⁵⁵ Rud' Il'ya Sergeyevich, military unit, Moscow, rud@mil.ru

Методика обеспечения сжатия и безопасности передачи данных в области телемедицины

Коновалов А.А.

***Аннотация:** В работе рассмотрены существующие подходы к решению вопроса сжатия и безопасности передачи данных в телемедицинских системах, учтены различные методы, алгоритмы способы достижения безопасности. Изучены отечественные и зарубежные стандарты по работе в сфере телемедицины, предложено собственное решение, которое может ускорить процесс развития данной области.*

***Ключевые слова:** телемедицина, видеоконференцсвязь, шифрование, DICOM, HL7, ГОСТ «информатизация здоровья», ЭКГ*

Введение

В нашем исследовании предпринята попытка сравнения существующих методов обеспечения безопасности и ускорения передачи медицинских изображений, и других специфических типов файлов, что поможет понять, в каких направлениях необходима работа по развитию безопасности отечественной телемедицины. Исследование основывается на модели телемедицины, определенной как «...информационные технологии, обеспечивающие дистанционное взаимодействие медицинских работников между собой, с пациентами и (или) их законными представителями, идентификацию и аутентификацию указанных лиц, документирование совершаемых ими действий при проведении консилиумов, консультаций, дистанционного медицинского наблюдения за состоянием здоровья пациента» (ФЗ № 242, 2018, статья 3). Компонентами модели являются субъекты, объекты, принципы, особенности, способы организации сети, методики передачи данных, методики сжатия и шифрования.

Решения

На сегодняшний день, существует множество стандартов, описывающих построение телемедицинской сети, взаимодействие между данными внутри нее. Самыми распространенными можно назвать DICOM [1, 2] для обработки и передачи медицинских изображений и HL7 [3, 4] для работы с медицинскими документами и сообщениями. В описываемых стандартах имеет место обеспечение безопасности передачи данных путем взаимодействия с различными криптографическими протоколами, задействуются алгоритмы шифрования данных. Несмотря на существование стандартов, принятых во многих странах мира, а также ГОСТов, определяющих практически все аспекты «информатизации здоровья», продолжают работы по улучшению отдельно взятых аспектов перечисленных стандартов, а также по предоставлению альтернативных методов для возможного развертывания собственных телемедицинских сетей где-нибудь в странах Африки [3 - 6].

В научных трудах приводится много интересных мыслей по улучшению качества работы с данными, сжатию медицинских данных и безопасности обмена ими [7, 8]. Высказываются различные идеи относительно модифицирования симметричных и асимметричных алгоритмов шифрования [9, 10], алгоритмов выработки общего ключа и хэширования, а также по кодировке и сжатию передаваемой информации [11, 12].

Текущая ситуация

Несмотря на то, что некоторые телемедицинские стандарты начали свое развитие еще в 1970-е гг. и на наличие огромного пласта знаний относительно рассматриваемой области медицины, в России и некоторых других странах лишь недавно стали приниматься законы и стандарты, регулирующие телемедицину.

По этой причине развитие телемедицины происходит недостаточно быстро, являясь при этом весьма важной отраслью для РФ благодаря неравномерности расселения людей по стране. Также из-за отсутствия до недавнего времени понятия «Телемедицина» в законодательстве и принятых государственных стандартов, продукты, разработанные в России, направленные на упрощение коммуникаций пациента с врачом, нельзя считать полностью полноценными телемедицинскими системами, т.к. в большинстве они представляют из себя видеоконференцию с выбранным доктором или службу вызова районного врача на дом.

Выводы

В заключение была предпринята попытка выстроить собственный алгоритм, обеспечивающий сжатие и безопасность передачи данных электрокардиограммы, основанный на некоторых научных трудах. В дальнейшем возможна реализация системы по обмену данными, основанная на предложенном алгоритме.

Литература

1. Магнитно-резонансные томографы XGY Oper. Стандарт DICOM [Электронный ресурс]. - 2019. - URL: <https://mri.com.ua/page/text/name%3Ddicom> (дата обращения 15.11.2019)
2. Cryptographic Message Syntax. Network Working Group [Электронный ресурс]. - 1999. - URL: <https://tools.ietf.org/html/rfc2630> (дата обращения: 16.11.2019)
3. Health Level Seven International - Homepage [Электронный ресурс]. 2019. - URL: <https://www.hl7.org/> (дата обращения: 11.11.2019).
4. Habr. Clinical Document Architecture (CDA) [Электронный ресурс]. - 2015. - URL: <https://habr.com/ru/post/255879/> (дата обращения: 12.11.2019).
5. B. Lakshmi Dhevi, K. S. Vishvakshenan, K. Senthamil Selvan, A. Rajalakshmi. Patient Monitoring System Using Cognitive Internet of Things // Journal of Medical Systems. Mobile & Wireless Health - 2018. - No. 42, 229 p.
6. A. Pandey, B. Singh Saini, B. Singh, N. Sood. An integrated approach using chaotic Map & Sample value difference method for electrocardiogram steganography and OFDM based secured patient information transmission // Journal of Medical Systems. - 2017. - Vol. 41. - 187 p.
7. Федорчук В.С. Сравнение Фурье и вейвлет преобразования // Синергия наук. - 2018. - № 22. - С. 1634-1641.
8. Горшков Ю.Г., Каиндин А.М., Веряев А.С., Зорин Е.Л., Марков А.С., Цирлов В.Л. Система телемедицины с предварительным шифрованием биометрической информации // Вопросы кибербезопасности. - 2015. - № 5 (13). - С. 63-69.
9. M. Raeiati, M. mahdi Khalilzadeh, S. R. Quchani, K. Bahaadinbeigy. Compression and encryption of ECG signal using wavelet and chaotically huffman code in telemedicine application // Journal of Medical Systems. - 2016. - Vol. 40. - 73 p.
10. A. Al-Haj, A. Mohammad, A. Amer. Crypto-watermarking of transmitted medical images // Journal of Digital Imaging. - 2017. - Vol. 30, No. 1. P. 26- 38.
11. B. Hassan, R. Ahmed, Bo Li, O. Hassan. An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an eHealth arrangement // IEEE Access. - 2019. - Vol. 7. - P. 69758-69775.

12. R.Sreejith, S.Senthil. A novel tree based method for data hiding and integrity in medical images // «2017 International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE 2017)» / Karur, India (April 2017). URL: <https://ieeexplore.ieee.org/document/8191946> (дата обращения: 03.11.2019)

Научный руководитель: Коннова Н.С., к.т.н., доцент кафедры ИУ8, tttasha@mail.ru

Compression and security technology for data transmission in telemedicine

Konovalov A. A.

Abstract: *The paper considers the existing approaches of solving the issue of compression and security of data transmission in telemedicine systems, various methods, algorithms and ways to achieve security are taken into account. The domestic and foreign standards for work in the field of telemedicine are investigated, own solution, which can accelerate the process of development of this area is proposed.*

Keywords: *telemedicine, video conferencing, encryption, DICOM, HL7, GOST "health informatization", ECG*

Интеллектуальная аналитика в обеспечении защищенности от комплексных угроз

Корнеев Н.В.¹⁵⁶, Меркулов В.Д.¹⁵⁷

В работе кратко дается характеристика и проблематика комплексных угроз, рассматриваются практические аспекты их формирования и реализации. С учетом выделенных особенностей комплексных угроз, предлагаются перспективные подходы к обеспечению защищенности от комплексных угроз, основанные на алгоритмах интеллектуального анализа и обработки данных больших объемов, поступающих в единую информационную среду от интегрированных подсистем защиты. Делается вывод, что построение подобной системы способно решить проблему обнаружения комплексных угроз путем поиска взаимосвязей между элементарными угрозами.

Ключевые слова: комплексная безопасность, информационно-аналитические системы защиты, корпоративные системы безопасности, обнаружение комплексных угроз.

Введение

В ретроспективе угрозы информационной безопасности рассматривались и изучались по отдельности, независимо друг друга, что было обусловлено сложившимися на тот момент условиями: требовались эффективные методы и средства защиты от хорошо формализованных угроз, которые можно назвать элементарными угрозами по причине их атомарности. Специалистами в различных областях безопасности разработаны эффективные меры и средства, способные обеспечить защищенность от конкретных элементарных угроз, которые можно условно разделить, в случае, например, рассмотрения вопроса защиты объектов топливно-энергетического комплекса, на угрозы физической безопасности, техногенной, промышленной и информационной [1].

Совокупность таких факторов, как размытость границ классификации угроз, частое наличие взаимосвязей между ними, практики ведения гибридных войн и рост числа атак, затрагивающих сразу несколько пространств функционирования объекта защиты [2, 3], привели к необходимости рассмотрения вопросов комплексной безопасности в новом контексте и появлению термина «комплексная угроза» (КУ). Комплексная угроза по своей природе состоит из нескольких элементарных угроз, связанных между собой посредством определенного синхронизирующего механизма [1].

Новый тип угроз требует совершенствования имеющихся средств и методов защиты, либо разработки совершенно новых подходов к обеспечению комплексной безопасности [4-8], базирующихся на, в том числе, современных технологиях интеллектуального анализа данных (Data Mining) и методах обработки данных больших объемов (Big Data).

Предпосылки к использованию ИАД для обнаружения КУ

Без привязки к конкретным свойствам защищаемого объекта, комплексная угроза С может быть представлена как совокупность (1) множества элементарных угроз Т и множества R взаимосвязей между ними:

$$C = \langle T, R \rangle \quad (1)$$

Проблема целеполагания комплексных угроз является одной из наиболее важных. Несмотря на то, что КУ является агрегатом множества элементарных угроз Т, которые сами

¹⁵⁶ Корнеев Николай Владимирович, доктор технических наук, доцент, РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва, nicssur@gmail.ru

¹⁵⁷ Меркулов Вячеслав Дмитриевич, инженер, РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва, mvd@decenter.tech

по себе способны нанести определенный ущерб, настоящая (основная) цель комплексной угрозы, в общем случае, только одна – это глубокая системная уязвимость. Значимые объекты критической информационной инфраструктуры (по ФЗ №187 от 26.07.2017) могут рассматриваться как одни из наиболее вероятных целей для атак, реализующих комплексную угрозу, но список возможных основных целей не должен ими ограничиваться. Основная цель в качественно спланированной КУ неочевидна для службы защиты до момента достижения цели злоумышленником, в некоторых случаях – и после, поскольку последствия реализации КУ и достижения основной цели могут быть скрытыми и растянутыми во времени.

Стоит также отметить, что реализация комплексной угрозы требует тщательного планирования атак, повышенного уровня теоретических знаний и практических навыков нарушителя, что приводит к выводу: злоумышленники, занимающиеся комплексными угрозами, по умолчанию имеют больше компетенций и знаний об объекте защиты, а следовательно – могут нанести гораздо больший ущерб.

Атаки, реализующие комплексную угрозу, могут быть растянуты во времени, либо происходить практически одновременно. Наблюдения, основанные на аспекте времени – одни из самых очевидных и простых для человека. В данном случае, анализ только временного аспекта атак может привести к неверному выводу о факте наличия или отсутствия комплексной угрозы. Обобщая подобные несовершенства мышления человека, проблема определения самого факта наличия комплексной угрозы является нетривиальной задачей.

Обозначенная проблема комплексных угроз – нелинейность и неявная внутривидовая связанность – может быть решена с использованием в системах комплексной безопасности мощного аналитического ядра, способного находить взаимосвязи $g \in R$ между элементарными угрозами t_i в составе множества T . Само аналитическое ядро предполагается строить на основе существующих алгоритмов интеллектуального анализа данных, перспективных [9] при решении задач обеспечения безопасности.

Событийный подход к рассмотрению комплексных угроз

Атаки, реализующие КУ, могут быть рассмотрены как цепочка событий-нарушений, синхронизированных, например, по аспекту времени. При работе с КУ, на общем уровне предлагается использовать событийный подход к рассмотрению и анализу потенциальных инцидентов, совокупность которых может быть классифицирована как комплексная угроза. В терминологических целях, вводятся два понятия:

1. Событие-нарушение: реализация элементарной угрозы в составе комплексной угрозы T .
2. Целевое событие-нарушение: определенная элементарная угроза из множества T , реализация которой является достижением цели злоумышленника.

С учетом данного подхода, комплексная угроза может быть представлена на концептуальном уровне в следующем виде (рис.1).

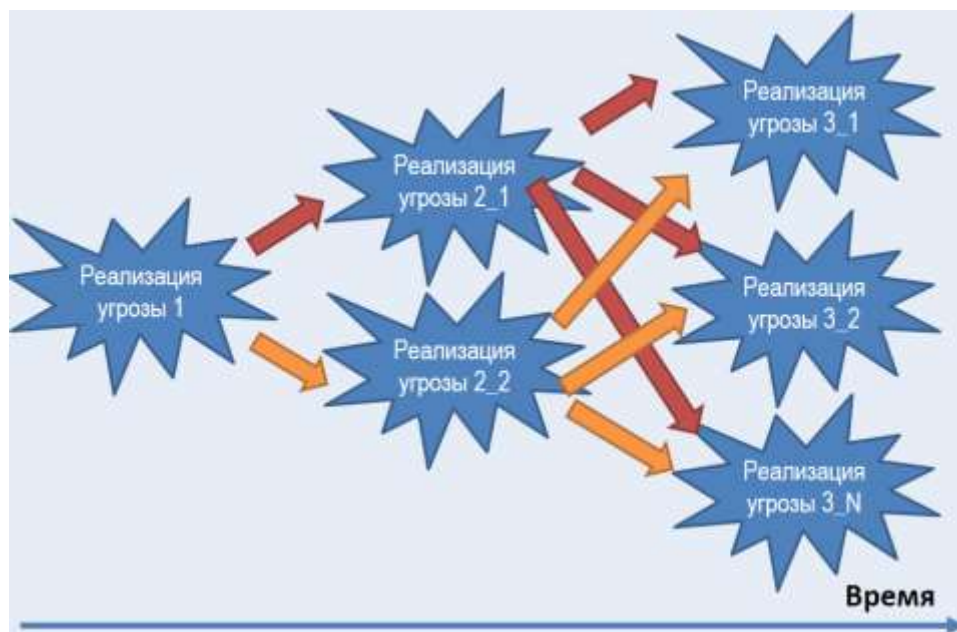


Рис.1. Концепт реализации комплексной угрозы при событийном подходе и синхронизации посредством времени

Очевидно, что при таком подходе, важными являются две задачи:

1. Анализ событий-нарушений с целью выявления связей, т.е. стремление к максимально полному описанию элементов множества R, что позволит спрогнозировать следующие атаки.
2. Недопущение достижения злоумышленником реализации атаки, которая приведет к наступлению целевого события-нарушения, что означает прежде всего определение потенциальных целевых событий-нарушений.

Немаловажным преимуществом описанного подхода является достаточно высокая распространенность SIEM и SEM систем, которые могут являться источником данных о событиях для дальнейшей аналитики.

Возможные источники данных для аналитики в рамках предприятия

Из-за сложности планирования и реализации КУ, а более формально – по причине отношения параметров «затраты на реализацию атаки» и «ожидаемый ущерб от атаки», логично предположить, что наиболее часто КУ формируются для нанесения ущерба крупным предприятиям и компаниям. В связи с этим, примем, что на рассматриваемом объекте защиты уже функционируют определенные программно-аппаратные системы, обеспечивающие защищенность от ряда элементарных угроз.

Существующая корпоративная система безопасности, в таком случае, изначально работает на обеспечение защищенности от конкретных элементарных угроз. Систематизировав данные угрозы и рассмотрев возможность существования взаимосвязей между ними, можно составить набор данных для дальнейшего анализа аналитическим ядром, результаты которого будут использоваться в процессе обнаружения КУ. База потенциальных элементарных угроз может формироваться из различных источников (рис. 2).



Рис.2. Источники данных для формирования базы потенциальных элементарных угроз

Хранимые атрибуты угроз, тип хранилища и прочие аспекты базы потенциальных угроз должны определяться под конкретные требования заказчика.

Помимо этого, предлагается интегрировать в единое хранилище информационные потоки с подсистем защиты от элементарных угроз. Сами же подсистемы защиты могут получать данные напрямую от датчиков (например, контролирующих физический периметр защиты), либо взаимодействуя с другими программными средами (например, АСУТП). Информационные потоки также могут поступать из ERP-систем, в случае их наличия.

Таким образом, имея базу потенциальных событий-нарушений и поступающие данные от подсистем защиты, становится возможным решение задачи обнаружения комплексных угроз путем применения алгоритмов анализа данных. В сущности, потребуется решение классических задач классификации, регрессии, кластеризации и аффинитивного анализа. Аналитическое ядро на основе алгоритмов интеллектуального анализа данных, решая упомянутые задачи, будет находить взаимосвязи между элементарными атаками, проводить мониторинг интегрированных в системе КБ информационных потоков, что в совокупности обеспечит решение проблемы обнаружения комплексных угроз.

Выводы

В работе рассмотрена практическая проблематика комплексных угроз и особенности их формирования и реализации, на основе чего предложены подходы к обеспечению защищенности, что наиболее эффективно может проявляться в наличии средств и методов выявления самого факта наличия КУ и определения списка возможных целей КУ. Реализация данных механизмов может быть достигнута, используя аналитику больших данных, интегрируемых из различных источников на уровне предприятия.

С учетом концепции цифровой трансформации производственных технологий «Индустрия 4.0» [10], описанная технология аналитического обнаружения комплексных угроз относится к областям «Аналитика и искусственный интеллект» и «Технологии обработки данных», являясь, таким образом, примером современного средства обеспечения кибербезопасности.

Литература

1. Гриняев С.Н., Правиков Д. И., Медведев Д. А. Комплексная безопасность ТЭК как объект научного анализа // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. -2019. -№03-2. -С. 24-30.
2. Медведев Д.А, Тарчокова А.А. Инструменты международной легитимации внешнеполитических действий России в условиях информационного противоборства // Информационные войны, 2018. №3. С.34-37
3. Арзуманян Р.В. Инструменты принуждающей мощи в системе национальной безопасности США // Стратегическая стабильность. 2017. № 1 (78). С. 52-68
4. Борисов С.А. Формирование комплексной системы информационной безопасности как важнейший элемент экономической безопасности предприятия // Экономическая безопасность России: проблемы и перспективы материалы II Международной научно-практической конференции. 2014. С. 359-365.
5. Корнеев Н.В. Система поддержки управления комплексной безопасностью объектов с массовым пребыванием людей // Информационные технологии. Проблемы и решения. – Уфа: Изд-во УГНТУ, 2019. 1(6). С. 174-183.
6. Корнеев Н.В. Приоритеты развития информационной безопасности для информационно-коммуникационных технологий // Информационные технологии. Проблемы и решения: материалы международной научно-практической конференции. - Уфа: Изд-во «Восточная печать», 2016. Т. 2. – С. 365-368.
7. Корнеев Н.В., Гончаров В.А. Разработка информационной системы поддержки принятия решений для мониторинга пожара в жилых и административных зданиях // Системы безопасности-2016: материалы двадцать пятой международной научно-технической конференции. - М.: Академия ГПС МЧС России, 2016. – С. 340-342.
8. Корнеев Н.В., Гончаров В.А. Модель поддержки управления комплексной безопасностью объектов социальной сферы с массовым пребыванием людей // Естественные и технические науки. 2018. № 4. С. 277-281.
9. Гарбук С.В. Перспективы применения интеллектуальных технологий для решения задач безопасности. // Национальная безопасность / nota bene. - 2016. - № 4. - С. 451-457. DOI: 10.7256/2073-8560.2016.4.19207
10. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. № 2 (26). С.2-15.

Intelligent analytics for complex security

Korneev N.V.¹⁵⁸, Merkulov V.D.¹⁵⁹

This works deals with complex threats detection problem. We start with definition of practical problems of complex threats. Next, we describe some approaches of building complex security systems that includes the analytical core. The analytical core bases on data mining algorithms and deals with big data flows, which are integrated from security subsystems into single data storage. Finally, the conclusion about using that system for complex threat detection is given.

Keywords: complex security, analytics-based security systems, corporate security systems, complex threats detection.

¹⁵⁸ Nikolai Korneev, Dr.Sc., professor, Gubkin Russian State University of Oil and Gas (National Research University), Financial University under the Government of the Russian Federation, Moscow, niccyper@mail.ru

¹⁵⁹ Vyacheslav Merkulov, engineer, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, mvd@decenter.tech

Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта

Костокрызов А.И.¹⁶⁰

Предложен подход к когнитивной обработке данных мониторинга, позволяющий применять возможности вероятностного моделирования для систем искусственного интеллекта (ИИ). Подход включает в себя модели и методы прогнозирования вероятности «успеха» и/или риска неудачи, поддерживающие их программные инструментари, способы решения задач обоснования упреждающих мер противодействия угрозам и эффективного управления рисками. Работоспособность подхода проиллюстрирована на примерах.

Ключевые слова: анализ, безопасность, вероятность, модель, риск, система, управление

1. Введение

Мировые тенденции развития современных систем различного функционального назначения свидетельствуют о необходимости кардинального разворота от «ручного» управления отдельными видами безопасности, основанного на выполнении устоявшихся инструкций и экспертных оценках складывающихся ситуаций, к реализации упреждающих мер на основе вероятностного прогнозирования. Это позволяет на основе прогностического взгляда вперед превентивно предпринимать эффективные управленческие воздействия. Такая идея красной линией проходит через все западные концепции и последние стандарты системной инженерии. Но как это сделать – остается за кадром. В мире еще нет универсального подхода к реализации этой идеи. В поиске – все ведущие страны мира. Особые надежды при этом возлагаются на применение систем ИИ.

В настоящей работе акцент сделан на приложениях, критичных с точки зрения обеспечения безопасности в зависимости от структурной сложности систем, формальных условий неопределенностей, реализуемых методов противодействия угрозам, а также условий функционирования отдельных элементов. Предлагаются вероятностные методы когнитивной обработки данных мониторинга, в результате применения которых получаются прогнозы вероятности «успешного» развития событий или риска «неудачи» и для применения, которых в качестве исходных данных выступают текущие и предыдущие данные мониторинга состояний составных элементов¹⁶¹.

Предлагаемые идеи, модели, методы и технологии рассчитаны на реализацию обратной связи для решения задач обоснования требований и условий, гарантирующих обеспечение задаваемых приемлемых вероятностей «успеха» и/или допустимых рисков.

Предлагаемые вероятностные методы развивают сложившиеся вероятностные подходы [1-18], применимые там, где имеет место некоторая похожая повторяемость событий.

2. Суть предлагаемого подхода

Мониторируемая система может сама представлять собой интересующую систему для исследования (например, диспетчерский интеллектуальный центр) или может быть частью

¹⁶⁰ Костокрызов Андрей Иванович, доктор технических наук, профессор, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, e-mail: Akostogr@gmail.com

¹⁶¹Примечания. Определение системы - по ГОСТ Р 57193-2016, риска – по ГОСТ Р 51898-2002, ГОСТ Р 51901.1-2002, ГОСТ Р 51897-2011, ГОСТ Р МЭК 61508-4-2012, ГОСТ Р 58494-2019, ГОСТ Р ИСО 31000-2010.

другой, более объемлющей интересуемой системы (например, комплексом функционально ориентированных роботов). Для выполнения функций интересуемой системы осуществляется сбор и обработка текущей информации. Предлагается осуществлять вероятностное прогнозирование развития критичных процессов с тем, чтобы не только действовать согласно прогнозу, но и сравнивать прогнозы и их совпадения с последующими реалиями, накапливать и использовать эти знания. Именно в накоплении, анализе и использовании появляющихся знаний о возможной целостности системы в будущем заключается когнитивность решений по данным мониторинга.

При функционировании системы в условиях складывающихся разнородных угроз степень приемлемости происходящих событий предлагается оценивать вероятностью «успеха» и/или «неудачи» с учетом последствий (риском «неудачи») в течение заданного прогнозного периода времени. В каждом конкретном случае моделирования понятие «успеха» должно быть определено в терминах приемлемого состояния интересуемой системы для выполнения заданных или ожидаемых функций. Понятие «неудачи» означает отсутствие «успеха».

Аналитическое прогнозирование рисков предлагается осуществлять на основе вероятностного моделирования. Для практического применения рекомендуются методы и модели [1-10, 14-18] (далеко не исчерпывающие список адекватных), где субъективные весовые коэффициенты исключены. Предлагаемые модели базируются на классически построенном вероятностном пространстве (Ω, B, P) , где Ω – конечное пространство элементарных событий; B – класс всех подмножеств множества Ω , удовлетворяющий свойствам сигма-алгебры; P – вероятностная мера на пространстве элементарных событий. При этом, поскольку пространство $\Omega = \{\omega_k\}$ – конечное, в моделях установлено отображение $\omega_k \rightarrow p_k = P(\omega_k)$ такое, что $p_k \geq 0$ и $\sum_k p_k = 1$.

Сложная система декомпозируется до составных элементов для решения проблем применительно к каждому из элементов и подсистем с возможностью их сворачивания в систему в целом. Каждый из элементов представляется в виде «черного ящика», и для него могут быть применены различные вероятностные модели для расчетов и построения искомой функции распределения (ФР) времени между соседними нарушениями целостности, учитывающие разнородные угрозы, предпринимаемые меры контроля, мониторинга и восстановления целостности. Ниже приводятся некоторые обобщенные модели «черного ящика» для прогнозирования рисков нарушения целостности.

3. Предлагаемые модели для перехода от частного к общему

3.1. Математическая модель для прогноза риска нарушения целостности системы при реализации технологии профилактической диагностики

Предполагается изначальная целостность системы (в частном случае система – это «черный ящик»). В процессе функционирования в результате реализации возможных угроз могут начать развиваться процессы, приводящие к нарушению целостности системы. Начало (инициирование) каждого из таких процессов служит источником потенциальной опасности. В системе осуществляется периодический контроль целостности. Из-за различных причин целостность системы может быть нарушена.

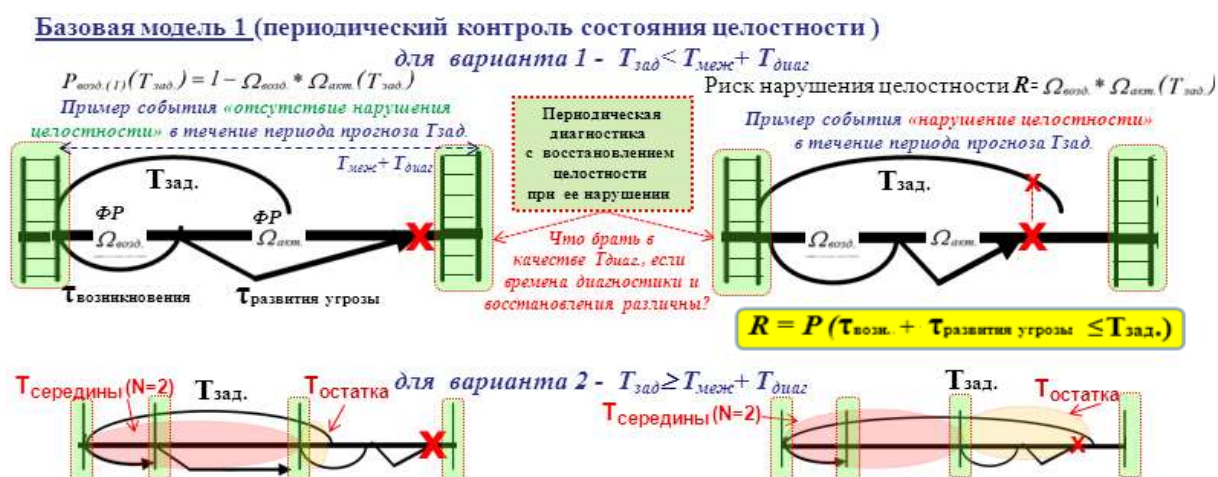
Примечание. В приложении к каждой системе (и ее критичных элементов) понятие и показатели обеспечения и нарушения целостности должны быть конкретизированы на уровне правил, инструкций по эксплуатации, обязанностей должностных лиц и т.п.

В рамках модели развитие критичных ситуаций в системе считается не нарушающим целостности в течение заданного прогнозного периода времени, если к началу периода нарушение целостности отсутствует и в течение всего периода либо источники опасности не инициируются, либо после инициации происходит их оперативное выявление и принятие адекватных мер противодействия. Предполагается, что существуют не только средства диагностики (контроля) целостности, но и способы поддержания и/или восстановления целостности при выявлении источников опасности или следов их инициации. Восстановление осуществляется лишь в период системного контроля.

За основу анализа принят следующий поэтапный алгоритм возникновения и реализации опасности: сначала источник опасности появляется и начинает инициироваться, а по прошествии свойственного ему периода инициации опасность разрастается до нарушения целостности системы. Если опасность постоянна (например, для опасного производства), выделяются приемлемый нормативный диапазон, который не должен нарушаться для показателей, характеризующих уровень опасности. Целостность считается нарушенной лишь после того, как инициировавшийся источник приводит к нарушению штатного режима функционирования (например, установленных пределов нормативного диапазона). Если инициировавшийся источник опасности был выявлен до наступления нештатной ситуации и приняты адекватные контрмеры, считается, что целостность системы не нарушена. Результатом применения очередной диагностики является полное восстановление нарушенной целостности системы до приемлемого уровня или подтверждение целостности при отсутствии ее нарушения.

Модель позволяет оценить вероятность нарушения целостности системы в течение заданного периода времени. Именно эта вероятность с учетом последствий определяется как риск нарушения целостности в течение заданного периода прогноза с учетом предпринимаемых мер периодического контроля и восстановления, а также возможных последствий от нарушений. Достижение приемлемого уровня риска является следствием достаточно частого диагностирования и применения эффективных средств диагностики, контроля и восстановления целостности при существующих ограничениях.

Примечание. Существование средств гарантированного выявления источников опасности или следов их воздействия и существование способов поддержания нарушенной целостности системы являются необходимыми условиями моделирования.



Для описания процессов возникновения и выявления опасных воздействий на систему введены обозначения:

σ — частота возникновения источника опасности;

β – среднее время инициации с разрастанием опасности до нарушения целостности;
 $T_{\text{меж}}$ – время между окончанием предыдущей и началом очередной диагностики;
 $T_{\text{диаг}}$ – длительность диагностики, включая восстановление целостности;
 $T_{\text{зад}}$ – длительность прогнозного периода времени.

Оценка риска нарушения целостности системы $R_{\text{наруш.}}$ в течение прогнозного периода $T_{\text{зад}}$ осуществляется по формуле:

$$R_{\text{наруш.}} = 1 - P_{\text{возд.}}, \quad (1)$$

где $P_{\text{возд.}}$ – это вероятность отсутствия нарушений целостности в течение $T_{\text{зад}}$.

Возможны два варианта:

- вариант 1 – заданный оцениваемый период $T_{\text{зад}}$ меньше периода между окончаниями соседних диагностик ($T_{\text{зад}} < T_{\text{меж}} + T_{\text{диаг}}$);
- вариант 2 – заданный оцениваемый период $T_{\text{зад}}$ больше или равен периоду между окончаниями соседних диагностик ($T_{\text{зад}} \geq T_{\text{меж}} + T_{\text{диаг}}$), т.е. за это время заведомо произойдет одна или более диагностик.

Для варианта 1 при условии независимости исходных характеристик вероятность $P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}})$ отсутствия нарушений целостности в течение периода $T_{\text{зад}}$ вычисляют по формуле (как распределение от суммы времен возникновения и инициации опасности на момент завершения периода прогноза $T_{\text{зад}}$ – см. рис. 1):

$$P_{\text{возд}(1)} = \begin{cases} (\sigma - \beta^{-1})^{-1} \{ \sigma e^{-T_{\text{зад}}/\beta} - \beta^{-1} e^{-\sigma T_{\text{зад}}} \}, & \text{если } \sigma \neq \beta^{-1}, \\ e^{-\sigma T_{\text{зад}}} [1 + \sigma T_{\text{зад}}], & \text{если } \sigma = \beta^{-1}. \end{cases} \quad (2)$$

Примечание - Эту же формулу используют для оценки вероятности отсутствия нарушений целостности без какой-либо диагностики.

Для варианта 2 при условии независимости исходных характеристик для расчетов возможны различные вероятностные меры.

Согласно первой мере вероятность $P_{\text{возд}(2)}$ отсутствия нарушений целостности в течение периода $T_{\text{зад}}$ может быть вычислена по формуле:

$$P_{\text{возд}(2)} = P_{\text{серед}} + P_{\text{кон}}, \quad (3)$$

где $P_{\text{серед}}$ – вероятность отсутствия нарушений целостности в течение всех периодов между диагностиками, целиком вошедшими в $T_{\text{зад}}$. С учетом доли этих периодов $\frac{N(T_{\text{меж}} + T_{\text{диаг}})}{T_{\text{зад}}}$ в общем оцениваемом периоде $T_{\text{зад}}$, расчет осуществляют по формуле

$$P_{\text{серед}} = \frac{N(T_{\text{меж}} + T_{\text{диаг}})}{T_{\text{зад}}} \cdot P_{\text{возд}(1)}^N(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{меж}} + T_{\text{диаг}}), \quad (4)$$

N – число периодов между диагностиками, которые целиком вошли в пределы времени $T_{\text{зад}}$, с округлением до целого числа, $N = [T_{\text{зад}} / (T_{\text{меж}} + T_{\text{диаг}})]$ – целая часть;

$P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{меж}} + T_{\text{диаг}})$ – вероятность отсутствия нарушений целостности за один период между диагностиками, целиком вошедший в пределы времени $T_{\text{зад}}$, вычисляют по формуле (2);

$P_{\text{кон}}$ – вероятность отсутствия нарушений целостности после последней диагностики (в конце $T_{\text{зад}}$). С учетом доли остатка $T_{\text{ост}} = T_{\text{зад}} - N(T_{\text{меж}} + T_{\text{диаг}})$ в общем прогножном периоде $T_{\text{зад}}$ расчет осуществляют по формуле

$$P_{\text{кон}} = \frac{T_{\text{ост}}}{T_{\text{зад}}} \cdot P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{ост}}); \quad (5)$$

Значение $P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{ост}})$ для остатка от задаваемого прогнозного периода вычисляют по формуле (2) с тем отличием, что вместо $T_{\text{зад}}$ стоит $T_{\text{ост}}$.

Другая возможная вероятностная мера для оценки вероятности $P_{\text{возд}(2)}$:

$$P_{\text{возд}(2)} = P_{\text{серед}} \cdot P_{\text{кон}}, \quad (6)$$

$$\text{где} \quad P_{\text{серед}} = P_{\text{возд}(1)}^N(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{меж}} + T_{\text{диаг}}), \quad (7)$$

$$P_{\text{кон}} = P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{ост}}). \quad (8)$$

В отличие от меры (3) отклонения расчетной вероятности за счет более частого контроля и восстановления целостности практически трудноразличимы, что для аналитика скрывает эффективность мер противодействия в управлении рисками.

3.2. Математическая модель для прогноза риска нарушения целостности системы при реализации технологии мониторинга

Технология мониторинга целостности является более общим случаем по сравнению с моделью 3.1. Между системными контролями целостности, осуществляемыми периодически, реализуется непрерывный мониторинг состояния системы силами каких-либо операторов (в качестве таковых могут выступать автоматические сканеры, человек за экраном монитора, на котором фиксируются показания датчиков и др.). В идеале это позволяет сразу же при обнаружении угрозы приступить к защите и восстановлению целостности системы. В моменты системного контроля также происходит восстановление целостности - например, путем штатной смены человека-оператора или подтверждением работоспособности датчиков и пр. Однако, операторам, в т.ч. автоматам, тоже свойственны ошибки, безошибочность их действий характеризуется временем наработки на ошибку, что является аналогом наработки на отказ. В отличие от предыдущей модели между диагностиками реализуется мониторинг состояний системы. Формально с учетом этих дополнительных мер целостность может быть нарушена лишь в случае, если наработка на отказ средств мониторинга окажется меньше, нежели период между диагностиками и именно в это оставшееся до следующей диагностики время произойдет инициация проникших источников опасности.

С учетом возможных последствий оценка риска нарушения целостности системы $R_{\text{наруш.}}$ в течение прогнозного периода $T_{\text{зад}}$ осуществляется по формуле (1).

Для варианта 1 ($T_{\text{зад}} < T_{\text{меж}} + T_{\text{диаг}}$) при условии независимости исходных характеристик вероятность $P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{нар}}, T_{\text{зад}})$ отсутствия нарушений целостности в течение периода $T_{\text{зад}}$ вычисляют по формуле:

$$P_{\text{возд}(1)}(T_{\text{зад}}) = 1 - \int_0^{T_{\text{зад}}} dA(\tau) \int_0^{T_{\text{зад}} - \tau} d\Omega_{\text{возд}} * \Omega_{\text{акт.}}(\theta). \quad (9)$$

где * – знак свертки;

$\Omega_{\text{возд.}}(t)$ – функция распределения (ФР) времени между возникновениями источника опасности, в инструментариях $\Omega_{\text{возд.}}(t) = 1 - \exp(-\sigma t)$, σ – частота возникновения источника опасности;

$\Omega_{\text{акт.}}(t)$ – ФР времени инициации источника опасности до угрожающих размеров, приводящих к нарушению целостности системы, в инструментариях $\Omega_{\text{акт.}}(t) = 1 - \exp(-t/\beta)$, β – среднее время инициации;

$A(t)$ – ФР времени наработки оператора на ошибку, в инструментариях

$A(t) = 1 - e^{-t/T_{\text{нар}}}$, $T_{\text{нар.}}$ – среднее.

Для варианта 2 ($T_{\text{зад}} \geq T_{\text{меж}} + T_{\text{диаг}}$) при условии независимости исходных характеристик также, как и для модели подраздела 3.1, для расчетов возможны различные вероятностные меры.

Таким образом, вероятность отсутствия нарушений целостности в течение периода $T_{\text{зад.}}$ определяется аналитическими выражениями (6) и (9) в зависимости от варианта соотношений между исходными данными. Это позволяет вычислить по формуле (4) искомый риск нарушения целостности системы в течение заданного периода прогноза с учетом предпринимаемых технологических мер контроля, мониторинга и восстановления целостности.

4. Моделирование для обоснования упреждающих мер. Примеры

Если в моделях подразделов 3.1 и 3.2 построить зависимость функции $P_{\text{наруш.}}(T_{\text{зад}})$ в точках расчета, когда $T_{\text{зад.}}$ пробегает значения от 0 до бесконечности (с заданной точностью), то эта зависимость будет характеризовать ФР времени нарушения целостности. Известный вид этой ФР, построенной по точкам, позволяет традиционными методами математической статистики определить среднюю наработку до нарушения целостности. Модели рекомендованы для применения стандартом ГОСТ Р 58494-2019. Точность моделей может быть повышена с помощью учета различий во времени диагностики и восстановления целостности составных элементов, что наряду с методами применения расчетов для сложных систем также рекомендовано этим стандартом.

Зафиксировав уровни «допустимых рисков» для системы и составных подсистем, а также, считая неизменными все параметры, за исключением одного, возможно решение различные оптимизационных задач, связанных с обоснованием эффективных упреждающих мер обеспечения целостности системы в условиях разнородных угроз. Классическими задачами являются максимизация эффекта (уровня качества или безопасности и др.) или минимум рисков, возможных ущербов при ограничениях или минимизация затрат при ограничениях на допустимые риски и иных ограничениях. Для расчетов предлагаются поддерживающие инструментальные комплексы [11-13].

Смысл применения оптимизационных постановок задач в следующем – за счет упреждающего выбора рациональных значений управляемых параметров анализируемых сценариев угроз и реализуемых мер упреждения и реакции:

- избежать излишних затрат при допустимых рисках и заданных критичных ограничениях на этапах концепции и технического задания (ТЗ), разработки, эксплуатации, сопровождения и развития системы, отдельных ее подсистем и элементов;
- минимизировать риски в процессе эксплуатации, сопровождения и развития системы и отдельных ее подсистем, и элементов при заданных критичных ограничениях.

Способы когнитивной обработки данных мониторинга в системах с функциями ИИ рассмотрим на примерах.

Пример 1 аналитического решения задачи планирования возможностей на основе данных мониторинга. Такие задачи актуальны для систем поддержки принятия решений. Мониторируемые данные используются для формирования таких значений исходных данных, как частота возникновения источника опасности (σ), среднее время инициации с разрастанием опасности до угроз, приводящих к нарушению целостности системы (β) и среднего времени восстановления целостности – см. раздел 3. На рис. 2 приведен вариант формирования исходных данных для моделирования в реальном времени.

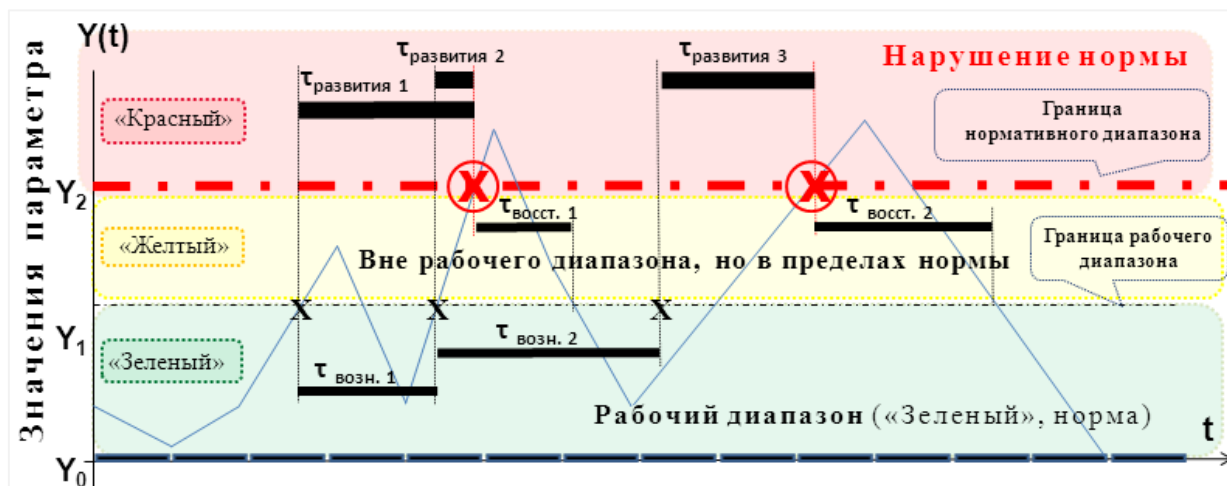


Рис. 2. Общий случай значений мониторируемого параметра относительно границ рабочего и нормативного диапазонов для формирования исходных данных моделей

По данным, отраженным на рис. 2, вычисляются следующие исходные данные моделей: частота возникновения источника опасности $\sigma = 1/[(\tau_{\text{возн. 1}} + \tau_{\text{возн. 2}})/2]$, среднее время инициации с разрастанием опасности до угроз, приводящих к нарушению целостности системы $\beta = (\tau_{\text{разв. 1}} + \tau_{\text{разв. 2}} + \tau_{\text{разв. 3}})/3$, среднее время восстановления $T_{\text{восст.}} = (\tau_{\text{восст. 1}} + \tau_{\text{восст. 2}})/2$. Далее решение задачи может быть осуществлено с использованием предложенных моделей.

Пример 2 прогнозирования времени на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона. Прогноз остаточного времени по данным мониторинга осуществляется при выходе значений какого-либо параметра конкретного оборудования за границы рабочего диапазона, оставаясь в границах нормативного диапазона. Если статистики недостаточно, то устанавливается допустимый риск выхода значений параметра за границы нормативного диапазона в течение заданного периода прогноза $R_{\text{доп}}$ ($T_{\text{зад}}$). Прогнозируемое время $T_{\text{упрежд. прогноз}}$ на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона оценивают как среднее время до перехода из состояния за границами рабочего диапазона, оставаясь в границах нормативного диапазона, в состояние за границами нормативного диапазона. Отсутствие статистики выхода за границы нормативного диапазона требует использования вероятностного моделирования. $T_{\text{упрежд. прогноз}}$ вычисляется с применением предложенной модели. Ищется решение обратной задачи: найти такое максимально большое время развития угроз x (т.е. неизвестное $x = \beta$), когда за этот же срок (т.е. $T_{\text{зад}}$ тоже равно неизвестному x) риск нарушения целостности системы впервые выйдет снизу на допустимый уровень риска. Т.е. искомое время (x) — это решение уравнения

$$R_{\text{наруш}}(\sigma, x, T_{\text{меж}}, T_{\text{диаг}}, x) = R_{\text{доп}}(x) \quad (10)$$

относительно параметра $x = T_{\text{упрежд. прогноз}}$, где параметр x занимает в формульном выражении $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}})$ в модели раздела 3 место параметров β и $T_{\text{зад}}$.

Решение существует, т.к. при возрастании β от нуля до бесконечности значение риска при прочих неизменных монотонно убывает от положительного фиксированного значения (зависящего от σ) до 0, а при возрастании периода прогноза $T_{\text{зад}}$ от нуля до бесконечности значение риска монотонно возрастает от 0 до 1. Здесь σ определяется по статистике данных мониторинга. Пример приложения подхода проиллюстрирован на рис. 3.

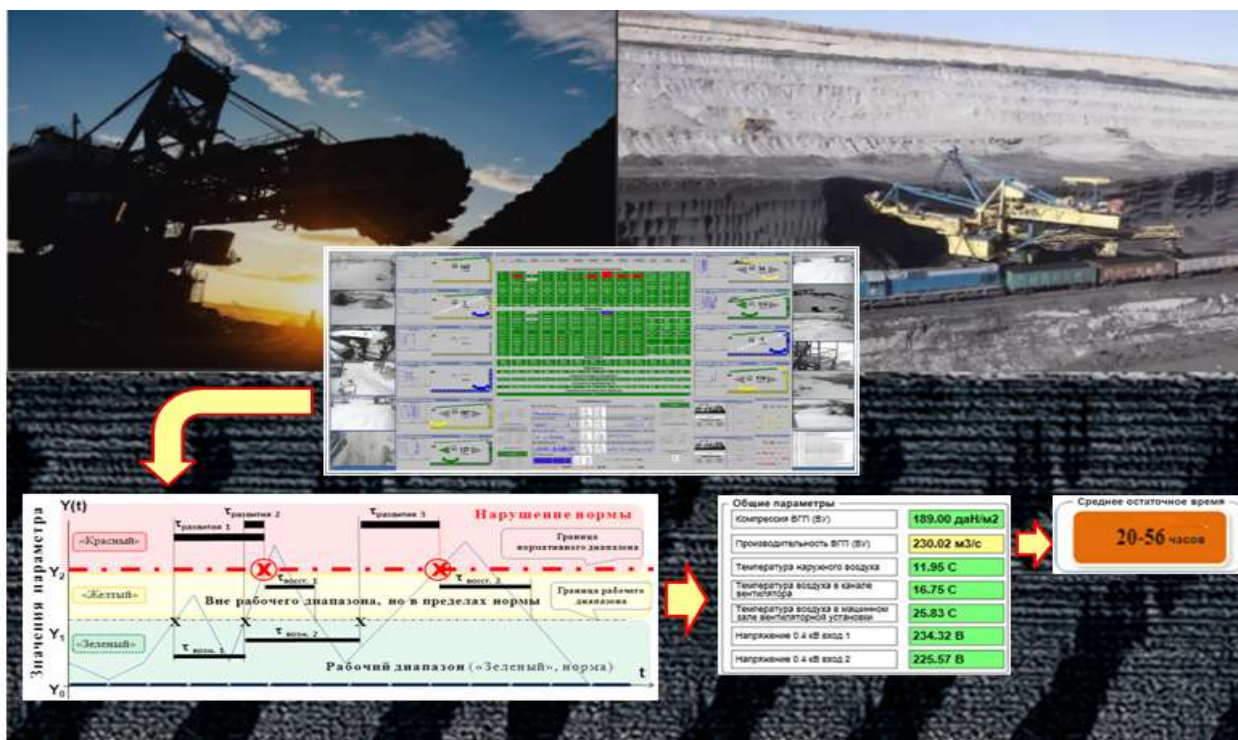


Рис. 3. Пример прогнозирования времени на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона

Пример 3 реализации и извлечения прагматических эффектов. В России создан комплекс обеспечения техногенной безопасности на объектах газораспределения нефтегазовой отрасли, служащий ярким примером достижения прагматических эффектов с использованием предложенных методов аналитического прогнозирования рисков. В созданном комплексе периферийные газорегуляторные пункты дополнительно оснащены датчиками вибрации (фиксирование землетрясения), пожара, наводнения, несанкционированного доступа, урагана, видеоизображение внутренней и внешней обстановки, а также интеллектуальными средствами реакции, способными реализовать процедуры распознавания, идентификации и раннего прогнозирования развития нештатных ситуаций. Реализованные технологические возможности использования космической связи позволяют реагировать за секунды. Эксплуатация комплекса в Калужской и Курской областях обеспечила безаварийное функционирование нефтегазовых объектов (до этого – по несколько аварийных ситуаций в год). Применение комплекса в период 2009-2014гг. обеспечило возможность экономии 8,5 млрд рублей, что достигнуто за счет эффективного внедрения функций прогнозирования рисков и обеспечения техногенной безопасности в технологическом процессе контроля и мониторинга газораспределения. Работа была удостоена премии Правительства РФ в области науки и техники за 2014 год [10, 15].

Выводы

Предложен подход к решению задач когнитивной обработки данных мониторинга в системах ИИ, развивающий сложившиеся подходы к прогнозированию рисков, обеспечению и повышению безопасности систем. Представлены вероятностные модели и методы, позволяющие прогнозировать вероятности «успеха» и/или риска неудачи, поддерживающие их программные инструментари, способы решения обратных задач. Применение предложенного подхода позволяет осуществлять противодействие угрозам и эффективного управления рисками. Работоспособность подхода проиллюстрирована на практических примерах.

Литература

- [1] Костогрызов А.И., Петухов А.В., Щербина А.М. «Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа». М.: Изд. «Вооружение, политика и конверсия», 1994.-278с.
- [2] Костогрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. М.: Изд. «Вооружение. Политика. Конверсия», 1996.- 280 с.
- [3] Kostogryzov A.I. "Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ)." Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium, USA, Dallas, pp.63-70, 2000.
- [4] Безкорвайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК. 150 задач анализа и синтеза и примеров их решения. М.: Изд. «Вооружение. Политика. Конверсия», 2002.- 304 с.
- [5] Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М. Изд. "Вооружение, политика, конверсия", 2004, 2-е изд.-2005.- 395с.
- [6] Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд. "Вооружение, политика, конверсия", 2008. – 404с.
- [7] Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. (2011) Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems, Proceedings of the 1st Intern.Conf. on Transportation Information and Safety, ICTIS, June 30-July 2,2011, Wuhan, China, p. 845-854
- [8] Kostogryzov A., Nistratov G., Nistratov A. (2012) Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, DOI: 10.5772/46106, Total Quality Management and Six Sigma, InTech, 2012, pp. 127-196, <http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management>
- [9] Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. (2013) Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes, DOI: [10.4236/ajor.2013.31A021](https://doi.org/10.4236/ajor.2013.31A021), American Journal of Operations Research, 2013, 3, p.217-244, <http://www.scirp.org/journal/ajor/>
- [10] Акимов В.А., Костогрызов А.И., Махутов Н.А., Фортон В.Е., Шойгу С.К. и др. /Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности. М.: МГОФ «Знание», 2015, - 936с.
- [11] Моделирование процессов в жизненном цикле систем "Моделирование процессов" - "ноу-хау" // Свидетельство о государственной регистрации программы для ЭВМ №2004610858
- [12] Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем // Свидетельство о государственной регистрации программы для ЭВМ №2006610219
- [13] Программно-вычислительный комплекс оценки качества производственных процессов // Свидетельство о государственной регистрации программы для ЭВМ №2010614145.

[14] Бурцева А.Е. Управление качеством функционирования системы транспортировки газа в условиях полуострова Ямал. Диссертация на соискание ученой степени канд. техн. наук по специальности 05.02.23. Научный руководитель - Костогрызов А.И., РГУ нефти и газа им. И.М.Губкина, 2013г.

[15] Абросимов Н.В., Костогрызов А.И., Махутов Н.А., Фортон В.Е., Шойгу С.К. и др. /Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Техногенная, технологическая и техносферная безопасность. М.:МГОФ «Знание», 2018, - 1016с. ISBN 978-5-87633-173-1.

[16] V. Artemyev, A. Kostogryzov, Ju. Rudenko, O. Kurpatov, G. Nistratov, A. Nistratov, Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRs), Milan, Italy, December 20-22, 2017, pp. 368-373. ISBN: 978-1-5386-3321-2

[17] Probabilistic modeling in system engineering. InTechOpen, Edited by A. Kostogryzov, 2018, 279p. ISBN: 978-1-78923-775-7

[18] A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, Combinatorics and Control, InTechOpen, 2019. DOI: <http://dx.doi.org/10.5772/intechopen.89168>

Risks prediction for artificial intelligence systems using monitoring data

Kostogryzov A.I.¹⁶²

The approach for cognitive processing of monitored data is proposed. An application for artificial intelligence systems allows to use the possibilities of probabilistic modeling. The approach includes the models and methods for prediction a probability of “success” and/or a risk of “failure”, software tools to support them, techniques for solving the problems of rationale preventive measures against threats and effective risk control. The approach applicability is demonstrated by examples.

Keywords: analysis, control, model, probability, risk, safety, system

¹⁶² Kostogryzov A.I., Dr. Sc., Professor, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, Moscow, Russia, e-mail: Akostogr@gmail.com

Аспекты оценки эффективности подготовки специалистов в области информационной безопасности

Кузнецова В.Ю.¹⁶³

В статье рассмотрены компетентностный и психологический аспекты оценки будущих специалистов в области защиты информации, описана технология оценки психологической предрасположенности абитуриентов к работе в области ИБ, а также показаны результаты опросов работодателей по вопросу ключевых компетенций сотрудника сферы информационной безопасности.

Ключевые слова: кадровое обеспечение, информационная безопасность, психологический портрет, компетентностный подход.

Введение

Одним из основных аспектов политики в области защиты информационных ресурсов Российской Федерации, является качественная подготовка специалистов в сфере защиты информации (ЗИ). Современные федеральные государственные образовательные стандарты (ФГОС) третьего поколения базируются на компетентностном подходе, который предполагает способность выпускников профильных учебных учреждений обладать знаниями, умениями и личностными качествами для продуктивной профессиональной деятельности [1-3].

В связи с этим перед вузами встает вопрос: что должен знать и уметь специалист в области ЗИ, какими профессиональными компетенциями он должен обладать? Также следует учитывать, что работа в такой области, как информационная безопасность, связана с психологической устойчивостью и моральными качествами. Следовательно, необходимо разработать методы учебно-воспитательной работы, в которых бы сочетались получение прочных профессиональных знаний и формирование необходимых нравственных качеств.

Проведенное исследование

Для исследования актуальных представлений различных групп экспертов о степени значимости профессиональных и общекультурных компетенций для успешной работы в области защиты информации был проведен опрос, в котором в качестве экспертов выступили: руководители подразделений правоохранительных и контролирующих органов государственной власти, представители банков и финансовых компаний, работники организаций, работающих в сфере оказания услуг по обеспечению ИБ, преподаватели профильных кафедр астраханских вузов.

Методом сбора данных было анкетирование. Эксперту предлагалось ранжировать по степени возрастания значимости 20 профессиональные (ПК) и 10 общекультурных компетенции (ОК) специалиста. ПК были, согласно [4-5] объединены в следующие категории: эксплуатационная (Э); организационно-управленческая (ОУ); проектная (П); экспериментально-исследовательская (ЭИ); научно-исследовательская (НИ). Кроме того, было необходимо сравнить между собой значимость выделенных выше категорий компетенций, а также ПК и ОК в целом, и расставить в списке по степени важности.

Обработка результатов анкетирования

Результаты обработки полученных оценок позволили сделать следующие выводы:

¹⁶³ Кузнецова Валентина Юрьевна, аспирант, ассистент кафедры информационной безопасности Астраханского государственного университета, Астрахань, arhelia@bk.ru

1. Ранг *ПК* по мнению большинства групп экспертов оказался равным рангу *ОК* в целом. Это свидетельствует о том, что важной частью компетенций специалиста по ЗИ являются личностные качества.

2. Эксперты правоохранительных органов в качестве важных указали организационно-управленческие компетенции, группа банковских работников - проектные, а представители ВУЗа - экспериментально-исследовательские и эксплуатационные компетенции.

3. Большинство групп экспертов на последнее место по значимости поставили компетенции, связанные с научно-исследовательской деятельностью. Подобное отношение работодателей объясняется тем, что развитие и финансирование исследовательских проектов, направленных на долгосрочную перспективу, для них не актуально или экономически нецелесообразно.

Также эксперты отметили, что будущий специалист в области ИБ не только должен обладать необходимым опытом и знаниями, но и по складу характера должен максимально соответствовать должности. Тогда он не только справится с задачей быстрее и качественнее, но и затратит на это меньше сил [6-7].

Переход к приему в ВУЗы по результатам ЕГЭ без личного собеседования не позволяет проводить диагностику личностных качеств и психологической устойчивости и оценивать профессиональную пригодность желающих обучаться по специальностям, связанным с информационной безопасностью. Однако такие методики есть. Одна из них – технология визуального распознавания «7 радикалов» В.В. Пономаренко, позволяющая определить основные черты характера человека и построить его психологический профиль по наблюдаемым внешним признакам [8].

На основании профиля формулируется психологический профиль, который описывает характер и поведенческие нюансы человека. Определение набора радикалов, влияющих на характер испытуемого, позволяет выявить феномены и закономерности его поведения; отношение к видам деятельности (какие задачи обладатель данного профиля будет решать легко, а с какими справиться не сможет); особенности коммуникации и управления; скрытые черты характера (как и когда могут проявиться черты характера, которые человек в стандартной ситуации не показывает).

Данная методика успешно применяется кадровыми служащими для подбора сотрудников, в том числе и для правоохранительных органов в области ИБ, но пока на данный момент для профотбора студентов не используется.

Выводы

Таким образом, требования современного рынка труда, специфика компетенций, необходимых для успешного освоения специальности требуют модернизации механизма отбора кадров для обучения и дальнейшей работы в сфере обеспечения ИБ, особенно с точки зрения психологической предрасположенности абитуриентов к работе в области ЗИ.

Полученные в ходе исследования результаты могут быть использованы для улучшения учебного процесса и уточнения методологии подготовки специалистов по ИБ в рамках современного ФГОС на основе более четкого понимания требований работодателей, а также для повышения квалификации действующих работников сферы в рамках профессиональной переподготовки и повышения квалификации работников.

Кроме того, реализованный в работе подход может быть применен для модернизации приемных кампаний на направления подготовки укрупненной группы специальностей «Информационная безопасность» [9-10].

Литература

1. Ажмухамедов И.М., Гурская Т.Г., Князева О.М., Оценка эффективности подготовки специалистов по информационной безопасности // Математические методы и информационно-

технические средства. Материалы XII Всероссийской научно-практической конференции: под ред. И.Н. Старостенко, Е.В. Михайленко, 2016: - Краснодар: С.3-5.

2. Анурьева, М.С. Направления развития отечественной системы подготовки специалистов по защите информации // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2013. Т. 18. № 1. С. 230-232.

3. Гришина Е. А. Оценка уровня сформированности профессиональной компетентности выпускников-психологов в практической деятельности // Вестн. Череповецк. гос. ун-та. 2008. № 1. С. 131–135.

4. Ажмухамедов А.И. Нечеткая когнитивная модель оценки эффективности работы персонала // [Электронный ресурс]. URL: <http://science.spb.ru/files/IzvetiyaTI/2016/33/articles/22/files/assets/common/downloads/publication.pdf> (дата обращения 26.10.2019).

5. Ажмухамедов И.М., Проталинский О.М. Методология моделирования слабоформализуемых социотехнических систем // Искусственный интеллект и принятие решений. – Москва: Федеральный исследовательский центр «Информатика и управление», 2014, С.145-150.

6. Ажмухамедов А.И. Модели и методы информационной поддержки управления социальной подсистемой организации на основе нечеткого когнитивного подхода: дис. ... канд. тех. наук. Астраханский. гос. тех. Университет: - Астрахань, 2017.

7. Личко А.Е. Психопатии и акцентуации характера у подростков/ А.Е. Личко. – 2-е изд., доп. и перераб. – М. : Медицина, 1983. – 255 с.

8. Кравцов А.А. Специфика профессиональной подготовки студентов по направлению информационная безопасность // Вестник Московского государственного лингвистического университета. – М.: 2013. № 16 (676). С. 137-149.

9. Брумштейн Ю.М., Гурская Т.Г., Ахмедова Р.Р., Александрович В.П. Подготовка специалистов по информационной безопасности на юге европейской части России: анализ доступности и полноты информации с позиций абитуриентов, вузов, регионов // Известия Волгоградского государственного технического университета, Волгоградский государственный технический университет: - Волгоград: С.7-16.

10. Макаревич О.Б. Комплексная система подготовки кадров по направлению «Информационная безопасность» // Известия ЮФУ. Технические науки. 2012. № 4 (129). С. 18-24.

Научный руководитель: Ажмухамедов Искандар Маратович, доктор технических наук, профессор, зав. кафедрой информационной безопасности Астраханского государственного университета, Астрахань, aim_agtu@mail.ru

Aspects of Evaluating Preparation Efficiency Information Security Specialists

V. Yu. Kuznetsova¹⁶⁴

Abstract. *The article considers the competence and psychological aspects of evaluating future specialists in the field of information security, describes the technology for assessing the psychological predisposition of applicants to work in the field of information security, and also shows the results of surveys of employers on the key competencies of an information security officer.*

Keywords: *Staffing, information security, psychological port-ret, competency-based approach.*

¹⁶⁴ Valentina Yu. Kuznetsova, postgraduate student, assistant of chair «Information security», Astrakhan State University, Astrakhan, arhelio@bk.ru

Исследование современных технологий добычи электронных денег в сетях блокчейн

Кулагин Г.И.¹⁶⁵

Аннотация. В статье на основе изучения механизма работы блок-сетей проведен анализ особенностей работы существующего Протокола извлечения электронных денег и подтверждения транзакции, в том числе алгоритма, который базируется на его работе, а также угроз, связанных с его использованием, на примере Bitcoin.

Ключевые слова: кибервалюта, криптовалюта

Введение

Электронные деньги получают всё более широкое распространение, ввиду удобства расчётов за покупки товаров в сети Интернет, высокой скорости проведения транзакций и безопасности сделок. Одним из перспективных видов электронных денег является криптовалюта [1].

Инструмент, необходимый для осуществления деятельности, связанной с криптовалютами – технология блокчейн, одной из основных компонент работы которой является майнинг, то есть процесс добычи новых блоков для функционирования сети, и понимание различных подходов к его реализации позволит создавать новые и улучшать существующие блокчейн-системы.

Структура и принцип работы сети на основе технологии блокчейн

Суть структуры сети, основанной на технологии блокчейн, заключается в создании последовательного неизменяемого списка записей, называемых блоками, которые связываются в цепь при помощи сложных математических алгоритмов и защищены криптографическим шифрованием. Каждый вновь созданный блок содержит информацию о накопившихся транзакциях и заголовок, а также хранит в зашифрованном виде данные о предыдущих блоках.

Любой участник сети блокчейн вправе создать свой собственный блок из транзакций, которые ожидают своего включения в цепь в так называемом "пуле неподтверждённых транзакций". Когда блок сформирован, остальные участники сети проверяют, является ли данный блок истинным и затем, если все согласны, этот блок подсоединяется строго к концу цепочки. Как только это произошло, внести в сформированный блок изменения уже невозможно.

Добавление нового звена в цепь приводит к автоматическому обновлению базы данных на всех подключённых к системе компьютерах, после чего участники сети (майнеры) приступают к формированию следующего блока.

Несмотря на такие преимущества блокчейн-сетей как децентрализация, прямая передача данных, прозрачность, безопасность, надёжность, компромисс и мгновенная синхронизация при их применении необходимо учитывать:

- возможность возникновения неопределенностей в состоянии системы;
- необходимость создания блоков через равные промежутки времени;
- сложность добычи нового блока должна изменяться пропорционально количеству участников процесса майнинга и их ресурсам;
- неравномерность распространения информации в системе;
- соперничество участников сети за вознаграждения от создания блока;

¹⁶⁵ Кулагин Глеб Игоревич, студент ИУ8-94, МГТУ им. Баумана, Москва, gleb.kulagin@yandex.ru

– убыточность для нечестных участников сети в связи с нарушением ими правил работы сети.

Метод, учитывающий эти достаточно строгие требования, называется Proof-of-Work (PoW) – доказательство выполнения работы.

Особенности работы метода Proof-of-Work на примере Bitcoin

Метод PoW – это протокол достижения консенсуса в сети блокчейн, применяемый для подтверждения транзакций и создания новых блоков. Концепции работы этого метода будут продемонстрированы на примере алгоритма Hashcash, используемого для добычи блоков в криптовалюте Bitcoin.

В Bitcoin (биткойн) используется следующая задача: "Найти такую последовательность символов, называемую *nonce*, чтобы результат двойного хеширования функцией SHA-256 итогового хеша всех транзакций, конкатенированного с этим *nonce*, был меньше заданной цели" [2].

$$bh = H(x \parallel nonce) \leq D(h), \quad (1)$$

где bh – искомый Block Header, то есть заголовок блока, $H()$ – функция хеширования, $D(h)$ – некоторая цель, выраженная в виде числа.

Эта задача не имеет алгоритма решения, кроме полного перебора.

По задумке создателя биткойна [3], блок должен добываться в среднем один раз в 10 минут, а вероятность его добычи зависит от количества узлов сети, занятых его поиском, и от их мощности. Поэтому, в основе сети блокчейн лежит идея сложности и цели.

Каждые 2016 блоков сеть вычисляет отношение:

$$k_{diff} = \frac{20160}{actual\ time} \quad (2)$$

где *actual time* – время, за которое были добыты 2016 последних блоков, 20160 минут – время за которое ожидалась их добыча.

Полученный коэффициент сложности определяет, насколько быстро находятся блоки. Если было найдено больше 2016 блоков за 2 недели, значит, вычислительную трудоёмкость задачи нужно повысить, а если меньше – понизить.

Для этого величина сложности, которая была до этого, умножается на полученный коэффициент.

$$New\ Difficulty = Difficulty * k_{diff} \quad (3)$$

Полученная сложность определяет хешрейт, необходимый оборудованию для успешного нахождения блока с приемлемой вероятностью, и цель – то число, меньше которого нужно найти значения хеша, чтобы вставить блок в цепь. Заранее определённая максимальная цель делится на полученную сложность, и результатом является новая цель – $D(h)$ из уравнения (1).

$$D(h) = \frac{MaxTarget}{New\ Difficulty} \quad (4)$$

Чем выше значение цели, тем точнее найти решение задачи, и наоборот.

В случае с алгоритмом Hashcash, цель – ничтожно малое число по сравнению со всей областью значений хеша и требуются квинтиллионы попыток, чтобы найти подходящее. Сам процесс решения задачи прост – для него требуется оборудование с высокой мощностью. Чем выше мощность, тем больше хешей в секунду можно перебрать. Начиная с нуля и постепенно инкрементируя двоичное значение *nonce*, алгоритм раз за разом

хеширует входные данные и сравнивает значение хеша с целью. Когда будет найден хеш меньше цели, алгоритм переходит на следующий этап.

Участник, решивший задачу, публикует блок в сеть и начинается проверка его подлинности. Если все транзакции в блоке правильные – блок включается в цепь, и процесс начинается заново. Майнер, встроивший свой блок получает награду и комиссию за переводы, которые были в блоке.

Каждый блок уникален, так как какие бы транзакции не выбрали два любых майнера, в начале блока указан кошелек майнера, на который ему поступит награда. Полученные монеты – это новые биткойны, представляющие из себя последовательность подписей в блоке, а вся сеть запомнит, что с этим кошельком закреплена запись о получении новых легитимных средств.

Майнеры не всегда в процессе решения задачи меняют только попсе. Некоторые настраивают оборудование так, что если не получается найти решение – итоговый хеш транзакций отвергается, и из пула неподтвержденных транзакций собирается новый набор, от которого вычисляется хеш, и поиск попсе начинается сначала. Такой подход используется, когда значения хеш-функции не могут быть распределены равномерно по всей области значений.

Возможна ситуация, когда для некоторых входных данных искомого попсе нет – тогда необходимо менять входные данные для решения задачи.

Если оборудование может перебирать r хешей в секунду, а D – текущая сложность нахождения нового блока, то вероятность нахождения нового блока за время, меньшее t секунд выражается следующей формулой [4]:

$$P\{T(r) \leq t\} = 1 - \exp\left(\frac{-rt}{D}\right) \quad (5)$$

Пусть число майнеров в сети равно n . Хешрейты каждого из них равны соответственно $r_1 r_2 \dots r_n$. Если майнер публикует блок сразу после его нахождения, то получится, что время T , за которое будет найден новый блок для цепи равняется наименьшей из случайных величин $T(r_i)$. Тогда, согласно свойствам экспоненциального распределения, получим:

$$P\{T = \min(T_1, T_2, \dots, T_n) \leq t\} = 1 - \exp\left(-\frac{t}{D} \sum_{i=1}^n r_i\right) \quad (6)$$

$$P\{T = T_i\} = \frac{r_i}{\sum_{j=1}^n r_j} \quad (7)$$

Данное выражение доказывает честность майнинга – участник, у которого мощность оборудования составляет долю p от мощности суммарно всех майнеров, имеет вероятность равную p найти новый блок быстрее остальных.

Возможна ситуация, когда несколько майнеров найдут решение примерно в одно время, и каждый будет иметь право построить свой блок в цепочку. Тогда произойдет "форк" – разветвление цепочки, характеризующее временной неопределенностью, и устраняется так.

Первоначально будет блокчейн с двумя "хвостами". Каждый узел сети сам решает, какую цепочку продолжать, так как они имеют одинаковую длину, и пока что обе верны. Как только будет найден новый блок, он будет присоединён лишь к одной из двух цепей.

После этого вступает в силу правило – "Всегда придерживаться самой длинной цепочки" – когда будет найден еще один блок, майнер присоединит его к самой длинной последовательности блоков, и следующий за ним поступит также. Итак, второй хвост через

время "отпадёт" – транзакции в нём будут признаны недействительными и сеть продолжит работать, как и прежде.

В случае масштабирования сети может возникнуть ситуация, в которой, во-первых, очень много мощностей работают впустую, а во-вторых, будет появляться много форков, которые впоследствии будут "отваливаться" от цепи и транзакции в них будут признаваться недействительными, что затруднит использование криптовалюты.

Таким образом, данный метод определяет следующее правило безопасности блокчейна: "Пока мощности всех честных участников сети превосходят мощности злоумышленника хотя бы на 1% , невозможно подделать блок или цепь блоков, так как в силах честных участников всегда отвергнуть неправильные блоки и транзакции".

Это является и сильной и слабой стороной данного подхода. Сильной, так как атака на сеть не зависит от навыков атакующего. Слабой, так как для поддержания работы сети одного только биткойна расходуется уже 0,2% всей электроэнергии в мире, и с ростом сети затраты на майнинг только растут.

Большое количество электроэнергии и оборудования тратится на решение бессмысленной математической задачи. И если для первичного распределения монет этот алгоритм выглядит целесообразно, то с течением времени майнинг по такой технологии будет всё менее оправдан.

Поэтому, актуальность метода PoW зависит от того, будут ли пользователи верить в биткойн в дальнейшем. Если к моменту окончания майнинга новых монет (примерно 2021 год) количество транзакций в сети будет недостаточным для того, чтобы окупать затраты майнеров, поддержание работы сети станет убыточным [5].

Ещё одним недостатком метода PoW является то, что объединение майнеров приносит им больше выгоды. Распределение диапазона перебора на сотни тысяч узлов сети приводит к тому, что у больших майнерских сообществ больше шансов найти новый блок. Это придаёт системе некоторую централизацию и негативно сказывается на её безопасности.

Выводы

В статье на основе исследования механизма сети блокчейн проведён анализ особенностей работы, преимуществ и недостатков существующего протокола добычи электронных денег и подтверждения транзакций, включая алгоритм, на которых базируется его работа, а также угроз, связанных с его применением, на примере криптовалюты биткойн.

Метод Proof-of-Work доказал стабильность своей работы при решении задачи масштабирования. И, несмотря на критику, он остаётся надёжным, так как подразумевает достижение консенсуса в любом случае за короткий промежуток времени, а разделение вероятности добычи блока пропорционально вкладу участника в поддержание работы сети является справедливым.

Однако перед алгоритмами майнинга стоит проблема обеспечения достаточной скорости и целостности работы в случае принятия криптовалюты как платёжной системы. Если счёт участников в сети перейдет на миллионы, то из-за задержек в распространении сигнала и трудности достижения консенсуса вся система может перестать стабильно работать.

Поэтому развитие новых протоколов консенсуса – это платформа для популяризации и экспансии всей технологии блокчейн.

Литература

1. Захаров Д.Н., Иванов В.Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. 2017. № S2 (20). С. 30-38.
2. Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen and Dong In Kim. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. SAO/NASA ADS arXiv e-prints Abstract Service, № 1805.02707, 40 с. – Режим доступа: <https://arxiv.org/pdf/1805.02707>.
3. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. The Cryptography Mailing List [Электронный ресурс]. – 2008. – Режим доступа: <https://www.mail-archive.com/search?l=cryptography@metzdowd.com&q=from:%22Satoshi+Nakamoto%22>.
4. Marit Rudlang. Comparative Analysis of Bitcoin and Ethereum. Norwegian University of Science and Technology, 85 с. – Режим доступа: <https://www.hdl.handle.net/11250/2451325>.
5. Yoad Lewenberg, Yonatan Sompolinsky and Aviv Zohar. Inclusive Block Chain Protocols. Financial Cryptography [Электронный ресурс]. – 2016. – Режим доступа: https://www.cs.huji.ac.il/~yoni_sompol/pubs/15/inclusive.pdf.

Научный руководитель: Лебедев А.Н.¹⁶⁶

Research of modern production technologies electronic money in blockchain networks

Kulagin G.I.¹⁶⁷

Abstract the article based on the study of the mechanism of the blockchain network the analysis of peculiarities of work of the advantages and disadvantages of the existing Protocol of extraction of electronic money and a transaction confirmation, including the algorithm, which is based on his work, as well as threats associated with its use, the example of Bitcoin.

Keywords: bitcoin, consensus, mining, transaction.

Principal investigator: Lebedev A.N.¹⁶⁸

¹⁶⁶ Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lebedevan@bmstu.ru

¹⁶⁷ Kulagin Gleb Igorevich, student, Bauman Moscow State Technical University gleb.kulagin@yandex.ru

¹⁶⁸ Anatoly Lebedev, PhD, Bauman Moscow State Technical University, Moscow, lebedevan@bmstu.ru

Доказательство сводимости задачи DLOG к задаче DH

Лебедев А. Н.¹⁶⁹

В работе приводится решение одной из самых давно стоявших теоретических проблем современной криптографии – доказательство эквивалентности взлома протокола Диффи-Хеллмана и решения задачи дискретного логарифмирования в соответствующей конечной группе. Решение задачи получено при условии справедливости гипотезы Римана о распределении нулей ζ -функции Римана на комплексной плоскости.

Ключевые слова: криптография, протокол Диффи-Хеллмана, сведение задачи дискретного логарифмирования к задаче Диффи-Хеллмана

1. Введение

С момента выхода в свет основополагающей работы Диффи и Хеллмана «Новые направления в криптографии» (1976) криптографы пытаются доказать, что сложность взлома протокола Диффи-Хеллмана - выработки общего секрета парой удаленных пользователей сети (задача DH) определяется сложностью известной математической проблемы – задачи дискретного логарифмирования в конечной группе (или задачи DLOG) [1 - 17].

Во многих случаях это, действительно, удастся строго доказать, но в самых интересных для криптографических приложений случаях этого доказать до последнего времени так и не удавалось [8-11].

В настоящем докладе мы изложим доказательство этого факта в предположении, что справедлива гипотеза Римана о том, что все нули ζ -функции Римана на комплексной плоскости лежат на прямой $\text{Re}(z) = 1/2$.

2. Постановка задачи

Определение 1. Пусть G – конечная циклическая группа, порожденная элементом g . Проблема вычисления элемента $g^{(x*y)}$ по элементам g^x и g^y группы G называется *задачей Диффи-Хеллмана* (или для краткости *DH*).

Один из наиболее прямолинейных способов решения проблемы DH, - это вычисление показателя x (или показателя y) по элементам g^x и g^y , а затем – вычисление элемента $g^{(x*y)}$.

Определение 2. Пусть G – конечная циклическая группа, порожденная элементом g . Проблема вычисления по элементу $a = g^x$ числа $x \pmod{p}$, где $p = |G|$ называется *проблемой дискретного логарифмирования* (или *DLOG*) по основанию g .

Для знакомства с детальными обсуждениями отношения этих двух задач можно воспользоваться работами [5-12].

В наиболее полном обзоре по этим и связанным с ними проблемам [8] на стр.12

справедливо отмечается, что при наличии любого способа решения задачи *DH* мы можем с полиномиально отличающейся от ее решения сложностью вычислять значения символа Лежандра

¹⁶⁹ Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., доцент МГТУ им. Н.Э. Баумана, Москва, lebedevan@bmstu.ru

$$\left(\frac{x}{q}\right) = x^{(q-1)/2} \pmod{q}$$

где $q = (p-1)/2$ – также большое простое число.

Число x называется квадратичным вычетом $\pmod{q}$, если значение символа Лежандра для числа x равно 1, и невычетом $\pmod{q}$, если значение символа Лежандра для числа x равно -1.

Далее там говорится: «Аналогично может быть вычислена целая последовательность

$$\left(\frac{x}{q}\right), \quad \left(\frac{x+1}{q}\right), \quad \left(\frac{x+2}{q}\right), \quad \dots \quad (1)$$

значений символов Лежандра. К сожалению, не известно способов эффективного вычисления числа $x \pmod{p}$ из этой неявной информации о числе x .»

3. Вычисление показателя x за полиномиальное от $\log(q)$ время

Предположим сначала для простоты изложения, что простое число p , по модулю которого ведутся основные вычисления, имеет вид $p = 4*q + 3$ (можно показать, как освободиться от этого ограничения на число p).

В этом случае хорошо известно [1], что на левой (младшей) половине отрезка $[1, q-1]$ количество квадратичных вычетов больше, чем количество невычетов.

Таким образом, вычисляя на основании алгоритма решения задачи *DH*, последовательность значений символов Лежандра (1), мы согласно известным результатам по теории чисел Ю. В. Линника [1] в предположении о справедливости гипотезы Римана о нулях ζ -функции Римана на комплексной плоскости [1], можем на длине последовательности (1), ограниченной сверху функцией вида $O(\log^2 q)$, определить, находится ли число x на левой (младшей) или правой половине отрезка $[1, q-1]$. А это означает, что мы можем определить старший бит в двоичном представлении числа x .

Затем, удаляя найденный старший бит числа x , и умножая полученный результат на 2, повторяем описанную выше процедуру.

В результате мы сможем также за время не более, чем $O(\log^2 q)$ определить второй по старшинству бит в двоичном представлении числа x .

Повторяя далее аналогичную процедуру не более, чем $O(\log q)$ раз, мы сможем определить все биты в двоичном представлении числа x .

4. Полиномиальные алгоритмы сводимости задачи *DLOG* к задаче *DH*

На основании изложенного выше описания алгоритма определения числа x по элементу $a = g^x$ мы можем сформулировать следующую теорему

Теорема 1. В предположении о справедливости гипотезы Римана о нулях ζ -функции Римана на комплексной плоскости можно построить алгоритм решения задачи *DLOG*, отличающийся по сложности не более, чем в $O(\log^3 q)$ раз от сложности алгоритма решения задачи *DH*.

Несложная модификация описанного алгоритма сводимости аналогичной задачи для группы точек эллиптической кривой над конечным полем, обозначаемой как *ECDLOG*, показывает, что справедлива следующая

Теорема 2. В предположении о справедливости гипотезы Римана о нулях ζ -функции Римана на комплексной плоскости можно построить алгоритм решения задачи *ECDLOG*, отличающийся по сложности не более, чем в $O(\log^3 q)$ раз от сложности алгоритма решения задачи *ECDH*.

5. Выводы

Получены серьезные новые аргументы в пользу подтверждения того факта, что сложность взлома протокола Диффи-Хеллмана при правильном выборе циклической группы, в которой производятся вычисления при выработке общего секрета парой удаленных пользователей сети, отличается от сложности задачи *DLOG* (соответственно *ECDLOG*) не более, чем в полиномиальное число раз.

Таким образом, всеобщая убежденность криптографов в том, что стойкость протокола Диффи-Хеллмана определяется сложностью задачи *DLOG* (соответственно *ECDLOG*) получает серьезное дополнительное подкрепление.

Литература

1. И. М. Виноградов, Основы теории чисел, Издание 16-е, Изд. Наука, М. 1997.
2. D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.*, Vol. 48, No. 177, pp. 95-101. 1987.
3. M. A. Cherepnev, On the connection between discrete logarithms and the Diffie-Hellman problem, *Discrete Math. Appl.*, 1996.
4. D. Coppersmith, I. Shparlinsky, On polynomial approximation and the parallel complexity of the discrete logarithm problem and breaking the Diffie-Hellman cryptosystem, *preprint*, Nov. 1996.
5. B. den Boer, Diffie-Hellman is as strong as discrete log for certain primes, *Advances in Cryptology – CRYPTO'88*, Lecture Notes in Computer Science, Vol. 403, pp.530-539, Springer-Verlag, 1989.
6. W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp. 644-645, 1976.
7. T. El-Gamal, A public key cryptosystem and signature scheme based on the discrete logarithm, *IEEE Transactions on Information Theory*, Vol. 31, No. 4, pp. 469-472, 1985.
8. N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, Vol. 48, pp. 203-209, 1987.
9. U. M. Maurer, S. Wolf, The Diffie-Hellman Protocol, Scientific Report, Grant SNF No. 20-42105.94, 1994.
10. U. M. Maurer, Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms, *Advances in Cryptology – CRYPTO'94*, Lecture Notes in Computer Science, Vol. 839, pp. 271-281, Springer-Verlag, 1994.
11. U. M. Maurer, S. Wolf, Diffie-Hellman oracles, *Advances in Cryptology – CRYPTO'96*, Lecture Notes in Computer Science, Vol. 1109, pp. 268-282, Springer-Verlag, 1996.
12. U. M. Maurer, S. Wolf, Lower bounds on generic algorithms in groups, *Proceedings of EUROCRYPT'98*, Lecture Notes in Computer Science, Vol. 1403, pp. 72-84, Springer-Verlag, 1998.
13. U. M. Maurer, S. Wolf, The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms, *SIAM Journal on Computing*, Vol. 28, No. 5, pp. 1689-1721, 1999.
14. K. S. McCurley, The discrete logarithm problem, in *Cryptology and computational number theory*, C. Pomerance (Ed.), Proceedings of Symposium In Applied Math., Vol. 42, pp. 49-74, American Math. Society, 1990.
15. R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1990.

16. C. P. Schnorr, Efficient identification and signatures for smart cards, *Advances in Cryptology – CRYPTO'89*, Lecture Notes in Computer Science, Vol. 435, pp. 239-252, Springer-Verlag, 1998.
17. V. Shoup, Lower bounds for discrete logarithms and related problems, *Advances in Cryptology – EUROCRYPT'97*, Lecture Notes in Computer Science, Vol. 1233, pp. 256-266, Springer-Verlag, 1997.

Proof of Reduction of the DLOG to the DH Problem

Lebedev A.N.¹⁷⁰

Abstract. *The paper presents the solution of one of the most long-standing theoretical problems of modern cryptography - the proof of equivalence of the Diffie-Hellman Protocol cracking and the solution of the discrete logarithm problem in the corresponding finite group. The solution of the problem is obtained under the condition of validity of the Riemann hypothesis on the distribution of zeros of the Riemann ζ -function on the complex plane.*

Keywords: *cryptography, Diffie-Hellman Protocol, DLOG, DH-problem, reducing the discrete logarithm problem to the Diffie-Hellman problem*

¹⁷⁰ Anatoly Lebedev, Ph.D., Assistant Prof., Bauman Moscow State Technical University, Moscow, lebedevan@bmstu.ru

Анализ стратегий ложных информационных систем

Лебедев А.Н.¹⁷¹, Марченков С.Д.¹⁷²

В статье автор рассматривает классификацию ложных информационных систем, то как они применяются в архитектуре всей сети. В ходе исследования рассматриваются тенденции принятия решений со стороны средств защиты информации, установленных на ложной информационной системе для противодействия различным атакам, в том числе для предотвращения угроз от несанкционированного доступа. Приводится анализ потребляемых ресурсов для обеспечения функционирования ложных информационных систем и оценка эффективности таких систем.

Ключевые слова: теория игр, несанкционированный доступ, информационная безопасность, средства обнаружения вторжения, виртуализация, honeypot

Введение.

Не все настройки комплексов СЗИ могут покрыть все уязвимые места ИС, ни одна система до конца не защищена. Так для обнаружения угроз «нулевого дня» или для донастройки СЗИ до более защищенного исполнения нередко применяют ложные информационные системы (ЛИС), которые стоят за средствами СОВ и при обнаружении злоумышленника принимают удар на себя. Таким образом, удастся проследить ходы противника и в зависимости от них выработать стратегии противодействия и доработки целевой ИС [1-5].

Классификация и архитектура

При реализации своих функций ЛИС обеспечивает три представленных ниже уровня в разных компонентах ИС¹⁷³.

1. Уровень сегмента (основных компонентов целевой системы). ЛИС имитирует целевую систему в целом.

2. Уровень хоста. Предполагает размещение компонентов ЛИС, имитирующих отдельные хосты, в компьютерной сети целевой системы. Этот уровень соответствует парадигме «хостов-ловушек» («Honeypot»).

3. Уровень сервиса/приложения. Целевой модуль сервиса/приложения вместе с модулем обмана вкладывается в обертку.

Структура динамической ДИС представлена в соответствии с рисунком 1 и отражает все три уровня.

¹⁷¹ Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lebedevan@bmstu.ru

¹⁷² Марченков Сергей Дмитриевич, студент, группы ИУ8-112, МГТУ им. Н.Э. Баумана, Москва, Marchenkov.s.d@gmail.com

¹⁷³ https://studbooks.net/1149627/informatika/arhitektura_sovremennyh_lozhnyh_informatsionnyh_sistem

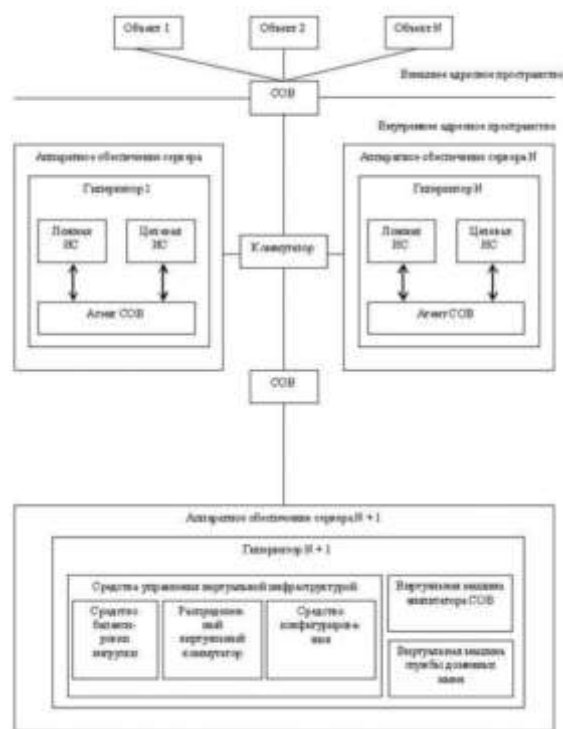


Рис.1. Динамическая структура ЛИС

В зависимости от назначения и решаемых информационной системой задач строится и ЛИС. Как правило ЛИС устанавливается на виртуальной машине или облачном сервере, подключенном к сети, но изолированным и строго контролируемым системными и сетевыми командами. Чтобы злоумышленники заметили обманную систему и начали атаковать ее, ЛИС разработаны так, чтобы быть преднамеренно уязвимыми, со слабостями, которые злоумышленник обнаружит и попытается использовать.

Существующие модули ЛИС, направленные на следующие обманные маневры¹⁷⁴:

- SSH ловушки (примеры, Kippo, Cowrite);
- HTTP ловушки (примеры, Glustopf, Nodepot, Google Hack HoneyPot);
- WordPress ловушки (Formidable HoneyPots, Blackhole for Bad Bots, Wordpot);
- Ловушки БД (ElasticHoney, HoneyMySQL, MongoDB-HoneyProxy);
- Email ловушки (HoneyMail, Mailoney, SpanHat);
- IoTловушки (HoneyThing, Kako);
- и другие (Dionaea, Miniprint, HoneyPot-ftp, HoneyNTP).

Соответственно выделяют некоторые признаки ЛИС:

- исследовательские / производящие;
- с высоким уровнем взаимодействия / с низким уровнем взаимодействия;
- программные / аппаратные / программно –аппаратные;
- степень масштабируемости.

Применяемые стратегии

Рассмотрим некоторые случаи применения ЛИС.

Предполагается, что с ростом популярности IoT, все чаще происходят DDOS атаки с использованием ботнетов. При использовании обороняющейся стороной (А) и атакующей (В), соответственно стратегий А: {«игнорировать активность», «усилить мониторинг»} и В:

¹⁷⁴ <https://securitytrails.com/blog/top-20-honeypots>

{«завершить атаку», «продолжить без паузы», «сделать паузу в атаке»}. Средний выигрыш игрока определяется следующим образом¹⁷⁵:

$$\overline{W}_A(p) = \overline{w}_A(P_A, P_B) = \sum_{s \in S} w_A(s) p(s) = \sum_{s_1 \in S_A} \sum_{s_2 \in S_B} w_A(s_1, s_2) \cdot P_{A, s_A} \cdot P_{B, s_B}$$

(1)

где W_A – функция выигрыша ЛИС, S_A, S_B – множество возможных ситуаций игроков А, В.

Если решать простую задачу о покрытии при различных условиях игры, можно с большой вероятностью вычислить есть ли оптимальные стратегии в чистых стратегиях игрока А, которые будут давать монотонно неубывающие функции выигрыша¹⁷⁶.

С обеих сторон затрачиваются ресурсы на реализацию стратегий атак и защиты. Можно формально описать затраты игрока А [5]:

$$C_A(t) = \sum_{i=1}^n c_i t_m(2)$$

где n – количество дополнительных параметров наблюдений,

c_i – затраты на мониторинг i -го параметра в течении времени t_m

Затраты игрока В вычисляются аналогично.

Оценка эффективности

Проведенные эксперименты показывают затраты на развертывание системы ЛИС в соответствии с таблицей 1.

Таблица 1

Расход вычислительных ресурсов сервера виртуализации

Объект	Процессорное время	Загруженность канала связи	Оперативная память	Память на жестком диске
Целевая ВМ	0,7%	0,001%	2 ГБ	42 ГБ
Ложная ВМ	0,75%	0,00005%	512 МБ	21 ГБ
Гипервизор	0,5%	0,0005%	256 МБ	0,5 ГБ

При небольших затратах на вычислительные ресурсы, ЛИС справляется с ее главной задачей отвлечением, атакующей стороны от целевой ИС, на обнаружение ЛИС или выхода ее из строя уходит от 10 минут до часа.

Выводы.

В ходе исследований были проанализированы методы настройки СЗИ с ЛИС, вычислена оценка эффективности по затрачиваемым ресурсам на основе методов виртуализации.

¹⁷⁵ <https://cyberleninka.ru/article/n/primenenie-metodov-teorii-igr-v-sistemah-obnaruzheniya-vtorozheniy/viewer>

¹⁷⁶ <http://dropdoc.ru/doc/10092/servisa-v-komp. yuternoj-seti-dlya-sistem-nepreryvnogo%3Bpdf>

Литература

1. Вишнеvский А.С. Обманная система для выявления хакерских атак, основанная на анализе поведения посетителей веб-сайтов // Вопросы кибербезопасности. 2018. № 3 (27). С. 54-62.
2. Калашников А.О. Пример использования теоретико-игрового подхода в задачах обеспечения кибербезопасности информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 49-54.
3. Сагатов Е.С., Шкирдов Д.А., Сухов А.М., Баскаков А.В. Обнаружение источников сетевых вторжений с помощью метода ловушек // Защита информации. Инсайд. 2018. № 5 (83). С. 16-21.
4. Шматова Е.С. Выбор стратегии ложной информационной системы на основе модели теории игр // Вопросы кибербезопасности. 2015. № 5 (13). С. 36-40.
5. Язов Ю.К., Сердечный А.Л., Шаров И.А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55-60.

Научный руководитель: Лебедев Анатолий Николаевич, кандидат физико-математических наук, доцент МГТУ им. Н. Э. Баумана, lebedevan@bmstu.ru.

Analysis of the Honeypots Lebedev A.N.¹⁷⁷, Marchenkov S.D.¹⁷⁸

In the article the authors consider the classification of false information systems, how they are used in the architecture of the entire network. The study examines the trends of decision - making by information security tools installed on a false information system to counter various attacks, including to prevent threats from unauthorized access. The analysis of consumed resources to ensure the functioning of complex information systems and evaluation of the effectiveness of such systems is given.

Keywords: game theory, unauthorized access, information security, intrusion detection, virtualization, honeypot

¹⁷⁷ Anatoly Lebedev, Ph.D, Bauman Moscow State Technical University, Moscow, lebedevan@bmstu.ru

¹⁷⁸ Sergey Marchenkov, student of Bauman Moscow State Technical University, Moscow, Marchenkov.s.d@Gmail.com

Исследование стеганографического метода хранения информации в текстурах 3D-объектов

Лебедев А.Н.¹⁷⁹, Николаенкова Е.К.¹⁸⁰

Аннотация. С расширением использования компьютерных сетей одной из важнейших задач становится обеспечение конфиденциальности и безопасности передаваемой информации. Для безопасной передачи данных в пункт назначения без нежелательного раскрытия или повреждения используется стеганография. Видеоигры представляют собой чрезвычайно популярный, широко распространенный пример передачи больших объемов данных между удаленными пользователями, что делает их привлекательными для стеганографии. Однако сегодня стеганография в видеоиграх является практически неисследованной темой. 3D-стеганография используется для встраивания или скрытия информации в 3D-объекты, не вызывая видимых или обнаруживаемых изменений. В работе приводится метод, с помощью которого информация может быть скрыта в трехмерной карте видеоигры.

Ключевые слова: стеганография, наложение текстур, метод Хсу и Ву, цифровой водяной знак, компьютерная графика

Введение

Список стеганографических методов ежегодно пополняется, изобретают более надежные и оригинальные способы сокрытия информации, в частности способ встраивания скрытых сообщений в трехмерные объекты [1].

3D-объекты играют ключевую роль во многих популярных и передовых технологиях, таких как виртуальная реальность. Приложения криптобезопасности для 3D-объектов и графики приобретают все большее значение, учитывая большое разнообразие способов создания 3D-объектов, используя программное обеспечение или 3D-сканирование, и учитывая их повсеместное использование во многих приложениях. Сокрытие информации, включая водяные знаки и стеганографию, – метод, который может скрывать информацию в цифровых файлах, не вызывая заметных изменений в носителях. Сокрытие 3D-информации началось в конце 90-х годов [2], когда художники и дизайнеры 3D-графики хотели обеспечить соблюдение своих авторских прав. С тех пор были предложены различные методы сокрытия трехмерной информации [3-6].

Требования к алгоритму встраивания данных в изображение

При использовании стегоконтейнера в виде текстуры в компьютерной сцене, учитывают требования к выбору метода, отличающиеся от тех, которые обычно применяются. Наиболее важные факторы:

Изменение освещения – яркость и цвета текстуры могут быть искажены в зависимости от источников света, используемых в сцене. Необходима достаточная устойчивость к манипуляциям с изображением.

Формат изображения – большой несжатый файл может привлечь внимание при отправке изображений через Интернет. Следует использовать форматы со сжатием с потерями для уменьшения размера файла, такие как JPEG.

Изменение геометрии – даже если текстура отображается на плоской поверхности, которая не находится непосредственно перед наблюдателем или камерой, могут произойти некоторые изменения в геометрии из-за используемой 3D-проекции. Если условия не

¹⁷⁹ Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lebedevan@bmstu.ru

¹⁸⁰ Николаенкова Екатерина Константиновна, студент МГТУ им. Н.Э.Баумана, Москва.
katenikolaenkova@gmail.com

идеальны, перспективная проекция будет манипулировать геометрией текстурного изображения, смещая, поворачивая или наклоняя различные части, основываясь на взаимном положении объекта и камеры [7].

Учитывая данные требования, более стойкими к разнообразным искажениям являются методы, использующие частотную область контейнера. Метод, предложенный Хсу и Ву, базируется на алгоритме встраивания ЦВЗ в массив коэффициентов ДКП блоков изображения-контейнера. Процесс восстановления изображения полностью симметричен. Метод позволяет сжимать некоторые изображения в 10-15 раз без серьезных потерь. Данный метод имеет недостаток – потеря яркости изображения после встраивания ЦВЗ, но он несущественен, так как сохранить оригинальное разрешение текстуры практически невозможно.

Алгоритм Хсу и Ву и результат его работы

Хсу (Chiou-Ting Hsu) и Ву (Ja-Ling Wu) [8] предложили алгоритм встраивания ЦВЗ в массив коэффициентов ДКП блоков изображения-контейнера.

Изображение C обычно полутонное, имеющее размер $X \times Y$, в качестве ЦВЗ используется двоичное изображение W размера $A \times Z$. Изображение ЦВЗ создают черно-белым, а перед скрытием заменяют интенсивность белых пикселей (255) на «1», т.к. пиксель в ЦВЗ может принимать значение «0» или «1». При скрытии изображения весь массив цифрового водяного знака делят на 255, а при извлечении, наоборот, умножают на 255.

Поскольку во время встраивания ЦВЗ будет обрабатываться только среднечастотный диапазон исходного изображения, то размер ЦВЗ должен быть меньше, чем размер контейнера. Для контейнера, разбитого на блоки 8×8 , при встраивании ЦВЗ лучше всего использовать $64 \times \frac{A \times Z}{X \times Y}$ коэффициентов ДКП. Отношение $\frac{A \times Z}{X \times Y}$ определяет количество информации, встроенной в выбранное в качестве контейнера изображение. На практике это количество встроенной информации пытаются уменьшить, т.к. это приведет к большей стойкости.

Представим изображение-контейнер C (формула 1) и ЦВЗ W (формула 2) в виде:

$$C = \{c(i, j)\}, \quad 0 \leq x < X, \quad 0 \leq y < Y, \quad (1)$$

где $c(x, y) \in \{0, \dots, 2^L - 1\}$ – интенсивность пикселя (x, y) , а L – количество бит, используемых для квантования интенсивностей в каждом пикселе;

$$W = \{w(a, z)\}, \quad 0 \leq a < A, \quad 0 \leq z < Z, \quad (2)$$

где $w(a, z) \in \{0, 1\}$ – двоичное значение пикселя (a, z) ЦВЗ.

Изображение - контейнер C можно разбить на $\frac{X}{8} \times \frac{Y}{8}$ блоков размерностью 8×8 . Для того, чтобы получить столько же блоков, необходимо разбить ЦВЗ на блоки размерностью $\frac{8 \times A}{X} \times \frac{8 \times Z}{Y}$.

Для создания изображения-контейнера или цифрового водяного знака необходимой размерности к ним могут быть добавлены дополнительные столбцы или строки [9].

Результат программной реализации встраивания и извлечения данных представлен на рисунке 1.



Рис.1. Встраиваемый ЦВЗ (а), исходное изображение (б), Полученное изображение-контейнер (в)

Анализ результатов работы и выводы:

1. ЦВЗ детектировался при любых оригиналах и ЦВЗ.
2. Чистый оригинал и оригинал с ЦВЗ визуально отличаются. Картинка с ЦВЗ в большинстве случаев теряет яркость.
3. Соотношение черных и белых пикселей в ЦВЗ, не играет особой роли. Данный метод позволяет всегда детектировать встроенное ЦВЗ, но ощутимо изменяет яркость оригинала.

Применение стеганографического метода в компьютерной графике

Наложение текстуры – метод, который создает видимость детализации и вводит в заблуждение путем отображения изображения, обычно содержащего информацию о цвете, на 3D-объект [10]. Это отображение цветов, в настоящее время в основном известное как диффузное отображение, берет растровое изображение и применяет его к поверхности фигуры или многоугольника. Впервые он был введен Эдвином Эрлом Кэтмаллом в его докторскую диссертацию в 1974 году [11], и его можно увидеть на рисунке 2.

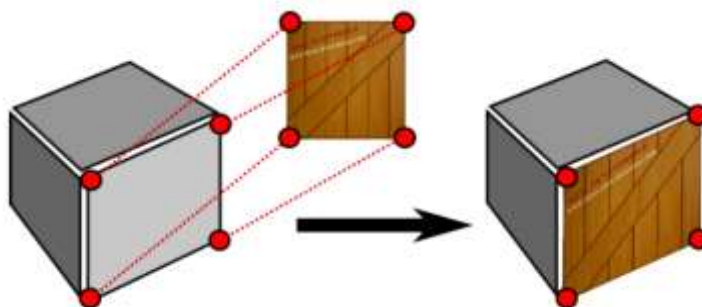


Рис.2. Иллюстрация того, как координаты стеготекстуры могут быть сопоставлены с координатами переднего многоугольника в кубе.

Возможно несколько вариантов получения зашифрованного изображения.

Первый способ представляет собой внутреннее кодирование и декодирование сообщения. Это означает, что текстура с сообщением сначала была закодирована, а затем применена к объекту. Позднее к трехмерному объекту снова будет получен доступ принимающей стороной, используя тот же Unity или сторонние программы по извлечению 3D-объектов из игры. Затем к полученной стеготекстуре применяется алгоритм декодирования.

Второй вариант использования, заключается в том, что принимающая сторона делает снимок экрана с текстурным объектом. Далее полученное изображение должно быть обрезано, т.е. содержать только текстурную сторону куба. Это можно

сделать вручную с помощью простого редактора изображений. Затем происходит декодирование изображения со скрытым сообщением.

Для того, чтобы это надежно сработало, пользователь должен иметь возможность свободно перемещаться по сцене. Видеоигры обычно предоставляют такую возможность, поэтому наиболее подходящим был выбран игровой движок Unity. В Unity была создана простая сцена, содержащая текстурированный куб, направленный источник света и камеру, направленную прямо на куб [12]. Сцена показана на рисунке 3.



Рис. 3. Сцена, используемая для оценки алгоритмов стеганографии в 3D-обстановке.

Источник света был настроен на нейтрально-белый цвет и расположен таким образом, чтобы он освещал объект из-за камеры. Это было сделано для того, чтобы максимально уменьшить негативное влияние 3D-рендеринга, описанного выше в требованиях к алгоритму, на результирующую стеготекстуру.

Выводы

Видеоигры, с их популярностью, простыми каналами распространения и требованиями к данным с высокой плотностью, являются оптимальной средой для передачи информации с использованием стеганографических методов. В работе был показан метод для сокрытия информации с использованием трехмерных игровых карт. Для встраивания данных применялся алгоритм Хсу и Ву. Данный метод позволит избежать значительных искажений, а использование сжатия повысит укрывистость стегообъектов. Также безопасность была достигнута с помощью особенности алгоритма – декодеру ЦВЗ требуется исходное изображение, извлечь данные без него практически невозможно. В настоящее время размер компьютерных игр на диске может достигать нескольких десятков гигабайт. Создание многочисленных 3D-моделей позволит обеспечить достаточно места для скрытого хранения и передачи больших объемов данных, а также сделает стегоанализы намного сложнее.

Литература

1. Макаренко С. И. Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии // Вопросы кибербезопасности. -2014. -№ 2(3). -С. 24-32.
2. Ryutarou Ohbuchi, Hiroshi Masuda, and Masaki Aono, "Embedding data in 3D models," in Interactive Distributed Multimedia Systems and Telecommunication Services . Springer, 1997, pp. 1–10.
3. Francis Cayre and Benoît Macq, "Data hiding on 3-D triangle meshes," IEEE Transactions on Signal Processing , vol. 51, no. 4, pp. 939–949, 2003.
4. Jae-Won Cho, R my Prost, and Ho-Youl Jung, "An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms," IEEE Transactions on Signal Processing , vol. 55, no. 1, pp. 142–155, 2007.
5. Ming Luo and Adrian G Bors, "Surface-preserving robust watermarking of 3-D shapes," IEEE Transactions on Image Processing , vol. 20, no. 10, pp. 2813–2826, 2011.
6. Adrian G Bors and Ming Luo, "Optimized 3D watermarking for minimal surface distortion," IEEE Transactions on Image Processing , vol. 22, no. 5, pp. 1822–1835, 2013.
7. MUSSIO, Luigi; FORLANI, Gianfranco; CROSILLA, Fabio. Data acquisition and analysis for multimedia GIS. 1st ed. Springer. ISBN 978- 3-211-82806-9.
8. Hsu C.-T., Wu J.-L., DCT-based Watermarking for Video, IEEE Transactions on Consumer Electronics, Vol. 44, No.1, Feb 1998, P. 206-216.
9. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: «МК-Пресс», 2006. — 288 с.
10. HECKBERT, Paul S. Survey of texture mapping. IEEE computer graphics and applications. 1986, vol. 6, no. 11, pp. 56–67.
11. CATMULL, Edwin. A subdivision algorithm for computer display of curved surfaces. 1974. Technical report. DTIC Document.
12. Richard Gono, "Steganography in computer graphics," Master's Thesis, Masaryk University Faculty of Informatics, Brno, Spring 2017, pp. 27-31.

Научный руководитель: Лебедев Анатолий Николаевич, кандидат физико-математических наук, доцент МГТУ им. Н. Э. Баумана, lebedevan@bmstu.ru.

Research of steganographic methods of information storage in textures of 3D-objects

Lebedev A.N.¹⁸¹, Nikolaenkova E.¹⁸²

Abstract. *With the expansion of the use of computer networks, one of the most important tasks is to ensure the confidentiality and security of transmitted information. Steganography is used to securely transmit data to the destination without unwanted disclosure or damage. Video games are an extremely popular, widespread example of transferring large amounts of data between remote users, making them attractive for steganography. Today, however, steganography in video games is a virtually unexplored topic. 3D steganography is used to embed or hide information in 3D objects without causing visible or detectable changes. The paper presents a method by which information can be hidden in a three-dimensional map of a video game.*

Keywords: *steganography, texture mapping, Hsu and Wu's approach, digital watermark, computer graphics*

¹⁸¹ Anatoly Lebedev, PhD, Bauman Moscow State Technical University, Moscow, lebedevan@bmstu.ru

¹⁸² Ekaterina Nikolaenkova, student, Bauman Moscow State Technical University, Moscow, katenikolaenkova@gmail.com

Разработка способа практической реализации технологии применения электронной подписи в рамках предприятия

Литвиненко Д.И.¹⁸³

Аннотация: Электронная подпись (ЭП) является по закону полноценной заменой рукописной подписи. Технология электронной подписи способна обеспечить высокую скорость обработки и подписания электронного документа, а также обезопасить его от возможной фальсификации. В данной статье рассматриваются общие и специальные требования для внедрения разрабатываемого программного модуля ЭП в стороннюю систему. Представлен выбор алгоритмов хэширования, формирования и проверки электронной подписи. А также выбор программных решений и технологий для разработки модуля. При этом внимание прежде всего уделяется безопасности, быстрдействию, экономической выгоде и удобству внедрения модуля ЭП в систему.

Ключевые слова: документооборот, целостность, идентификация, безопасность, хэширование, асимметричное шифрование.

Введение

В настоящее время одной из актуальных проблем в мире является проблема информационной безопасности. Это объясняется тем, что информационные технологии коренным образом изменили нашу жизнь. Большая часть оборота информации и документов теперь осуществляется в электронном виде. Это позволяет значительно сократить время, затрачиваемое на обмен документацией, усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов [1]. Поэтому важной пунктом в согласовании документов является электронная подпись.

Требования к разработке модуля

Идеей данной работы является разработка модуля для подписи «Карт испытаний электронной компонентной базы». Модуль внедряется в уже готовую программу. Человек, проводивший испытания, должен внести результаты и подписать их. После подписи всех испытаний, карта подписывается ответственным за всю работу сотрудником. Далее – данный документ формируется в нужном формате, после чего его можно отправить на печать. Следовательно, помимо общих требований должны быть сформулированы специальные требования, характерные разрабатываемому модулю ЭП. В рамках данной разработки такими требованиями являются:

не отрицание авторства – невозможность автора отказаться от подписи. Включает в себя также однозначную идентификацию пользователя (никто не может представиться другим лицом, никто не может подделать подпись);

обеспечение целостности – после подписания документа нет возможности исправить подписанный данные, при этом сохранив подпись. Все изменения в документе необходимо заново подписывать;

обеспечение доступности – при подписи любого испытания, все остальные испытания доступны для редактирования. Так же есть возможность поставить две и более за различные испытания;

требования по обеспечению высокой скорости обработки и подписания электронного документа – разрабатываемый модуль не должен иметь неоправданно сложную структуру, которая будет влиять на скорость обработки данных. Так как на сегодняшний день существуют готовые программные решения, отвечающие требованиям быстрдействия [2];

¹⁸³ Литвиненко Дарья Игоревна, студент МГТУ им. Н.Э. Баумана, Москва, Litvinenko10.10@mail.ru

требования, связанные с возможностью последующей доработки – это необходимо для возможности использования данного модуля как отдельного приложения или внедрения модуля в другие приложения. В отдельных случаях, может понадобится изменение алгоритмов хэширования информации, алгоритмов шифрования, процедуры хранения ключей подписи и тд;

экономические требования необходимо минимизировать затраты на внедрение, использование и поддержку процедуры ЭП.

Выбор алгоритмов хэширования и алгоритмов формирования и проверки ЭП.

При подписании документа, а также проверки ЭП одной из основных процедур является процедура хэширования. Данная операция необходима для осуществления безопасности информации, хранящейся в документе, от изменений в случае умышленных действий пользователей или случайных изменений. На основе подсчета хэш-суммы используется механизм контроля целостности. Данный механизм может обеспечивать целостность данных путем подсчета эталонной контрольной суммы и последующего сравнения эталонных контрольных сумм с контрольными суммами, полученными при проверке ЭП. Существует множество алгоритмов для вычисления контрольных сумм. Среди них множество зарубежных (например, MD5, SHA512). Однако, существует и отечественный алгоритм вычисления контрольной суммы –ГОСТ Р 34.11-2012. Данный ГОСТ обеспечивает повышенную криптографическую стойкость и является действующим российским криптографическим стандартом, который определяет процедуру вычисления хэш-функции. В основу стандарта 2012 года была положена функция хеширования под названием «Стрибог». Данное хэширование содержит в себе функцию сжатия (g-функция), построенную на блочном шифре с помощью конструкции Миягучи – Пренеля, признанной одной из наиболее стойких [3].

Второй из главных процедур является процедура шифрования и дешифрования данных. В основе формирования и проверки ЭП применяется асимметричное шифрование. Существует множество видов асимметричных шифров, например, RSA, Elgamal и др. Существует также отечественный алгоритм ГОСТ Р 34.10-2012. На сегодняшний день он является действующим отечественным стандартом, который содержит описание процессов формирования и проверки электронной цифровой подписи (ЭЦП), реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем [4]. Для определения параметров и идентификаторов эллиптических кривых для случая эллиптических кривых в канонической форме с простыми модулями длины 512 бит можно воспользоваться рекомендацией Технического комитета по стандартизации «Параметры эллиптических кривых для криптографических алгоритмов и протоколов» [5].

Выбор программных решений и технологий для разработки

Важным этапом в разработке является выбор программных решений и технологий, на основе которых будет строиться данная разработка.

Необходимо выбрать:

язык программирования. Желательна реализация объектно-ориентированной модели, так как это удобно для проектирования и дальнейшей поддержки приложения. Полезным будет наличие библиотек, содержащих готовые средства шифрования и ЭП. А также иметь возможность создания пользовательского интерфейса;

базу данных. Среди множества существующих СУБД, реализующих различную степень функционала, отличающихся подходами реализации, скоростью ввода-вывода и обработки данных, степенью изолированности, необходимо выбрать конкретный продукт. Это должно быть целесообразное решение, способное обеспечить выполнение всех требований [6];

аппаратное средство для хранения ключей ЭП.

Вывод

Исходя из вышесказанного, можно сделать вывод, что разрабатываемый модуль ЭП будет востребован не только в рамках отдела, но и на рынке программного обеспечения. Данная разработка повысит производительность труда сотрудников, проводивших испытания, а также их руководителей.

Целью дальнейших исследований будет практическая разработка и испытание программного модуля ЭП. Особое влияние будет уделено вопросам безопасности функционирования модуля при работе этого модуля в недоверенной операционной среде.

Литература

1. Волошин И.П. Электронная цифровая подпись / Е. З. Герчикова, И. П. Волошин // Рабочая программа дисциплины. – Саратов: «Российский экономический университет имени Г.В. Плеханова» Саратовский социально-экономический институт (филиал), 2014, – 22 с.

2. Зеленкина В.С., Тихомиров В.А., Разработка методики и внедрения процедуры электронной подписи комплекта документации технологического процесса // Научно-техническое творчество аспирантов и студентов – Комсомольский-на-Амуре государственный технических университет, 2018. С. 168-170.

3. Лавриков И.В, Маршалко Г.Б., Рудской В.И., Смышляев С.В., Шишкин В.А. Обзор результатов анализа хэш-функций ГОСТ Р 34.11-2012 // Проблемы ИБ. Компьютерные сети – Санкт-Петербургский политехнический университет Петра Великого, 2015. С. 147-153.

4. Акилов А.А, Диченко С. А., Жарких А.А Анализ построения электронно цифровой подписи по ГОСТ Р 34.10-2012 // Прикладные информационные системы и программное обеспечение – К: Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, 2018. С. 22-61.

5. ГОСТ 34.11—2012 Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов.— М., 2016. — 11 с.

6. Городничев М.Г., Шалаумов Э.В. Разработка модуля цифровой подписи для последующего внедрения в систему электронного документооборота // Технологии информационного общества – М.: Издательство дом Седиа паблишер. 2019. С. 490-492.

Научный руководитель: **Лебедев А.Н.** ¹⁸⁴

Enterprise-wide implementation of a digital (electronic) signature technology

Litvinenko D.I. ¹⁸⁵

Abstract: *Electronic signature (EP) is by law a complete replacement of handwritten signature. This article discusses the General and special requirements for the implementation of the developed software module EP in a third-party system. The choice of algorithms for hashing, formation and verification of electronic signatures is presented. At the same time, attention is primarily paid to the safety, speed, economic benefits and convenience of implementing the EP module into the system.*

Keywords: *document flow, integrity, identification, security, hashing, asymmetric encryption.*

Principal investigator: **Lebedev A.N.** ¹⁸⁶

¹⁸⁴ Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lebedevan@bmstu.ru

¹⁸⁵ Daria Litvinenko, student of Bauman Moscow State Technical University, Moscow, Litvinenko10.10@mail.ru

¹⁸⁶ Anatoly Lebedev, PhD, Bauman Moscow State Technical University, Moscow, lebedevan@bmstu.ru

Защищенная переработка визуальной информации в автоматизированной оптико-электронной системе наземно-космического мониторинга

Ловцов Д.А.¹⁸⁷, Гаврилов Д.А.¹⁸⁸, Макаренко Г.И.¹⁸⁹

Аннотация. Рассматриваются основные подходы к построению автоматизированной оптико-электронной системы наземно-космического мониторинга, обеспечивающей защищенную переработку визуальной информации в условиях информационного соперничества. Результаты имеют теоретическое и практическое значение при решении задач обеспечения информационной эффективности в различных сферах деятельности, требующих переработки визуальной информации.

Ключевые слова: защищенная переработка привилегированной визуальной информации, эффективность, точность, информационное соперничество

Введение

Глобальная информатизация и информационное соперничество обуславливают актуальность разработки рациональной методологии построения эффективных автоматизированных оптико-электронных систем наземно-космического назначения (АОЭС НКМ), характеризующихся высокими значениями показателей точности, оперативности, надежности, устойчивости, живучести, а также высокой степенью информационной защищенности для обеспечения функционирования в условиях агрессивной информационной среды. Одной из проблем в области автоматизированной обработки изображений является обеспечение высокой точности решения конкретных поставленных задач, устойчивых к различным оказывающим негативное влияние агрессивным факторам, с четко обозначенным и исследованным диапазоном применимости.

Построение эффективной АОЭС представляется возможным на основе применения проблемно-ориентированного варианта комплексного «ИКСД»-подхода («информационно-кибернетически-синергетически-дидактического») [1], т.е. системного подхода с акцентированием внимания на его информационном, кибернетическом, синергетическом и дидактическом аспектах, состоящего в интеграции методологии информационного подхода (при котором объект рассматривается как целенаправленная информационная система), методологии кибернетического подхода (при котором объект рассматривается как система управления на уровне информационных процессов и алгоритмов функционирования информационной базы) с методологией синергетического подхода (при котором объект рассматривается как динамическая самоорганизующаяся система, взаимодействующая со средой) и методологией дидактического подхода (при котором объект рассматривается как система способная к самообучению) в составе

¹⁸⁷ Ловцов Дмитрий Анатольевич, заслуженный деятель науки РФ, доктор технических наук, профессор, ОАО «Институт точной механики и вычислительной техники им. С.А. Лебедева РАН», г. Москва, e-mail: dal-1206@mail.ru

¹⁸⁸ Гаврилов Дмитрий Александрович, кандидат технических наук, ОАО «Институт точной механики и вычислительной техники им. С.А. Лебедева РАН», г. Москва, e-mail: gavriloov.da@mipt.ru

¹⁸⁹ Макаренко Григорий Иванович, старший научный сотрудник, ФБУ НППЦИ при Министерстве юстиции РФ, г. Москва, e-mail: intell2019@ya.com

методологии системного подхода (при котором объект рассматривается как сложноорганизованная многоуровневая и многоаспектная система).

Концептуально-логическая модель и основные задачи АОЭС НКМ

В качестве концептуально-логической модели АОЭС НКМ можно использовать известную инвариантную функциональную структуру (рис. 1) [1,2], представленную в виде комплекса функциональных подсистем: измерения (P_1), наблюдения (P_2), идентификации (P_3), выработки управленческих решений (P_4), централизованной координации (P_5), информационного обмена (P_6), а также информационной защиты (P_7), необходимой при функционировании в условиях информационного соперничества и обеспечивающей необходимую защищенность переработки информации. На объект управления (P_0) в момент времени t поступают различные входные воздействия: функциональные $R(t)$, внешние целевые $X(t)$ и внешние координирующие $X'(t)$, на которые формируются соответствующие отклики $Q(t)$, $Y(t)$, $Y'(t)$.

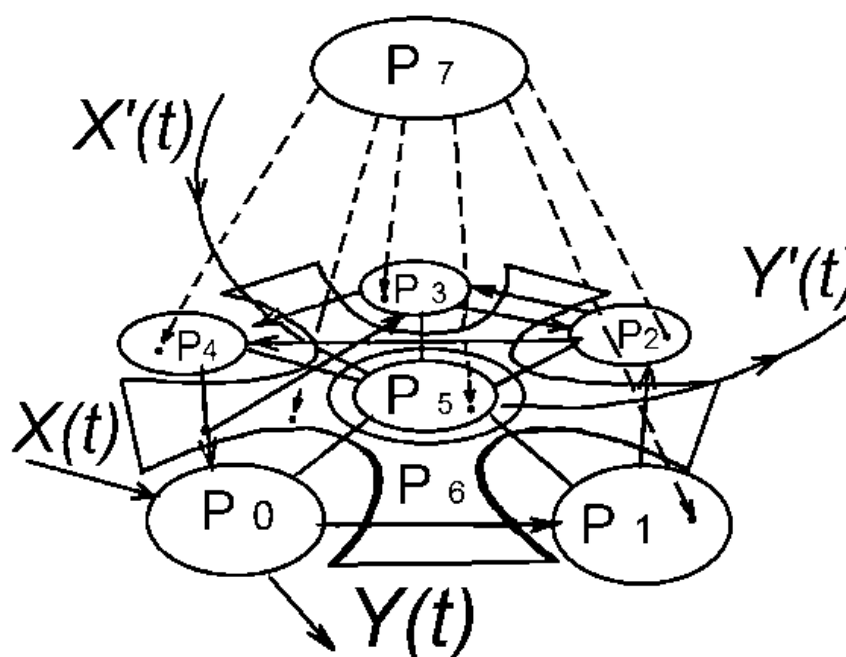


Рис. 1. Концептуально-логическая модель АОЭС НКМ

Основные задачи АОЭС НКМ – стабилизация, детектирование, локализация и классификация объектов интереса на фото- и видеоданных применительно к различным фоно-целевым обстановкам. Трудности при решении данных задач возникают вследствие: потери информации при проецировании трехмерной сцены (экспозиции) на плоскость изображения, наличия шума на изображении, изменения экспозиции сцены, сложной формы объектов, изменения формы объекта, частичных или полных перекрытий и загораживаний объектов сцены, сложной траектории движения объекта, выхода объекта за пределы кадра и появления объекта в кадре, относительного движения камеры, требований обработки в реальном времени и др. [2,3]. Задачи АОЭС НКМ распределяются по функциональным подсистемам следующим образом: обеспечение стабилизации видеоизображений – подсистема P_1 [4]; детектирование, локализация и сопровождение – P_2 [5]; классификация и селекция – P_3 [6,7]; формирование управляющих воздействий – P_4 ;

построение обучающих выборок и настройка системных методов – P_5 [8]; сжатие динамического диапазона и передача сигналов [9]– P_6 ; криптопреобразование сигналов – P_7 .

Реорганизация и отображение многоуровневой АОЭС НКМ на концептуально-логической модели

Схема реорганизации и отображение многоуровневой АОЭС НКМ на концептуально-логической модели представлена на рис. 2.

Уровни реорганизации характеризуются следующим образом:

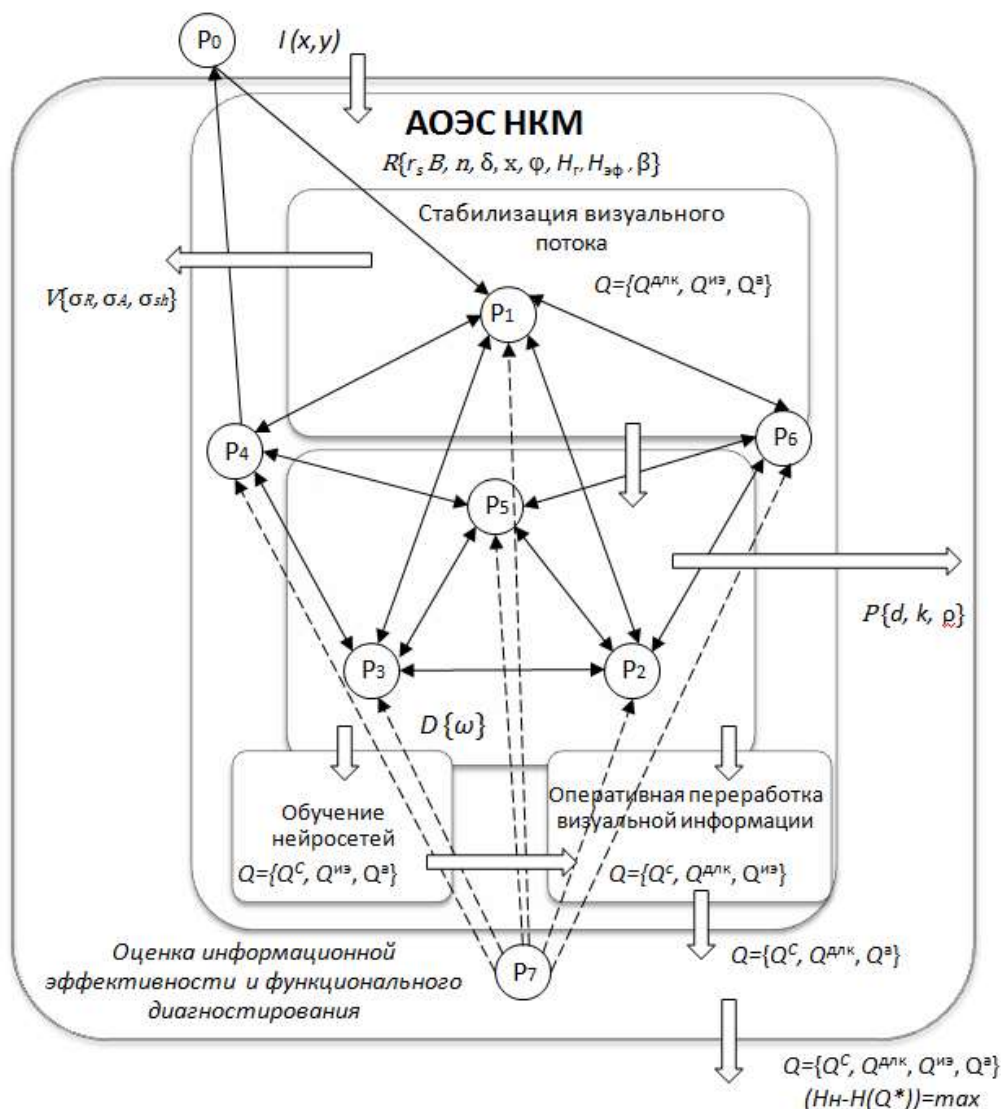


Рис. 2. Схема реорганизации и отображение многоуровневой АОЭС НКМ на концептуально-логической модели

Уровень 1. Выбор способа $t \in M$ действий (метода) из множества M возможных способов по алгоритму A .

$A: t \in M$.

Основными подсистемами, функционирующими на данном уровне, являются подсистема измерения (P_1) и подсистема координации (P_5).

Уровень 2. Адаптация и модификация методов для решения задач в условиях информационного соперничества. В результате обучения в реальных условиях и сужения

множества неопределенности H формируется эффективный алгоритм A выбора способа действия.

$$H \rightarrow 0, A = F\{G, K\}.$$

Основной подсистемой, функционирующей на данном уровне, является *подсистема информационного обмена* (P_6).

Уровень 3. Самоорганизация, выбор стратегической модели осуществляется на основе обоснования и задания текущих операторов G выходов, K оценки качества способа действия, соответствующих главной цели $S(t)$. Оператор выходов G определяет правило отображения множества X элементов на входе в множество Y результатов на выходе при данном $t \in M$ способе действий, выбранном из множества M в условиях неопределенности H .

$$G: X \times M \times H \rightarrow Y.$$

Оператор K оценки качества способа действий определяет правило отображения множества Y результатов на выходе при данном $t \in M$ способе действий, выбранном из множества M , в множество величин R , связанное с характеристиками качества работы системы

$$K: M \times Y \rightarrow R.$$

Основными подсистемами, функционирующими на данном уровне, являются *подсистема наблюдения* (P_2) и *подсистема идентификации* (P_3).

Уровень 4. Административное управление, принятие решений на основе полученной аналитической информации. Основной подсистемой, функционирующей на данном уровне, является *подсистема принятия решений* (P_4).

При этом требуемая степень защищенности и безопасности информационных массивов поддерживается подсистемой информационной защиты (P_7) непрерывно на всех уровнях. Информационная безопасность включает обеспечение достоверности (помехоустойчивость и помехозащищенность), конфиденциальности (скрытность, доступность и имитостойкость), сохранности (целостность, готовность) привилегированной визуальной информации. Таким образом, защищенность информации заключается в способности не допускать случайного или целенаправленного искажения или разрушения, раскрытия или модификации информационных массивов в информационной базе [10].

Обеспечение информационной эффективности и безопасности АОЭС НКМ в условиях информационного соперничества

Одним из главных требований разработки эффективной АОЭС НКМ является обеспечение качества переработки содержательной визуальной информации, поступающей на вход системы в виде информационного потока.

Качество переработки информации может быть охарактеризовано совокупностью свойств, определяющих степень ее соответствия целям переработки. В общем случае можно выделить внутренние показатели качества, характеризующие содержательность системы и внешние показатели качества, определяющие защищенность системы. Внутренние показатели качества отвечают за такие свойства переработки информации как существенность – свойство информации, позволяющее сохранять ценность с течением времени, и включающее показатели полноты, обеспечивающие рациональность управления, и релевантности, отвечающие за соответствие динамическому состоянию объектов, а также кумулятивность – свойство, позволяющее отражать действительность в небольшом информационном массиве, и включающее показатели избирательности, обеспечивающие квалификационный выбор ограниченного количества информационных единиц из информационного массива большого объема, и гомоморфизма, позволяющие

агрегировать крупные информационные массивы в малое число информационных единиц [11].

Внешние показатели качества обеспечивают свойства конфиденциальности достоверности и сохранности информации. Свойство конфиденциальности определяет статус внешней доступности информации и характеризуется показателями доступности (определяющим степень разграничения в использовании информационных массивов), скрытности (закключающемся способностью противостоять раскрытию смысла информации), имитоскойкости, (определяющим степень защиты информации от внедрения и заключающемся в способности не допустить попадания в систему дезинформации). Свойство достоверности характеризует степень соответствия реальных информационных единиц их истинному значению и определяется параметрами помехоустойчивости и помехозащищенности. Свойство сохранности заключается в возможности целевого применения визуальных информационных массивов и способности не допускать нарушения целостности информационных массивов в процессе эксплуатации систем.

Процесс переработки визуальной информации охватывает широкий спектр методов, имеющих различное применение. Из множества методов выделяется определенный их набор с целью построения алгоритмов для решения конкретных поставленных задач [12, 13, 14].

В общем случае технологический процесс переработки визуального информационного потока представляет собой совокупность последовательных действий, направленных на анализ информации и приведение ее на выходе системы к требуемому виду. В технологическом процессе переработки входного информационного потока можно выделить следующие три основные технологические операции. *Во-первых*, рецепция, включающая процессы формирования и регистрации изображений, а также предварительное сжатие и восстановление. *Во-вторых*, интерпретация, в результате которой осуществляется интеллектуальная обработка, обобщение полученных данных, контроль и принятие решений. *В-третьих*, операция коммуникации, отвечающая за прием и передачу информационного потока. При этом в целях обеспечения безопасности на операцию коммуникации передается не общий массив визуальных данных, а уже частично переработанная визуальная информация, содержащая определенные данные необходимые для обеспечения дальнейшего восстановления полной значимости. Например, в случае использования нейросетевых методов дешифрирования визуальной информации обеспечивается формирование обучающих выборок, а для дальнейшей работы по информационному каналу передаются не массивы обучающих изображений, а веса нейросети, полученные в процессе обучения [15,16].

При построении эффективной АОЭС НКМ важнейшей задачей является определение качественных показателей информационной безопасности (рис. 3).

Основными характеристиками, влияющими на эффективность и безопасность АОЭС НКМ, являются показатели информационной точности K_T , оперативности K_{on} , добротности K_D , устойчивости $K_{уст}$, живучести $K_{жив}$, каждому из которых соответствует определенный показатель значимости $0 \leq \lambda_i \leq 1$, $\sum \lambda_i = 1, i = 1, \dots, 5$. Основными качествами данных характеристик является максимальное использование потенциальных возможностей АОЭС НКМ. Информационная безопасность АОЭС НКМ определяется как функция частных показателей эффективности

$$K_{эф} = \sum \lambda_i f(K_T, K_{on}, K_D, K_{уст}, K_{жив}) \Rightarrow \max.$$



Рис. 3. Обеспечение эффективности АОЭС НКМ в условиях информационного соперничества

Выводы

Представлены основные подходы к обеспечению защищенной переработки визуальной информации в условиях информационного соперничества в автоматизированной оптико-электронной системе наземно-космического мониторинга.

Рассмотренные предложения по обеспечению защищенной переработки информации в АОЭС НКМ представляют теоретико-прикладную значимость при решении задач разработки эффективных автоматизированных оптико-электронных систем специального (межотраслевого и др.) назначения, обеспечивающих переработку многоаспектной визуальной информации, и позволяют значительно повысить эффективность использования имеющихся методов и средств *детектирования, локализации и классификации* изображений и, как следствие, улучшить качество распознавания визуальной информации, обеспечить конфиденциальность переработки информации, а также повысить сохранность и достоверность оценки ситуаций в условиях интенсивного информационного соперничества и непрерывно меняющейся обстановки.

Литература

1. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна // Вопросы кибербезопасности. – 2018. – №4(28). – С. 9-20, DOI: 10.21681/2311-3456-2018-4-9-20.
2. Козачок А.В. Спецификация модели управления доступом к разнотипным ресурсам компьютерных систем // Вопросы кибербезопасности. – 2018. – №4(28) – С. 2-8, DOI: 10.21681/2311-3456-2018-4-2-8.
3. Деундяк В.М., Могилевская Н.С. Стойкость полиномиальной схемы разделенной передачи конфиденциальных данных // Вопросы кибербезопасности. – 2018. – №4(28). – С. 38–45. DOI: 10.21681/2311-3456-2018-4-38-45

4. Maximov R.V., Krupenin A.V., Sharifullin S.R., Sokolovsky S.P. Innovative development of tools and technologies to ensure the russian information security and core protective guidelines // Вопросы кибербезопасности. –2019. – №1(29). – С.10-17, DOI: 10.21681/2311-3456-2019-1-10-17.
5. Гаврилов, Д.А., Местецкий, Л.М., Семенов А.Б. Метод разметки изображений самолетов на аэрокосмических снимках на основе непрерывных морфологических моделей // Программирование. –2019. – № 6. –С.3-12, DOI: 10.1134/S0132347419060025
6. Скобцов В.Ю., Кругликов С.В., Ким Д.С., Новоселова Н.А., Архипов В.И., Кульбак Л.И., Николаева Е.Д., Лапицкая Н.В., Вакульчик Е.Н., Саксонов Р.В. Анализ показателей надежности, живучести и телеметрии бортовой аппаратуры малых космических аппаратов // Вопросы кибербезопасности. 2018. –№4(28) –С.54-69, DOI: 10.21681/2311-3456-2018-4-54-69.
7. Gavrillov D.A. Quality assessment of objects detection and localization in a video stream // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. – 2019. –Т. 2. – С. 40–55.
8. Gavrillov D.A. et al. Use of Neural Network Based Deep Learning Techniques for the Diagnostics of Skin Diseases // Biomed. Eng. (NY). – 2019. – т. 52, –№ 5. –с. 348–352.
9. Гаврилов Д.А. Павлов А.В., Щелкунов Д.Н. Аппаратная реализация сжатия динамического диапазона цифровых изображений на ПЛИС Xilinx // Журнал радиоэлектроники. –2018. –№ 10. – DOI 10.30898/1684-1719.2018.10.6, <http://jre.cplire.ru/jre/oct18/6/text.pdf>.
10. Гаврилов Д.А., Павлов А.В. Поточная аппаратная реализация алгоритма SURF // Известия ВУЗов. Электроника. –2018. –Т. 23. – № 5. – С.502-511, DOI: 10.24151/1561-5405-2018-23-5-502-511.
11. Гаврилов Д.А., Ивкин А.В., Щелкунов Н.Н. Система тестирования алгоритмов стабилизации видеоизображений, функционирующих в режиме реального времени// Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. –2018. –№ 4. – С. 112–126, DOI: 10.18698/0236-3933-2018-4-112-126.
12. Пунь А.Б., Гаврилов Д.А., Щелкунов Н.Н., Фортунатов А.А. Алгоритм адаптивной бинаризации объектов в видеопоследовательности в режиме реального времени // Успехи современной радиоэлектроники. – 2018. –№ 9. – С. 40–48, DOI 10.18127/j20700784-201809-05.
13. Гаврилов Д.А., Мелерзанов А.В., Асадов А.Е., Жаров В.П. Вторичная профилактика и контроль терапии меланомы с использованием телемедицинских технологий и стандартизированной обработки данных // Проблемы стандартизации в здравоохранении. –2018. – № 7–8. –С. 45–54 DOI.org/10.26347/1607-2502201807-08045-054.
14. Lovtsov D. A., Loban A. V. An Effective New Technology for the Distributed Processing of Measurement Data by S/C Automated Control System// Solar System Research, –2015, –Vol. 49, –No. 7, pp. 614–620, DOI: 10.1134/S0038094615070151.
15. Lovtsov D. A., Karpov D. S. Dynamic Planning of Navigation Determinations of Airspace and Missile Objects in an Automated Flight Test Control System // Solar System Research, 2011, Vol. 45, No. 7, pp. 645–651, DOI: 10.1134/S003809461107015X/
16. Ловцов Д.А. Развитие информационной сферы общественно-производственной деятельности: достижения, угрозы безопасности и правовое регулирование // Государство и право в новой информационной реальности. –2018. –№1. DOI: 10.31249/pras/2018.01.01

Автоматизированное средство статической инструментации исполняемого кода встроенного программного обеспечения

Малахов М.В.¹⁹⁰, Алексеев К.А.¹⁹¹

***Аннотация.** На сегодняшний день все большую актуальность приобретает задача поиска уязвимостей и недеklarированных возможностей в программном обеспечении различных устройств. При решении данной задачи широко применяются методы динамического анализа, одним из важных этапов которого является процедура сбора трассировочной информации. В работе обосновывается выбор инструментации кода, как метода сбора трассировочных сведений при проведении динамического анализа встроенного программного обеспечения. Кратко приводится описание данной технологии. Выдвигаются основные требования к средству инструментации исполняемого кода различных микроконтроллерных архитектур. Предлагается возможный подход к построению такого средства. Описываются особенности средства, разработанного в соответствии с предложенным подходом, а также проводится его исследование на предмет удовлетворения выдвинутым требованиям.*

Ключевые слова: информационная безопасность, поиск уязвимостей, динамический анализ, программное обеспечение для анализа кода микроконтроллеров.

Введение

В настоящий момент времени с развитием вычислительной техники и проникновением всевозможных электронных устройств в различные сферы жизни человека всё большую актуальность приобретает задача поиска уязвимостей и недеklarированных возможностей (НДВ) во встроенном программном обеспечении (ВПО). Актуальность данной задачи косвенным образом подтверждается тем, что в последние годы было принято несколько документов, регламентирующих процесс разработки безопасного программного обеспечения [1] и процесс поиска в нём уязвимостей и НДВ [2].

Одной из важных составляющих методики ФСТЭК по выявлению уязвимостей и НДВ является процедура динамического анализа [2], который осуществляется путём отслеживания состояний программы при подаче ей специально сгенерированных входных данных. Однако отслеживание состояний встроенного программного обеспечения во время его выполнения (сбор трассировочных сведений) является достаточно сложной задачей, в том числе и из-за разнообразия микроконтроллерных архитектур, ВПО которых необходимо исследовать. В связи с этим часть процедур, связанных с поиском уязвимостей и НДВ в ВПО, не может проводиться в полной мере.

Таким образом, актуальной становится задача разработки средства сбора трассировочной информации во время выполнения ВПО, написанного для различных микроконтроллерных архитектур.

1. Методы сбора трассировочных сведений, используемые при динамическом анализе ВПО

¹⁹⁰ Малахов Михаил Валерьевич, МГТУ им. Н.Э. Баумана, Москва, misha.malaxow@yandex.ru

¹⁹¹ Алексеев Кирилл Анатольевич, МГТУ им. Н.Э. Баумана, Москва, k-alexeewk7@yandex.ru

Существующие на данный момент времени подходы к сбору трассировочных сведений во время выполнения ВПО базируются на применении технологий эмуляции или инструментации кода.

Современные эмуляторы способны полностью имитировать функциональность ядра и периферии микроконтроллеров. Такие эмуляторы позволяют контролировать выполнение каждой инструкции исследуемой программы и отслеживать все обращения к памяти [3]. Однако в ряде случаев эмуляция нецелесообразна или просто невозможна. К таким случаям относятся: необходимость исполнения кода с полностью соответствующей реальному устройству циклограммой выполнения; анализ программного обеспечения, работающего на устройстве со сложной периферией или в связке с другими устройствами; отсутствие исчерпывающей документации на ядро микроконтроллера или его отдельные блоки. Также к недостаткам эмуляторов следует отнести существенное замедление выполнения программного обеспечения, по сравнению с реальным устройством, а также высокую сложность добавления поддержки новой архитектуры и периферии [4].

В описанных случаях целесообразным является применение инструментации кода, представляющей собой частичное изменение программы, при котором она или её часть, которую необходимо исследовать, сохраняет свою функциональность, но также производит дополнительные действия, целью которых является извлечение информации о состоянии программы в ходе её выполнения [5]. Программное обеспечение, подготовленное инструментатором, может работать на реальном устройстве или в связке с другими устройствами, практически не оказывая влияния на его скорость работы, также следует отметить, что процесс создания инструментатора является менее трудоёмким, чем процесс создания эмулятора.

Существующие инструментаторы подразделяются на инструментаторы исходного и исполняемого кода, которые, в свою очередь, бывают статическими, вносят изменение в ВПО до начала его исполнения, и динамическими, меняют код непосредственно во время работы ВПО [6]. Динамическая инструментация осуществляется обычно посредством подключения специальных динамических библиотек или с использованием отладочных интерфейсов. При решении задач по поиску уязвимостей и НДВ в ВПО микроконтроллеров исходный код зачастую недоступен, а отладочные интерфейсы, как правило, закрыты для использования. Все это делает невозможным применение динамической инструментации, равно как и инструментации исходного кода.

Популярные в настоящий момент средства инструментации кода предназначены лишь для работы с наиболее популярными архитектурами, такими как ARM, x86 и x86-64 и не ориентированы на легкую доработку под другие архитектуры [7].

В связи с этим в интересах решения задач по поиску уязвимостей и НДВ в ВПО была выявлена потребность в разработке средства статической инструментации исполняемого кода ВПО, написанного для различных микроконтроллерных архитектур.

1. Основные требования к разрабатываемому средству

В докладе обоснован следующий перечень требований к разрабатываемому средству:

- а) Сохранение работоспособности исследуемого программного обеспечения и добавление функционала трассировки.
- б) Возможность работы в условиях ограниченных размеров памяти кода и данных.

- в) Возможность быстрого добавления новых микроконтроллерных архитектур в средство инструментации.

2. Основные сведения о разработанном средстве

В докладе представлена предложенная авторами методика проведения инструментации кода, основное содержание которой включает следующие действия. На первом этапе необходимо найти свободные области в памяти кода и памяти данных, которые будет использовать инструментатор в ходе своей работы. Далее надо выбрать точки программного обеспечения, в которых будет вызываться инструментирующий код. Инструкции вызова инструментирующего кода будут собой заменять другие инструкции, которые необходимо сохранить и потом исполнить. После вставки инструкций вызова инструментирующего кода в оригинальный бинарный файл, происходит создание инструментирующего кода с учетом потребностей пользователя и добавление в этот код вытесненных инструкций. Последним этапом является компиляция полученного кода и его добавление в бинарный файл.

Код, создаваемый разработанным средством инструментации, состоит из нескольких блоков с различными функциями. Первым блоком является блок восстановления контекста, который необходим для восстановления значений регистров, изменяемых в процессе инструментации. Блок сохранения контекста является первым блоком, на который передаётся управление из основной программы. Он сохраняет текущие значения регистров, изменяемых в ходе инструментации. Блок управляющего кода определяет, адреса перехода на функциональный блок и блок выполнения вытесненных инструкций в зависимости от места вызова инструментирующего кода. Блок функционального кода содержит в себе непосредственно полезный код. Данный код в зависимости от целевого предназначения может выполнять сбор трассы выполнения программы, отслеживание состояния регистров и памяти микроконтроллера; а также пользователь может реализовать функционал по изменению участков кода, например, для исправления ошибок или обхода защитных механизмов. Блок выполнения вытесненных инструкций сначала вызывает блок восстановления контекста, после чего выполняет инструкции, которые были заменены при вставке инструкций перехода на инструментирующий код и передаёт управление основной программе.

Инструментирующий код создаётся посредством автоматической подстановки значений в заранее сгенерированные пользователем шаблоны ассемблерного кода. Причем этот процесс идентичен для различных архитектур. Автоматическое заполнение шаблонов происходит с помощью использования довольно простого языка подстановок. Таким образом, основные особенности архитектуры контроллера учитываются с помощью изменения шаблонов, данная особенность позволяет добавлять новые архитектуры микроконтроллеров, не затрагивая саму логику работы инструментатора.

Важной особенностью инструментатора является возможность добавления поддержки новой микроконтроллерной архитектуры. Этот процесс состоит из четырех основных этапов:

- 3) Создание файла формата json, в котором указываются основные особенности этой архитектуры, такие как команды вызова инструментирующего кода и возврата из него, а также инструкции, вместо которых нельзя вставлять инструкции вызова инструментирующего кода. Обычно это инструкции, меняющие направление графа потока управления или позиционно-зависимые инструкции.

- 4) Создание ассемблерных шаблонов с учетом особенностей процесса их автоматического заполнения.
- 5) Определение регистров общего и специального назначения, изменяемых в процессе работы инструментирующего кода, и проведение корректировки шаблонов сохранения и восстановления контекста.
- 6) Добавление функционала по обработке автоматически генерируемого с помощью шаблонов ассемблерного кода в случае необходимости.

3. Некоторые характеристики разработанного средства инструментации исполняемого кода

Инструментатор реализован в виде плагина к дизассемблеру IDA Pro на языке Python 2.7, выбор данной связки технологий обуславливается тем, что IDA, по мнению авторов, на данный момент времени является самым удобным средством анализа исполняемого кода, а также поддерживает возможность дизассемблирования машинного кода различных микроконтроллерных архитектур [8].

Генерация инструментирующего кода занимает порядка нескольких секунд на среднем аппаратном обеспечении. При этом скорость работы исследуемого ВПО после инструментации замедляется несущественно. Потребляемая в ходе работы инструментатора память в областях кода и данных зависит от написанных шаблонов. В настоящей реализации для контроллеров на базе ядра i8051 для трассировки 4 ячеек памяти в 7 точках инструментации используется порядка 400 байт.

В докладе представлены результаты практической отработки разработанного средства инструментации по автоматизированной вставке в исполняемый код ВПО микроконтроллеров, построенных на архитектурах ARMv6, i8051 и Tricore, трассировочного функционала.

Заключение

Опираясь на все выше сказанное, можно заключить, что разработанный инструментатор отвечает всем выдвинутым требованиям.

Сохранение функционала исходного программного обеспечения гарантируется особенностями передачи управления между блоками инструментирующего кода, процессом его добавления, а также наличием блоков сохранения и восстановления контекста. Функционал по трассировке сосредоточен в создаваемом инструментатором функциональном блоке.

Код шаблонов по умолчанию и компоновка блоков инструментирующего кода оптимизированы, что позволяет вести работу с микроконтроллерами, у которых объемы памяти кода и памяти данных сильно ограничены.

Использование модульной архитектуры и использование объектно-ориентированного программирования позволили абстрагироваться от особенностей конкретной архитектуры при написании кода инструментатора. Это обуславливает относительную простоту и скорость добавления поддержки новых микроконтроллерных архитектур. На данном этапе этот процесс занимает пару дней, причем основная работа сводится к написанию ассемблерных шаблонов.

Направлениями дальнейших, проводимых авторами исследований является доработка существующего инструментатора в области оптимизации его работы, а также разработка

средств динамического анализа ВПО на основе разработанного инструментатора исполняемого кода, в том числе разработка средства, подтверждающего наличие потенциальных уязвимостей и НДВ в исполняемом коде ВПО.

Литература

1. Барабанов А.В. 28 магических мер разработки безопасного программного обеспечения / А.В. Барабанов, А.С. Марков, В.Л. Цирлов // Вопросы кибербезопасности, 2015, № 5 (13), с. 2-10.
2. Сердечный А.Л. Методика выявления уязвимостей и недеklarированных возможностей в программном обеспечении / А.Л. Сердечный // Презентация доклада начальника лаборатории ФАУ «ГНИИИ ПТЗИ ФСТЭК России», 16 слайдов. Режим доступа: <http://new.groteck.ru/images/catalog/70840/e75c72a254fcc880fa65657fdb144063.pdf>. (Дата обращения 04.11.2019)
3. Kruegel C. Full System Emulation: Achieving Successful Automated Dynamic Analysis of Evasive Malware / C. Kruegel. // Article presented at Black Hat 2014. Режим доступа: <https://pdfs.semanticscholar.org/0188/89086d30f75f5bec7142d02079ced0b7d623.pdf>. (Дата обращения 04.11.2019)
4. Довгалюк П.М. Применение программных эмуляторов в задачах анализа бинарного кода / П.М. Довгалюк, В.А. Макаров, В.А. Падарян и др. // Труды Института системного программирования РАН, том 26, вып. 1, 2014, стр. 277-296. DOI: 10.15514/ISPRAS-2014-26(1)-9.
5. Ермаков М.К. Применение статической бинарной инструментации с целью проведения динамического анализа программ для платформы ARM / М.К. Ермаков, С.П. Вартаков // Труды Института системного программирования РАН, том 27, вып. 1, 2015, с. 5-24. DOI: 10.15514/ISPRAS-2015-27(1)-1.
6. Nethercote N. Dynamic binary analysis and instrumentation / N. Nethercote // University of Cambridge, 2004, 170 -pp. Режим доступа: <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-606.pdf>. (Дата обращения 04.11.2019)
7. Островский А.С. Использование бинарной инструментации кода в динамическом анализе программного обеспечения / А.С. Островский, М.В. Малахов // Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции, 2018, с. 148-151.
8. Hex-Rays: about IDA. Режим доступа: <https://www.hex-rays.com/products/ida/index.shtml>. (Дата обращения 07.11.2019)

Научный руководитель: Островский Александр Сергеевич, доцент, доктор технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, aleksandr_ostrovsky@mail.ru.

Automated tool for static instrumentation firmware's binary code

Malahov M.V.¹⁹², Alexeev K.A.¹⁹³

Abstract. *Currently, the task of searching vulnerabilities and undeclared features in the firmware of various devices is becoming increasingly relevant. In solving this problem, dynamic analysis methods are widely used, one of the important stages of which is the procedure for collecting trace information. In this paper are substantiated the choice of code instrumentation as a method of collecting trace information during dynamic analysis of firmware. A brief description of this technology is provided. The main requirements to the instrumentation tool for binary code of various microcontroller architectures are advanced. A possible*

¹⁹² Mihail Malahov, MSTU, Moscow, Russia. E-mail: misha.malaxow@yandex.ru.

¹⁹³ Kirill Alexeev, MSTU, Moscow, Russia. E-mail: k-alexeev7@yandex.ru.

approach to the construction of such tool is proposed. The features of the tool developed in accordance with the proposed approach are described, as well as its research is carried out to meet the requirements.

Key words: *information security, vulnerability searching, dynamic analysis, microcontroller code analysis software.*

References

1. Barabanov A.V. 28 magicheskikh mer razrabotki bezopasnogo programmno obespecheniya / A.V. Barabanov, A.S. Markov, V.L. Tsirlov // Voprosy kiberbezopasnosti, 2015, № 5 (13), pp. 2-10.
2. Serdechnyy A.L. Metodika vyavleniya uyazvimostey i nedeklarirovannykh vozmozhnostey v programmnom obespechenii / A.L. Serdechnyy // Prezentatsiya doklada nachal'nika laboratorii FAU «GNII PTZI FSTEK Rossii», 16 slaydov. URL: <http://new.groteck.ru/images/catalog/70840/e75c72a254fcc880fa65657fdb144063.pdf>.
3. Kruegel C. Full System Emulation: Achieving Successful Automated Dynamic Analysis of Evasive Malware / C. Kruegel. // Article presented at Black Hat 2014. URL: <https://pdfs.semanticscholar.org/0188/89086d30f75f5bec7142d02079ced0b7d623.pdf>.
4. Dovgalyuk P.M. Primeneniye programmnykh emulyatorov v zadachakh analiza binarnogo koda / P.M. Dovgalyuk, V.A. Makarov, V.A. Padaryan i d.r. // Trudy Instituta sistemnogo programirovaniya RAN, tom 26, vyp. 1, 2014, pp. 277-296. DOI: 10.15514/ISPRAS-2014-26(1)-9.
5. Yermakov M.K. Primeneniye staticheskoy binarnoy instrumentatsii s tsel'yu provedeniya dinamicheskogo analiza programm dlya platformy ARM / M.K. Yermakov, S.P. Vartanov // Trudy Instituta sistemnogo programirovaniya RAN, tom 27, vyp. 1, 2015, pp. 5-24. DOI: 10.15514/ISPRAS-2015-27(1)-1.
6. Nethercote N. Dynamic binary analysis and instrumentation / N. Nethercote // University of Cambridge, 2004, 170 -pp. URL: <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-606.pdf>.
7. Ostrovskiy A.S. Ispol'zovaniye binarnoy instrumentatsii koda v dinamicheskom analize programmno obespecheniya / A.S. Ostrovskiy, M.V. Malahov // Bezopasnyye informatsionnyye tekhnologii. Sbornik trudov Devyatoy vserossiyskoy nauchno-tekhnicheskoy konferentsii, 2018, pp. 148-151.
8. Hex-Rays: about IDA. URL: <https://www.hex-rays.com/products/ida/index.shtml>.

Алгоритм защиты терминальных программ от анализа на основе виртуальных машин с секретной архитектурой

Маркин Д. О.¹⁹⁴, Вихарев А. Н.¹⁹⁵, Звягинцев С. А.¹⁹⁶, Павлов Д. И.¹⁹⁷

В работе описан алгоритм защиты терминальных программ от анализа. Объектом защиты в работе являются терминальные программы. Алгоритм защиты терминальных программ основан на применении виртуальных машин. Проведен анализ особенностей и условий функционирования терминальных программ, описана модель угроз. Разработана структурная схема системы защиты программного обеспечения на основе виртуальных машин. Предложенная система защиты представляет собой аналог несимметричной криптографической системы, в которой секретным ключ является архитектура виртуальной машины, а открытым – исполняемый байт код. Эффективность предложенного алгоритма по частным показателям качества (оперативности) проверена путем сравнительного анализа программных реализаций на C/C++ и Java.

Ключевые слова: виртуализация, динамическая архитектура, несимметричная криптосистема.

Введение

В ряде автоматизированных систем ПО доступно исследователям в виде исходного или байт-кода. Подобные системы используют интерпретаторы либо виртуальные машины для исполнения кода. Защита такого типа ПО от анализа требует применения подходов, обеспечивающих максимальное затруднение анализа исходных текстов – т.е. применения методов обфускации [1].

Проблема защиты программных реализаций на основе применения технологий виртуализации и других методов защиты затрагивалась в научных трудах Аранова В. Ю., Петрова А. С.[2,3], Речистова Г. С.[4], а также Казарина О. В., Варнавского Н. П., Захарова В. А., Кузюрина Н. Н. и Шокурова А. В. [1,5], Зегжды П. Д., Бойко В. П., Заборовского В. С., Подловченко Р. И., Иванникова В. П., Сомборсона К., Викстромома Д. и других. В указанных работах отмечалась необходимость защиты программных реализаций от технологий обратной разработки, основанных, в том числе на методах статического и динамического анализа ПО.

1. Объект защиты

В данной работе объектом защиты являются терминальные программы (активные данные), передаваемые между узлами системы, обеспечивающей их исполнение на данных узлах [7,8]. Реализация концепции активных данных может базироваться на применении скриптовых языков программирования, таких как *PHP*, *Perl*, *Python*, *Ruby*, *JavaScript* и других (рис. 1), а также способности приложений, выполняющих роль интерпретатора, обрабатывать содержание данных (например, тела *HTTP(s)*-запросов) как программный код.

¹⁹⁴ Маркин Дмитрий Олегович, канд. техн. наук, Академия ФСО России, г. Орёл, mdo@academ.msk.rsnet.ru

¹⁹⁵ Вихарев Антон Николаевич, Академия ФСО России, г. Орёл

¹⁹⁶ Звягинцев Станислав Александрович, Академия ФСО России, г. Орёл

¹⁹⁷ Павлов Дмитрий Игоревич, Академия ФСО России, г. Орёл

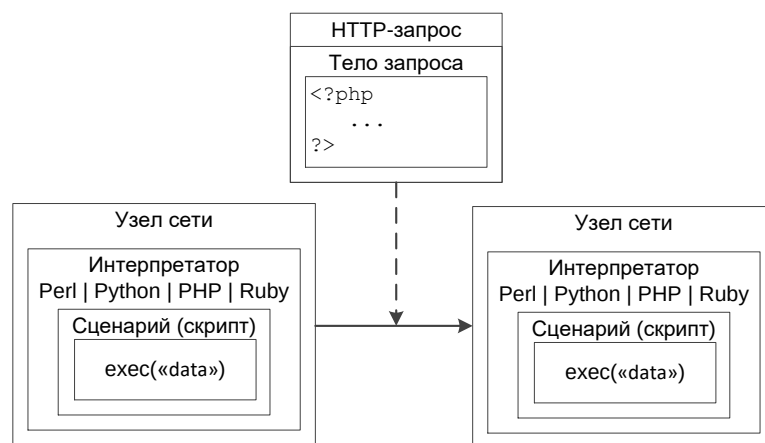


Рис. 5. Реализация концепции активных данных на основе применения скриптовых языков

Эффективность такой реализации была проверена в работах [9, 10] на базе сети веб-прокси серверов с помощью ряда разработанных программных средств [11, 12], а также с использованием испытательного стенда на основе МАУ под управлением ОС Android [13] и управляющего веб-сервера для решения типовой задачи факторизации [14].

Недостатками использования технологии активных данных являются:

- необходимость обеспечения аутентичности кода, защиты клиентского приложения от анализа, авторизации исполняемых активных данных, т. е. защиты от компрометации клиентского приложения;
- необходимость использования интерпретаторов;
- передача кода в виде исходных текстов;
- необходимость диспетчеризации.

Проблема обеспечения авторизации терминальных программ обусловлена отсутствием доверия к устройству, на котором они выполняются.

Одним из наиболее эффективных способов защиты исходного текста ПО от анализа, не исключающий применения других методов, является внедрение технологии виртуализации кода [4, 6, 8].

2. Математическая модель системы защиты активных данных от анализа на основе виртуализации исполняемого кода

Под защитой ПО авторы [2] понимают такой метод выполнения программы, при котором невозможно выявить процесс обработки данных и восстановление алгоритма работы программы, либо максимально его затруднить решение данных задач. Формально, данную задачу можно представить как

$$Y = F(X, K), \quad (1)$$

где X – множество входных данных, Y – множество выходных данных, K – множество данных, определяющих право на лицензионное использование экземпляра ПО, F – отображение, определяющее множество процессов обработки входных данных. Таким образом, задача защиты ПО заключается в затруднении восстановления отображения F .

Формально, задача обфускации [3] состоит в получении отображения (обфускатора)

$$F': (X, K) \xrightarrow{F'} Y, \quad (2)$$

функционально эквивалентного отображению F в смысле получения эквивалентного множества выходных данных Y при таких же множествах входных данных (X, K) .

В ряде работ отмечалось, что обфускаторы могут использоваться для создания криптосистем с открытым ключом [6], гомоморфных систем шифрования [6], схем дезавуируемого шифрования и односторонних функций с секретом.

Общая структурная схема системы, в которой осуществляется обмен и исполнение активных данных (терминальных программ) представлена на рисунке 6, где ВМ – виртуальная машина.

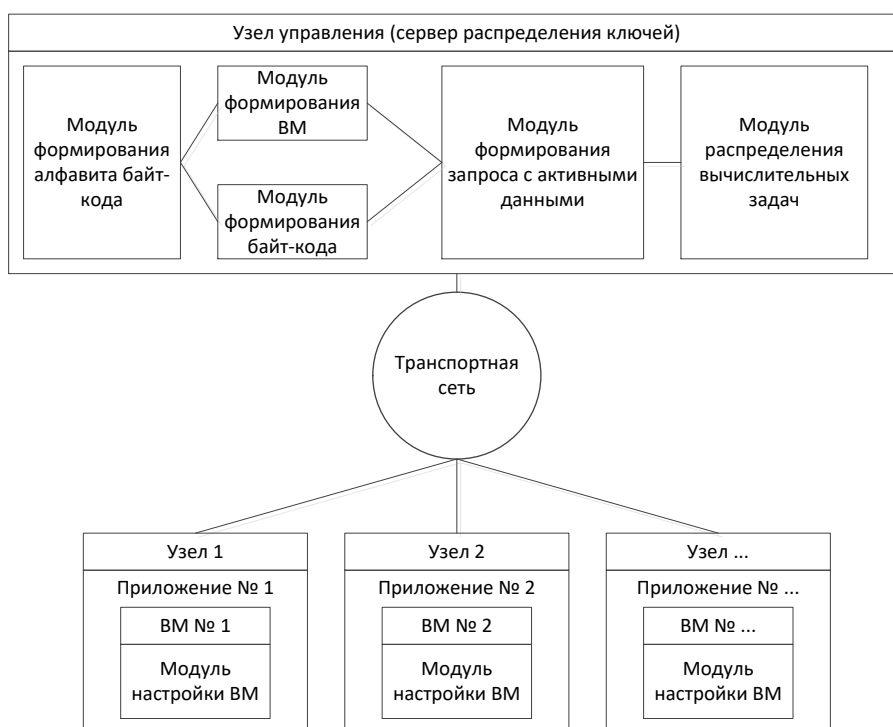


Рис. 6. Структурная схема система обмена терминальными программами

Процесс функционирования защищаемого ПО можно представить как криптосистему [1, 16] (рис.3), в которой алгоритм обфускатора и сформированный ключ являются криптограммами, а защищаемый алгоритм и исходные данные – открытым текстом.

$$(F_{VM}, X_B) = E(F, X, K), \quad (3)$$

где F – отображение, определяющее множество процессов обработки входных данных, X – множество входных данных, K – секретный ключ криптосистемы, X_B – множество входных данных (байт-код) для виртуальной машины F_{VM} , F_{VM} – отображение, определяющее множество процессов обработки входных данных, представленных в виде байт-кода, E – шифр, удовлетворяющий принципам Керкгоффса для криптосистем [17].

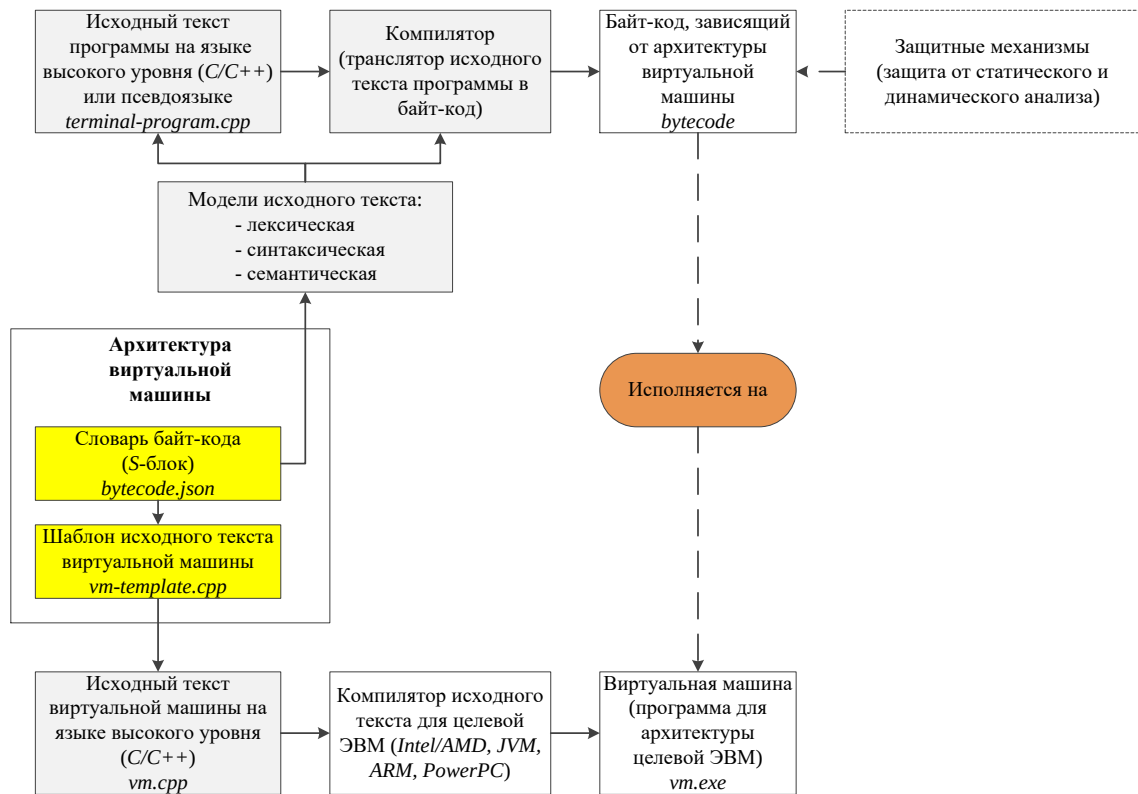


Рис. 7. Система защиты активных данных

Отображения F , F_{VM} , F_S и E в общем случае могут быть представлены в виде конечного автомата:

$$A(X, S, Y, h, f), \quad (4)$$

где X, S, Y – непустые множества элементов входного, внутреннего (состояния автомата) и выходных символов алфавитов, а h, f – отображения, определяющие функцию переходов между состояниями и функцию выходов автомата.

Таким образом, процесс отображения исходного (защищаемого) алгоритма и набора входных данных в защищенный может быть представлен как:

$$X \xrightarrow{E_B} X_B, \quad (5)$$

$$F \xrightarrow{E_F} F_{VM}, \quad (6)$$

при условии, что $Y' = Y$, где $Y' = F_{VM}(X_B)$, а $Y = F(X, K)$, а $(E_B, E_F) \in E$.

Секретным ключом $K = (K_X, K_B, K_{VM})$ в предлагаемой криптосистеме являются:

- множество подстановок K_X , определяющих соответствие между элементами множества X и элементами множества X_B – элементы алфавита байт-кода (словаря байт-кода);

- множество подстановок K_B , определяющих соответствие между инструкциями или операциями (правилами преобразования) из множества F и элементами подмножества F_{VM} – элементы алфавита байт-кода (словаря байт-кода);

- множество K_{VM} элементов F_{VM} , определяющих архитектуру виртуальной машины.

В свою очередь, исполняемый машинный код виртуальной машины также должен быть сформирован с учетом используемого словаря байт-кода $(K_X, K_B) \subset K$, а также избранной архитектуры виртуальной машины.

Суть предлагаемого решения заключается в том, что каждый экземпляр реализации виртуальной машины и исполняемый на нем байт-код являются уникальными, строго

соответствующими друг другу. Иными словами, байт-код и виртуальная машина, сформированные с использованием разных ключей $K = (K_X, K_B, K_{VM})$ будут несовместимы.

Секретным ключом являются:

- словарь байт-кода `bytecode.json`;
- архитектура виртуальной машины `vm-template.cpp` и получаемая на ее основе виртуальная машина `vm.cpp`.

Процедуру формирования `vm.cpp` можно описать отображением

$$F \xrightarrow{E_F(K_{VM}, K_B)} F_{VM}, \quad (7)$$

или $F_{VM} = E_F(F, K_{VM}, K_B)$.

Процедуру формирования байт-кода, способного выполняться только в заданной виртуальной машине, можно описать отображением

$$X \xrightarrow{E_B(K_X, K_B)} X_B, \quad (8)$$

или $X_B = E_B(X, K_X, K_B)$.

Таким образом, представленная криптосистема обеспечит получение выходных данных $Y' = Y$, где $Y' = F_{VM}(X_B)$, а $Y = F(X, K)$, а $(E_B, E_F) \in E$, но при этом процесс анализа экземпляра программной реализации $F_{VM}(X_B)$ по сравнению с реализацией $F(X, K)$ будет значительно затруднен.

Таким образом, сущность защиты программного кода на основе обфускации с использованием виртуальных машин заключается в том, чтобы заставить исследователя перейти от анализа машинных инструкций известной архитектуры (например, x86) к незнакомому набору виртуальных команд, которые увеличат сложность и, соответственно, затрачиваемое время на анализ защиты.

В рассматриваемой в работе несимметричной криптосистеме процесс зашифрования на открытом ключе эквивалентен процессу трансляции (отображению) E_B защищаемого исходного текста X в байт-код X_B :

$$X \xrightarrow{E_B(K_X, K_B)} X_B, \quad (9)$$

или $X_B = E_B(X, K_X, K_B)$, где K_X – множество подстановок, определяющих соответствие между элементами множества X и элементами множества X_B – элементы алфавита байт-кода (словаря байт-кода); K_B – множество подстановок, определяющих соответствие между инструкциями или операциями (правилами преобразования) из множества F (множество инструкции исходного текста защищаемого приложения) и элементами подмножества F_{VM} – элементы алфавита байт-кода (словаря байт-кода), используемые в виртуальной машине.

При этом открытым ключом является словарь байт-кода K_X , а закрытым – архитектура виртуальной машины, скомпилированная на основе того же словаря байт-кода $(K_X, K_B) \subset K$.

3. Эффективность системы защиты активных данных в распределенной вычислительной системе

Для того, чтобы преодолеть защитные механизмы, исполняемые встроенной в приложение виртуальной машиной как инструкции байт-кода, необходимо решить следующие задачи:

- 1) проанализировать работу компонентов интерпретатора виртуальной машины:
 - выделить машинные коды инструкций байт-кода;
 - определить фактические инструкции, исполняемые при выполнении обнаруженных инструкций байт-кода;
- 2) выделить семантику инструкций байт-кода на основе анализа фактически исполняемых машинных инструкций;

3) восстановить логику работы целевого кода (алгоритм).

Для оценивания эффективности предлагаемой системы было разработано два прототипа ее программной реализации [12]: на языке *C/C++* (рис. 7) и на языке *Java* (рис. 8) и проведены эксперименты по сравнительному анализу вычислительной сложности данных прототипов.

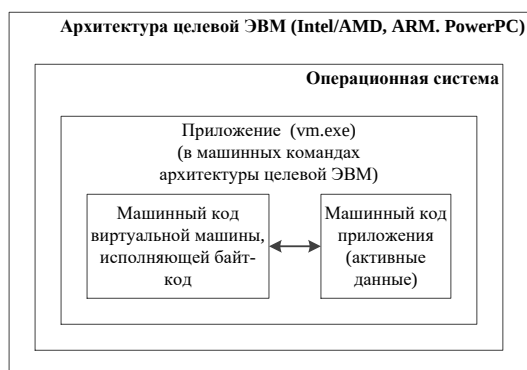


Рис. 8. Функционирование виртуальной машины в целевой среде

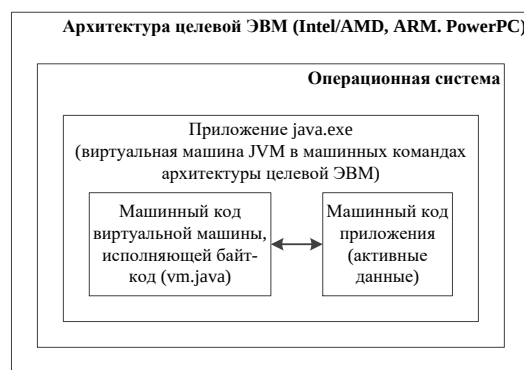


Рис. 9. Функционирование виртуальной машины vm.java

Проведенный сравнительный анализ реализаций показал, что время выполнения защищенного приложения увеличивается примерно в 1,71 раза и в 14 раз объем кода.

Полученные результаты позволяют сделать следующие выводы:

1. Предлагаемая система защиты имеет недостаток, выраженный в том, что защита ПО с использованием предлагаемой системы предъявляет повышенные требования к вычислительной системе, в которой исполняется защищаемое ПО и снижает его производительность.

2. Достоинствами предложенной системы является:

- повышение сложности анализа ПО за счет вынуждения исследователя проводить анализ кода с неизвестными кодами виртуальных команд;
- невозможность выполнения байт-кода на виртуальной машине, если байт-код и виртуальная машина сформированы с использованием различных секретных ключей.

Выводы

В работе была предложена система защиты активных данных в распределенной вычислительной системе на основе применения виртуальных машин. Сформированы требования к ней, на основе проведенного анализа условий функционирования. Эффективность по частным показателям качества (оперативности) предложенной системы проверена в виде приложений на *C/C++* и *Java*.

Литература

1. Варнавский, Н. П. Современное состояние исследований в области обфускации программ: определение стойкости обфускации / Н. П. Варнавский, В. А. Захаров, Н. Н. Кузюрин, А. В. Шокуров // Труды ИСП РАН. – 2014. – Т. 26. – Вып. 3.
2. Петров, А. С. Технология защиты программного кода посредством применения виртуальной машины / А. С. Петров, А. А. Петров // Вестник ВГУ. – 2009. – № 9 (103), часть 1. – С. 117–122.
3. Аранов, В. Ю. Метод и средства защиты исполняемого программного кода от динамического и статического анализа : автореф. дис. ... канд. техн. наук : 05.13.19 / В. Ю. Аранов. – Санкт-Петербург, 2014. – 18 с.
4. Речистов, Г. С. Программное моделирование вычислительных систем : учебное пособие / Г. С. Речистов, Е. А. Елюгин, А. А. Иванов и др. – 2-е изд., испр. и доп. – Москва : МФТИ, 2013. – 222 с.

5. Казарин, О. В. Надежность и безопасность программного обеспечения / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт. – 2018. – 342 с.
6. Kaiyuan Kuang Enhanced virtual-machine-based code obfuscation security through dynamic bytecode scheduling / Kaiyuan Kuang, Zhanyong Tang, Xiaoqing Gong, Dingyi Fang, Xiaojiang Chen, Zheng Wang // Computers & Security. – 2018. – № 74. – P. 202–220.
7. Кулешов, С. В. Активные данные в цифровых программно-определяемых системах / С. В. Кулешов, О. В. Цветков // Информационно-измерительные и управляющие системы. – 2014. – Т. 12. – № 6. – С. 12–19.
8. Маркин, Д. О. Комплекс алгоритмов защищенных туманных вычислений на основе технологии активных данных / Д. О. Маркин, С. М. Макеев, А. Н. Вихарев // Известия Тульского государственного университета. Технические науки. – 2019. – Выпуск 3. – С. 263–269.
9. Маркин, Д. О. Организация анонимного доступа с помощью веб-прокси / Д. О. Маркин, А. С. Галкин, П. А. Архипов // Наукоемкие технологии в космических исследованиях Земли. – 2016. – Т. 8, № 5. – С. 44–49.
10. Маркин, Д. О. Исследование устойчивости анонимной сети на основе технологий веб-прокси / Д. О. Маркин, А. С. Галкин, П. А. Архипов // Вопросы кибербезопасности. – 2016. – № 2 (15). – С. 21–28.
11. Автоматизированная система управления содержанием удаленных информационных ресурсов: свидетельство о государственной регистрации программы для ЭВМ № 2016617298 Российская Федерация / Д. О. Маркин, С. М. Макеев, В. Д. Ленчук, А. А. Охрименко, Р. В. Шапкин ; авторы и правообладатели Д. О. Маркин, С. М. Макеев, В. Д. Ленчук, А. А. Охрименко, Р. В. Шапкин. – № 2016614475 ; заявл. 04.05.2016; зарегистрировано в Реестре программ для ЭВМ 29.06.2016 г
12. Программный агент обеспечения распределенных вычислений на основе технологии активных данных для узла вычислительной сети на базе мобильных устройств под управлением операционной системы Android : свидетельство о государственной регистрации программы для ЭВМ № 2018660343 Российская Федерация / Д. О. Маркин, М. А. Трохачёв, А. Э. Земцов, А. А. Юркин ; авторы и правообладатели Д. О. Маркин, М. А. Трохачёв, А. Э. Земцов, А. А. Юркин. – № 2018617165 ; заявл. 10.07.2018; зарегистрировано в Реестре программ для ЭВМ 22.08.2018 г.
13. Маркин, Д. О. Разработка агента туманных вычислений для мобильных устройств под управлением операционной системы Android / Д. О. Маркин, М. А. Трохачев // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : материалы XI Межрегиональной научно-практической конференции [Электронный ресурс] / под ред. О. М. Голембиовской, М. Ю. Рытова. – Брянск : БГТУ, 2019. – 190 с. – С. 136–141.
14. Маркин, Д. О. Алгоритм решения задачи факторизации средствами туманных вычислений / Д. О. Маркин, А. Э. Земцов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : материалы XI Межрегиональной научно-практической конференции [Электронный ресурс] / под ред. О. М. Голембиовской, М. Ю. Рытова. – Брянск : БГТУ, 2019. – 190 с. – С. 126–129.
15. Маркин, Д. О. Анализ методов и средств исследования программного обеспечения / Д. О. Маркин, Д. И. Павлов, С. А. Звягинцев // Актуальные направления развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации: XI Всероссийская межведомственная научная конференция: материалы и доклады (Орёл, 5–6 февраля 2019 г.) В 10 ч. Ч. 10 / под общ. ред. П. Л. Малышева. – Орёл: Академия ФСО России, 2019. – 200 с. – С. 34–37.
16. Sahai, A. How to Use Indistinguishability Obfuscation: Deniable Encryption, and More / A. Sahai, B. Waters // CRYPTO ePrint, 2013.
17. Auguste Kerckhoffs. La cryptographie militaire. Journal des sciences militaires, 1883.

Terminal Software Secure Algorithm Based on Virtual Machines With Secret Architecture

Markin D. O.¹⁹⁸, Viharev A. N.¹⁹⁹, Zvyagintcev S. A.²⁰⁰, Pavlov D. I.²⁰¹

The work contains description of terminal software secure algorithm. The aim of the algorithm is providing software security against analysis. The secure object is terminal programs. The algorithm is based on virtual machines application. The authors present the results of main terminal software functioning features, threats model. The presented algorithm is the basis for secure terminal software system based on virtual machines with secret architecture. This system is the analog of asymmetric cryptosystem. The private key of such cryptosystem is the virtual machines' architecture. The public key is executing byte code. Efficiency of presented system was checked by time and code volume complexity of two test programs coded on C/C++ and Java program languages.

Keywords: virtualization, dynamic architecture, asymmetric cryptosystem.

¹⁹⁸ Dmitry Markin, candidate of technical sciences, The Academy of Federal Security Guard Service of the Russian Federation, Oryol, mdo@academ.msk.rsnet.ru

¹⁹⁹ Anton Viharev, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

²⁰⁰ Stanislav Zvyagintcev, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

²⁰¹ Dmitry Pavlov, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

Технологии распознавания моделей точек входа веб-приложений**Маркин Д. О.²⁰², Зверев А. А.²⁰³, Саклаков А. И.²⁰⁴, Рыков Д. А.²⁰⁵**

В работе представлен анализ существующих технологий распознавания моделей точек входа веб-приложений. Описаны наиболее распространенные модели точек входа, используемые для передачи данных в веб-приложения. Проведен анализ современных средств автоматизированного тестирования веб-приложений, их достоинств и недостатков. Описаны современные информационные технологии, используемых в информационных веб-ресурсах, а также технологии и применяемые способы, и средства защиты программного обеспечения веб-приложений от анализа. Сформулированы основные проблемы по идентификации и распознаванию точек входа с точки зрения реализации автоматизированного интеллектуального фаззинга веб-приложений в целях поиска уязвимостей и недеklarированных возможностей.

Ключевые слова: фаззинг, веб-ресурс, модель веб-ресурса, поиск уязвимостей.

Введение

Как показывает статистика, современные веб-приложения имеют большое число проблем, связанных с обеспечением информационной безопасности, а поиск уязвимостей требует серьезных вычислительных ресурсов и высокой квалификации персонала, отвечающего за вопросы информационной безопасности. В связи с этим актуальной задачей является создание автоматизированных и автоматических средств поиска уязвимостей веб-приложений, позволяющих осуществлять эффективный анализ защищенности веб-ресурсов.

Одним из эффективных способов решения задачи автоматизированного анализа защищенности является фаззинг веб-приложений [1, 2, 3, 4]. Данный метод тестирования представляет собой тестирование на основе модели "черного" ящика (функциональное тестирование), т.е. в условиях отсутствия сведений о приложении или в отдельных случаях модели "серого" ящика, когда о веб-приложении имеется некоторая информация.

Построение автоматизированных средств анализа защищенности информационных систем и веб-приложений, поиска уязвимостей в них рассматривались в работах М. Саттона, П. Амини [1] и других. Вопросы оценивания защищенности информационных систем затрагивались в научных трудах Хорева П. Б. и Петрова С. А. [5], Котенко И. В., Степашкина М. В. [6] Машкиной И. В., Саенко И. Б., Азарова А. А., Тулупьева А. Л., Азарновой Т. В. и Полухина П. В. [7], Горюнова М. Н. и Мацкевича А. Г. [8] и других. Актуальные практические вопросы и инструменты оценивания защищенности веб-приложений представлены на свободных информационных ресурсах проектов OWASP, MITRE, White Hat, DISA и других.

Однако в связи с постоянным совершенствованием информационных технологий и способов представления информации, кодирования веб-приложений, синтаксической и семантической разметки электронных документов проблема автоматизации тестирования защищенности остается актуальной. Данное обстоятельство указывает на объективную необходимость внедрения новых подходов по распознаванию структурных элементов веб-приложений, отвечающих за ввод данных (запрос) в информационную систему и получение ответа от нее.

²⁰² Маркин Дмитрий Олегович, канд. техн. наук, Академия ФСО России, г. Орёл, mdo@academ.msk.rsnet.ru

²⁰³ Зверев Артем Александрович, Академия ФСО России, г. Орёл

²⁰⁴ Саклаков Алексей Иванович, Академия ФСО России, г. Орёл

²⁰⁵ Рыков Даниил Алексеевич, Академия ФСО России, г. Орёл

Анализ способов построения фаззеров веб-приложений

Классическая схема фаззинга в условиях отсутствия информации об объекте тестирования (модель "черного ящика") не совершенна в силу потребности перебора практически неограниченного набора входных данных для получения исчерпывающих результатов.

В связи с этим используют различные подходы, позволяющие формировать выборки входных данных, позволяющие с большей вероятностью обнаруживать ошибки в объектах тестирования, в том числе с учетом информации об объекте тестирования (рис.1). К ним относятся:

схемы фаззинга с псевдослучайной генерацией входных данных;

схемы фаззинга с обратной связью, в т.ч. с применением интеллектуальных методов обработки выходных данных [2];

фаззинг на основе данных об известных ошибках и уязвимостях [3], в том числе на основе информации открытых баз данных, списков и метрик (CVE, CWE, NVD, CVSS, бюллетеней *Microsoft*);

фаззинг на основе данных о составе и структуре объекта тестирования, включая схемы фаззинга, извлекающие данную информацию из объекта тестирования.



Рис. 10. Схема фаззинга с обратной связью при формировании входных данных

В отношении веб-ресурсов и веб-приложений представленная схема фаззинга сравнительно эффективно применяется и в настоящее время. На сегодняшний день существует множество фаззеров веб-приложений: *Web Scarab*, *BurpSuite*, *Skyfish*, *SPIKE Proxy*, *OWASP WSFuzzer (SOAP)*, *Rfuzz*, *Fuzzops*, *PowerFuzzer*, *w3af*, *WebFuzz*, отдельные средства тестирования веб-приложений есть в составе таких инструментальных средств как *X-Spider*, *Nessus*, *OpenVAS*, *nmap* и других.

Одним из общих существенных недостатков указанных средств является проблема построения структурной модели произвольного веб-ресурса, которая позволила бы более эффективно направлять входные данные в исследуемые веб-приложения и его программное окружение. Решение данной проблемы лежит в разработке эффективного приложения, так называемого "робота-паука", способного эффективно распознавать все множество возможных точек входа с учетом современного уровня развития и внедрения информационных технологий, а также средств защиты приложений от анализа.

Однако факт существования эффективного решения данной проблемы находится под сомнением по следующим причинам:

– информационные технологии, формы представления информации, кодирования веб-приложений, синтаксической и семантической разметки информационных ресурсов постоянно совершенствуются;

– веб-приложения могут разрабатываться с применением технологий обфускации и других технических решений по защите от анализа [9, 10];

– количество вариантов форм представления точек входа веб-приложений с учетом текущего уровня развития информационных технологий бесконечно велико.

Модели точек входа веб-приложений

Очевидно, что чем более качественно будут формироваться входные данные для очередной итерации тестирования, тем выше вероятность обнаружения ошибок либо недекларируемых возможностей. Наличие актуальной модели исследуемого объекта позволяет учитывать важную информацию при формировании очередной выборки входных данных и, соответственно, повышает результативность фаззинга. Таким образом, для эффективного распознавания формы представления точки входа веб-приложения необходимо иметь ее описательную модель.

Современные технологии синтаксической и семантической разметки информационных ресурсов, а также средства разработки веб-приложений, функционирующих, в том числе на стороне веб-клиента, позволяют создавать в составе информационного ресурса различные точки входа веб-приложений.

Наиболее распространенные варианты моделей точек входа веб-приложений представлены ниже:

1. На основе данных *URL*, а также *HTML*-тегов, определяющих гиперссылки, и других тегов с параметром *href* например

```
<a href="URL ресурса">Текст</a>
```

2. На основе данных веб-форм и параметра *action*:

```
<form action="index.php">  
  <input type="text" name="" />  
  <input type="hidden" name="" value="" />  
  <input type="submit" value=" " />  
</form>
```

3. На основе специализированных *HTML*-тегов, указывающих на ресурсы, а также *HTML*-тегов с параметром *src*:

```
<video src="<URL>"></video>  
<audio src="<URL>"></audio>  
  
<embed src="<URL>"></embed>
```

4. На основе ссылок на *JavaScript*-приложения и стили *CSS*:

```
<script src="URL ресурса с JavaScript-приложением" />  
<link rel=stylesheet href="URL ресурса со стилями CSS" />
```

5. На основе *HTML*-тегов, определяющих фреймы:

```
<frame src="URL ресурса" />  
<iframe src="URL ресурса" />
```

6. На основе инструкций *@import* в таблицах каскадных стилей *CSS*:

```
<style>  
  @import "URL ресурса"  
</style>
```


7. На основе параметра *url* инструкций в таблицах каскадных стилей:

list-style: url(...)
background-image: url(...)
behavior: url(...)

Каждый из предложенных вариантов допускает параметризацию *URL* после символа "?" с заданием значений, передаваемых в заголовке *HTTP*-запроса как *GET*-параметр. Возможны и другие варианты разметки электронных документов, определяющих точки входа в веб-приложения.

Ряд информационных систем могут строиться на основе так называемой концепции "единой" точки входа в веб-приложение. Суть данной концепции заключается в том, что определяется только одна явная точка входа в веб-приложение, которая параметризуется, за счет чего и формируется все множество ответов веб-клиенту в виде электронных документов. Как правило, это информационные системы на базе ряда *PHP* и *Python*-фреймворков, например, *Yii2* или *Django*.

Наиболее известными на данный момент расширениями веб-клиентов являются *ActiveX*, *JavaScript*, *HTML5*, *CSS*, *Google Dart* и другие.

Существует большое количество надстроек над данными расширениями – фреймворков, позволяющих создавать приложения в специально сформированном программном окружении со специфическим синтаксисом языка программирования. К ним относятся такие фреймворки *JavaScript* как *Angular*, *React*, *Socket*, *Polymer*, *Meteor*, *Backbone* и другие, а также библиотеки *JavaScript*: *jQuery*, *jQuery UI*, *MooTools*, *Dojo*, *Kendo UI*, *Webix* и другие.

Наиболее известными веб-серверами в настоящее время являются: *Apache*, *Nginx*, *Microsoft IIS*, *LightHTTPd*, *Google Web Server*, *Resin*, *Cherokee*, *Rootage*, *Open Server*, *H20*, *THTTPD*, *Jetty*, а расширения, отвечающие в том числе за обработку запросов и параметров заголовков – *CGI*, *PHP*, *Perl*, *Python*, *ASP*, *ISAPI* и другие.

Наиболее наглядным примером обработки *HTTP*-заголовка веб-серверов в совокупности с расширением веб-клиента, обрабатывающим *CSS*-документ является создание "невидимой" *HTML*-разметки, когда содержание *HTML*-страницы формируется через *CSS*-документ, передаваемый в заголовке *HTTP*-запроса:

Link <css-without-html.css>;rel=stylesheet

В составе подгружаемого документа "*css-without-html.css*" определен стиль с параметром "content", внутри которого находится электронный документ с *HTML*-разметкой (*mathiasbynens.be/demo/css-without-html*).

Существенную сложность в распознавании точек входа веб-приложений создают технологии защиты исполняемого, а также интерпретируемого кода приложений от анализа [6, 7], такие как обфускация и шифрование.

В ряде случаев, распознавание точек входа, после применения обфускаторов, становится практически нереализуемым и не позволит сформировать адекватную модель информационного ресурса.

Выводы

В работе проведен анализ технологий, необходимых для распознавания точек входа, при построении адаптивных фаззеров веб-приложений. Сформулирована проблема эффективного распознавания точек входа для веб-приложений, защищенных средствами обфускации и шифрования. Обоснована необходимость наличия средства анализа

информационной модели веб-ресурса при построении эффективного фаззера веб-приложений.

Полученные результаты позволят обосновать структуру эффективного средства фаззинга веб-приложений в целях поиска уязвимостей и недеklarированных возможностей.

Отдельные аспекты технологии фаззинга веб-приложений реализованы в работах [3, 4, 11] с использованием программного средства [12].

Литература

1. Саттон, М., Fuzzing: исследование уязвимостей методом грубой силы [пер. с англ.] / М. Саттон, А. Грин, П. Амини. – Санкт-Петербург : Символ-Плюс, 2009. – 560 с., ил.
2. Полухин, П. В. Байесовские модели и алгоритмы управления процессом тестирования веб-приложений методом фаззинга: дис. 05.13.18 / П. В. Полухин. – Воронеж, 2016. – 180 с.
3. Маркин, Д. О. Распределенное тестирование веб-приложений методом фаззинга на основе технологий веб-прокси и активных данных / Д. О. Маркин, А. С. Галкин // Труды Северо-Кавказского филиала Московского технического университета. Ч. 2. – Ростов-на-Дону: ПЦ "Университет" СКФ МТУСИ, 2017. – 442 с. – С. 61–72.
4. Маркин, Д. О. Алгоритм распределенного тестирования веб-приложений на основе технологий веб-прокси и активных данных / Д. О. Маркин, П. А. Архипов, А. С. Галкин // Информационные системы и технологии. – 2018. – № 1. (105). – С. 93–101.
5. Петров, С. А. Методы искусственного интеллекта в задачах обеспечения безопасности компьютерных сетей / С. А. Петров, П. Б. Хорев // Труды 18 МНТК "Радиоэлектроника, электротехника, и энергетика". – Издательский дом МЭИ, 2012. – Т. 2. – С. 63.
6. Котенко, И. В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак / И. В. Котенко, Е. В. Степашкин, Е. В. Дойникова // Проблемы информационной безопасности. Компьютерные системы. – 2011. – № 3. – С. 40–57.
7. Азарнова, Т. В. Исследование процесса фаззинга SQL-инъекций веб-приложений на основе динамической сети Байеса / Т. В. Азарнова, П. В. Полухин // Вестник Воронежского государственного ун-та. Серия: Системный анализ и информационные технологии. – 2014. – № 1. – С. 120–129.
8. Горюнов, М. Н. Распознавание функциональных объектов программного обеспечения в условиях отсутствия исходных текстов / М. Н. Горюнов, В. Т. Еременко, А. Л. Ершов, А. Г. Мацкевич // Информационные системы и технологии. – 2013. – № 5. – С. 112–120.
9. Казарин, О. В. Надежность и безопасность программного обеспечения / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт. – 2018. – 342 с.
10. Варнавский, Н. П. Современное состояние исследований в области обфускации программ: определение стойкости обфускации / Н. П. Варнавский, В. А. Захаров, Н. Н. Кузюрин, А. В. Шокуров // Труды ИСП РАН. – Т. 26. – Вып. 3. – 2014.
11. Маркин, Д. О. Распределенное тестирование веб-приложений методом фаззинга на основе технологий веб-прокси и активных данных / Д. О. Маркин, А. С. Галкин // Труды Северо-Кавказского филиала Московского технического университета. – Ч. 2. – Ростов-на-Дону : ПЦ «Университет» СКФ МТУСИ, 2017. – 442 с. – С. 61–72.
12. Программный комплекс распределенного тестирования удаленных веб-ресурсов: свидетельство о государственной регистрации программы для ЭВМ № 2017618056 Российская Федерация / Д. О. Маркин, А. С. Галкин, П. А. Архипов, А. А. Юркин, Н. Д. Смирнов ; авторы и правообладатели Д. О. Маркин, А. С. Галкин, П. А. Архипов, А. А. Юркин, Н. Д. Смирнов. – № 2017613310 ; заявл. 06.04.2017; зарегистрировано в Реестре программ для ЭВМ 21.07.2017 г.

Web Application Entry Points Recognition Technologies

Markin D. O.²⁰⁶, **Zverev A. A.**²⁰⁷, **Saklakov A. I.**²⁰⁸, **Rykov D. A.**²⁰⁹

Abstract. *The work contains actual web application entry points recognition technologies analysis. The most popular web application entry points` models are described. The authors present the analysis of contemporary facilities of web application automatic testing used for weaknesses detection. Actual information technologies used by web resources and their main features are analyzed. Also the works contains detailed description of contemporary methods and facilities used for web application software defense against analysis. The authors came to the conclusion about main technical problems during identification and recognition of web application entry points need for intelligent web application fuzzing used for weaknesses backdoor and spyware detection.*

Keywords: *fuzzing, web resource, informational web resource model, vulnerability detection.*

²⁰⁶ Dmitry Markin, candidate of technical sciences, The Academy of Federal Security Guard Service of the Russian Federation, Oryol, mdo@academ.msk.rsnet.ru

²⁰⁷ Artyom Zverev, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

²⁰⁸ Alexey Saklakov, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

²⁰⁹ Daniil Rykov, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

Современные технологии построения доверенных сред исполнения приложений на уровне базовой системы ввода-вывода

Маркин Д. О.²¹⁰, Умбетов Т. К.²¹¹, Архипов М. А.²¹², Миначев В. М.²¹³

Статья посвящена проблемам доверия к программно-аппаратным платформам иностранного производства и способам решения этих проблем при помощи доверенных сред исполнения. Проведен анализ требований законодательства по защите компьютерных систем средствами технологий доверенной загрузки. Исследованы особенности реализаций современных технологий построения доверенных сред исполнения приложений, применяемых на уровне базовой системы ввода-вывода. Сформулированы основные проблемы доверия к современным программно-аппаратным платформам иностранного производства. Проведен сравнительный анализ отечественных технических решений по повышению доверия к средствам доверенной загрузки импортного производства. На основе результатов анализа сформулированы выводы и направления развития.

Ключевые слова: доверенная загрузка, TrustZone, ARM, TEE, TSM, BIOS

Введение

В сложившихся геополитических обстоятельствах доверие к программно-аппаратным техническим решениям иностранного производства исключено. Однако в связи с отсутствием аналогичных отечественных технологий и элементной базы применяются специальные процедуры проверки соответствия, позволяющие повысить степень доверия к подобным техническим решениям. Объективная потребность в повышении защищенности исполнения приложений, функционирующих в составе систем безопасности и обрабатывающих защищаемую информацию, привела к появлению технических решений, создающих так называемые доверенные среды исполнения (ДСИ) на основе аппаратных средств доверенных загрузки (СДЗ) или аппаратно-программных модулей доверенной загрузки (АПМДЗ). Наиболее далеко в разработке таких средств защиты продвинулись разработчики компаний *Intel*, *ARM*.

Основополагающая нормативная база, определяющая базовые требования к средствам доверенной загрузки, порядку их разработки и оценки соответствия, это закон "О защите государственной тайне", федеральные законы "Об информации, информационных технологиях и защите информации", "О техническом регулировании", базовые ведомственные нормативные акты "Положения о системе сертификации" ФСБ и ФСТЭК, Приказ ФСТЭК России № 119, методические документы и профили защиты. Общие требования к СДЗ, процедурам и критериями оценки безопасности заданы также в стандартах ГОСТ ISO/IEC 17000–2012, ГОСТ Р ИСО/МЭК 15408–1–2–3, ГОСТ Р 51583–2014.

Критически важными факторами, способными нанести ущерб безопасности обрабатываемой информации являются:

8. Отсутствие отечественной элементной базы.

В данных условиях на любом из этапов разработки средств защиты информации (СЗИ), в том числе, программно-аппаратного или аппаратного, могут быть внедрены программно-аппаратные закладки, способные нанести ущерб безопасности обрабатываемой информации.

²¹⁰ Маркин Дмитрий Олегович, канд. техн. наук, Академия ФСО России, г. Орёл, mdo@academ.msk.rsnet.ru

²¹¹ Умбетов Тимур Курганбекович, Академия ФСО России, г. Орёл, tmrider@yandex.ru

²¹² Архипов Михаил Андреевич, Академия ФСО России, г. Орёл

²¹³ Миначев Владислав Маратович, Академия ФСО России, г. Орёл

9. Отсутствие доверенной среды/средства разработки (компилятор программного кода).

Создавшиеся предпосылки привели к появлению технологии доверенных сред исполнения ДСИ (*TEE – Trusted Execution Environment*). Соответственно, аппаратные компоненты системы, обеспечивающие создание такой среды, называются средствами доверенной загрузки (*TSM – Trusted Security Module*). При этом необходимо различать ДСИ, построенные на основе технологий программной виртуализации, т.е. только лишь за счет программного обеспечения, и ДСИ, построенные с использованием аппаратного обеспечения [1, 2].

Сложность создания СДЗ обусловлена необходимостью их функционирования в составе аппаратных платформ иностранного производства, в том числе с учетом их архитектуры в целом, и архитектуры подсистемы защиты в частности.

В работе [3] проведен сравнительный анализ и классификация таких сред. По хронологии появления выделены три группы:

1. *System Management Mode (SMM)* и *Dynamic Root for Measurements (DRTM)*.

2. *Intel Management Engine (ME)*, *AMD Platform Security Processor (PSP)* и *ARM TrustZone*.

3. *Intel Software Guard Extensions (SGX)*.

Технология *System Management Mode*

Принцип технологии *System Management Mode*²¹⁴ основан на следующем:

– передача управления доверенному обработчику осуществляется на основе прерывания *System Management Interrupt (SMI)*;

– адрес обработчика *SMM* недоступен для перезаписи, загружается в специализированный регистр *SMRAM* на этапе работы *BIOS*

– код *SMM* имеет привилегии кольца "ring-2" (рис. 11).

Кольцо 3 (Ring 3)	Пользовательские приложения	Пользовательские приложения (опционально)
Кольцо 0 (Ring 0)	Ядро ОС и драйвера	Ядро ОС и драйвера (опционально)
Кольцо -1 (Ring -1)	Гипервизор (опционально) (<i>Hypervisor</i>)	
Кольцо -2 (Ring -2)	Режим управления системой (<i>System Management Mode</i>)	
Кольцо -3 (Ring -3)	Модуль управления <i>Intel</i> (<i>Intel Management Engine</i>)	

Рис. 11. Уровни привилегий исполняемого кода в процессорах *Intel/AMD*

Технология *Intel ME*

Технология *Intel ME* [4] основана на внедрении микрокомпьютера (рис. 12) в процессоры *Intel*, включая сервера, рабочие станции, ПЭВМ, планшетные компьютеры и смартфоны с уровнем привилегий в кольце "ring-3" (наивысшие). Защищенность ДСИ

²¹⁴ Intel. 64 and IA-32 Architectures Software Developer's Manual / Intel Inc. – URL: <http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html>. – Accessed: 31.10.2019.

обеспечивается использованием области памяти с однократной записью, в которую загружается образ программного обеспечения, целостность и аутентичность которого обеспечивается криптографическими средствами защиты (электронная подпись) [4]. Основная задача – поддержка технологии *Intel Active Management Technology (AMT)* (рис. 13). Необходимо отметить, что известны исследования, когда был успешно внедрен и исполнен произвольный код в режиме работы *Intel ME* [5].

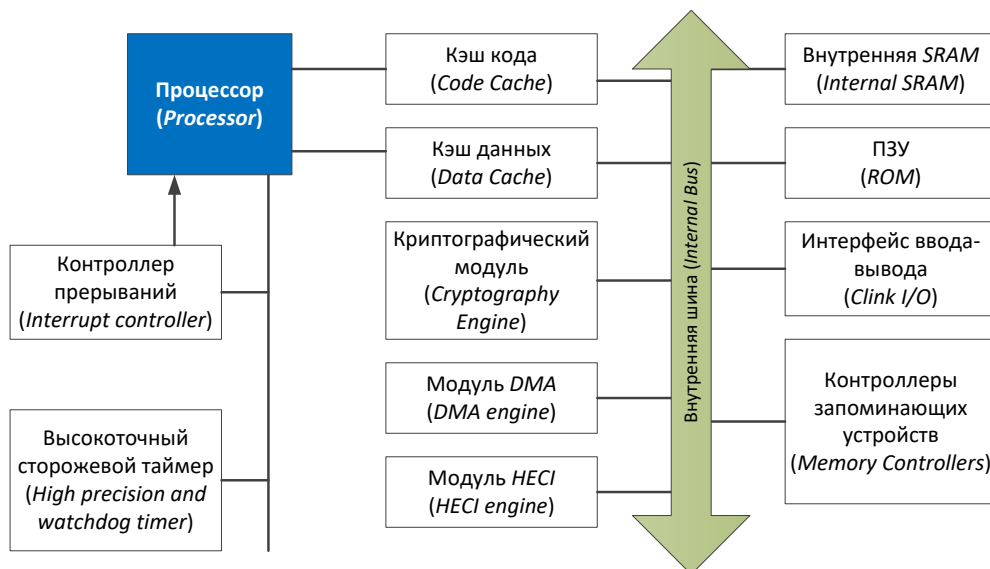


Рис. 12. Архитектура ME-контроллера

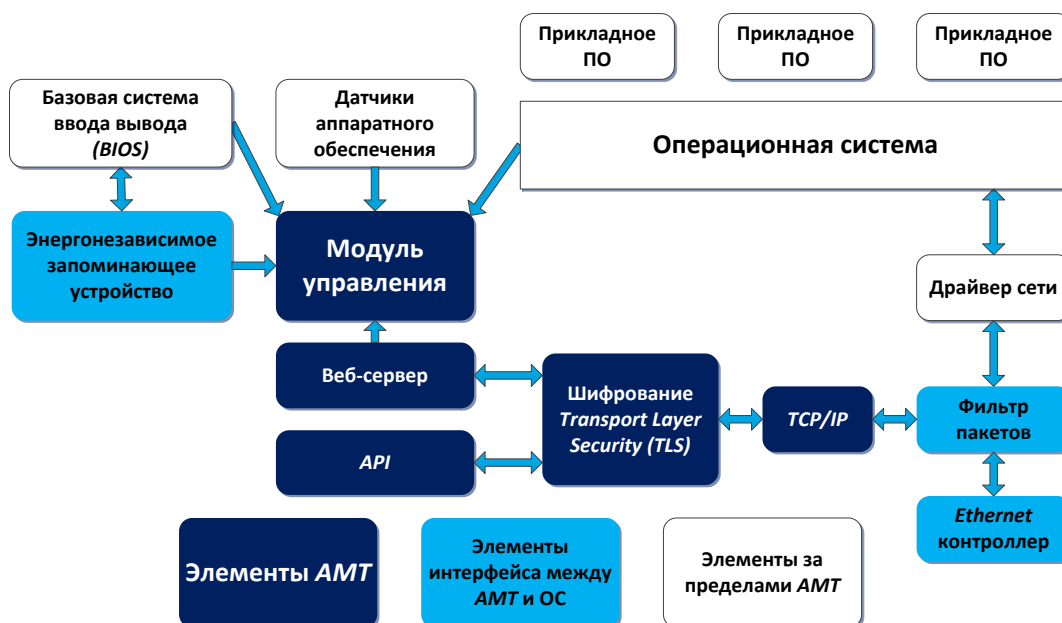


Рис. 13. Концептуальная архитектура Intel Active Management (AMT)

Технология AMD Secure Processor

Данная технология является клоном технологии *Intel ME* в процессорах компании AMD. В отношении СДЗ возможности технологии реализованы в *AMD Secure Processor*²¹⁵,

²¹⁵ AMD TATS BIOS Development Group. AMD Security and Server Innovation. – URL: <http://www.uefi.org/sites/default/files/resources/UEFI PlugFest AMD Security and Server innovation AMD March 2013.pdf>. – 2013. – Accessed: 31.10.2019.

известный также как *Platform Security Processor (PSP)*. По сути, это дополнительный процессор, встроенный в основной *AMD* процессор.

Другим вариантом создания ДСИ на базе *PSP* процессора является технология *System Management Unit (SMU)*²¹⁶, основанная на внедрении в северный мост дополнительного модуля, отвечающего за решение различных системных задач в процессе загрузки и работы ПЭВМ, по сути, являющегося микроконтроллером с собственным процессором. Таким образом, учитывая, что северный мост включен в состав современных процессоров *Intel/AMD*, технология *AMD Secure Processor* на основе *SMU* является аналогом *Intel ME*.

Технология *Dynamic Root of Trust for Measurement (DRTM)*

Технология *DRTM*, также называемая "поздняя загрузка" реализована также в процессорах *Intel* и основана на обеспечении возможности вызова в произвольный момент времени модуля *DRTM*. Такая возможность обеспечивается технологией *Trusted eXecution Technology (TXT)* [6] и специальной инструкцией процессора **SENTER**. Аналогом технологии *Intel TXT* в *AMD* является так называемая защищенная виртуальная машина – *Secure Virtual Machine*²¹⁷, для вызова которой используется инструкция **SKINIT**.

Технология *Intel Software Guard Extensions (SGX)*

Сущность технологии *SGX* [7] заключается в использовании набора инструкций и механизмов доступа к памяти в процессорах *Intel*. Их назначение – в создании специальных защищенных контейнеров (анклавов), используемых как ДСИ и позволяющих обеспечивать целостность и конфиденциальность обрабатываемой информации в условиях отсутствия доверия к *BIOS*, прошивке контроллера, коду гипервизора и операционной системе. Некоторые исследователи считают технологию *SGX* развитием технологии *TXT* [8]. В работе [9] описана платформа *OpenSGX* с открытым исходным текстом, позволяющая эмулировать аппаратные компоненты *Intel SGX* на уровне инструкции модифицированной виртуальной машины *QEMU*, а также продемонстрировано как *OpenSGX* может обеспечивать защиту информации в узлах *Tor*-сети.

Технология *TrustZone*

Технология *TrustZone*²¹⁸ формирует две среды исполнения приложений или так называемых в терминах компании *ARM* "мира". ДСИ на основе *TrustZone* называется в терминологии *ARM* – *Secure World* или *Secure OS*, "недоверенный" – *Rich Execution Environment* или *Rich OS* (*iOS*, *Android*, *Sailfish*, *Tizen*, *Linux*, *Windows* и др.). Порядок загрузки ЭВМ с процессором *ARM* (рис. 14), а взаимодействие режимов ДСИ (*Secure OS*) и гостевой операционной системы (ОС) (*Rich OS*) (рис. 15).

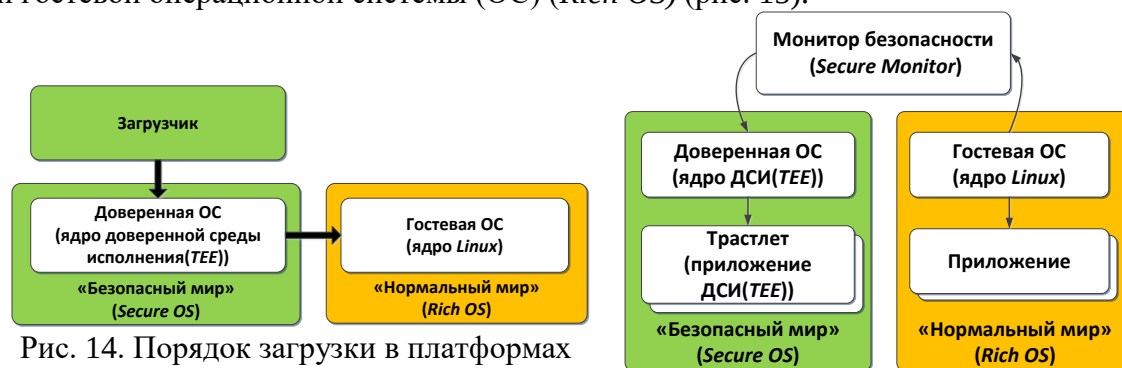


Рис. 14. Порядок загрузки в платформах на основе *ARM*-процессоров

²¹⁶ Intel. Trusted Execution Technology / Intel Inc. – URL: <http://www.intel.com/content/www/us/en/trusted-execution-technology/trusted-execution-technology-security-paper.html>. – Accessed: 31.10.2019.

²¹⁷ Advanced Micro Devices, Inc. AMD64 Architecture Programmer's Manual Volume 2: System Programming. – URL: <http://support.amd.com/TechDocs/24593.pdf>. – 2015. – Accessed: 31.10.2019.

²¹⁸ ARM. ARM Security Technology – Building a Secure System using TrustZone Technology. – URL: http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf. – 2019. – Accessed: 31.10.2019.

Рис. 15. Взаимодействие доверенной
и гостевой ОС

Сущность технологии *TrustZone* заключается в манипулировании режимами работы процессора с помощью сигнала, устанавливаемого битом *NS (Non-Secure)*.

Если *NS=1*, то процессор – в режиме *Non-Secure* (гостевая ОС, или *Rich OS*, или *Normal World OS*), если *NS=0*, то в доверенном, то есть *Secure*-режиме (доверенная ОС или *Trusted OS*, или *Trusted Execution Environment (TEE)*).

Бит *NS* – внешний сигнал, подключенный от процессора почти ко всей периферии. В общем случае периферия к *CPU* подключена шинами адреса, данных и управления. *NS* входит в состав сигналов управления для тех процессоров, где *TrustZone* реализована. Таким образом, от *CPU* к устройству идут не просто команды *Read*, *Write*, а *Secure Read*, *NonSecure Read*, *Secure Write*, *NonSecure Write*.

Отечественные технологии создания доверенных сред исполнения

Процессоры с отечественной архитектурой **ELBRUS (E2K)** производит единственная компания в России – АО "МЦСТ". При этом производство развернуто на Тайване (фаблесс бизнес-модель).

Компания "Байкал Электроникс" – дочерняя компания ОАО "Т-Платформы" производит процессоры с архитектурой *ARMv8 – Baikal*.

Таким образом, собственная отечественная архитектура есть только у компании АО "МЦСТ" – **ELBRUS**.

В августе 2019 года компанией ЗАО "Аладдин Р.Д." сертифицирован модуль "Аладдин *TSM*"²¹⁹, основанный на использовании технологии *TrustZone*, по требованиям ФСТЭК "Требования к средствам доверенной загрузки" и профилю защиты "ИТ.СДЗ.УБ2.ПЗ", что позволяет использовать его в отечественных технических решениях по реализации СЗИ на объектах критической информационной инфраструктуры (КИИ), в информационных системах персональных данных (ИСПДн) и государственных информационных системах. Модуль "Аладдин *TSM*" основан на процессорах *ARM NXP/Freescale i.MX6* и программном обеспечении, сертифицированном по 2-му классу доверия. Поддерживаются процессоры *NXP i.MX6 Solo*, *Dual*, *DualLite*, *Quad*, а также *UltraLite* и *ULL*.

Технология даёт возможности "перепрошивать" современные импортные ARM-процессоры [10-12] (только для линейки *i.MX6*), загружая в их *TrustZone* российскую доверенную *Secure OS* с необходимыми функциями защиты.

Выводы

На современном этапе развития элементной базы и технологий создания СДЗ реализованы различные подходы, позволяющие обеспечить доверенный режим функционирования СЗИ и средств ее обработки. Однако отечественные наработки в этой области значительно отстают от иностранной и требуют совершенствования существующих подходов по применению встраиваемых на аппаратном уровне компонентов, обеспечивающих создания среды доверенного исполнения.

Литература

1. Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. № 1 (14). С. 24-30.
2. Гефнер И.С., Марков А.С. Механизмы реализации атак на уровне базовой системы ввода/вывода // Защита информации. Инсайд. 2017. № 5 (77). С. 80-83.

²¹⁹ Доверенная платформа для процессоров ARM // ЗАО "Аладдин Р.Д.". – Режим доступа: <https://www.aladdin-rd.ru/catalog/tsm>. – Дата обращения: 24.09.2019.

3. Fengwei Zhang SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security / Fengwei Zhang // HASP, 2016 (june 18). – 2016. – p. 8.
4. Ruan, X. Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine / X. Ruan. – Apress. – 2014.
5. Wojtczuk, R. Introducing Ring-3 Rootkits. / R. Wojtczuk, A. Tereshkin. – URL: <http://invisiblethingslab.com/itl/Resources.html>. – 2009. – Accessed: 31.10.2019.
6. Marek, R. AMD x86 SMU Firmware analysis - Do you care about Matroshka processors? – URL: <https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2503/original/ccc-final.pdf>. – 2014. – Accessed: 31.10.2019.
7. Mckeen, F. Innovative Instructions and Software Model for Isolated Execution / F. Mckeen, I. Alexandrovich, A. Berenzon, C. Rozas, H. Shafi, V. Shanbhogue, U. Savagaonkar // in Proceedings of the 2nd Workshop on Hardware and Architectural Support for Security and Privacy (HASP'13), 2013.
8. Costan, V. Intel SGX Explained / V. Costan, S. Devadas. – URL: <https://eprint.iacr.org/2016/086.pdf>. – 2016. – Accessed: 31.10.2019.
9. Jain, P. OpenSGX: An Open Platform for SGX Research / P. Jain, S. Desai, S. Kim, M.-W. Shih, J. Lee, C. Choi, Y. Shin, T. Kim, B. B. Kang, D. Han. // in Proceedings of the 2016 Annual Network and Distributed System Security Symposium (NDSS'16), San Diego, CA (feb. 2016). – 2016.
10. Волков, А. TrustZone: доверенная ОС и ее приложения // Блог компании Аладдин Р.Д. – Режим доступа: <https://habr.com/ru/company/aladdinrd/blog/428311/>. – Дата обращения: 24.09.2019.
11. Волков, А. Программирование под ARM TrustZone. Secure Monitor // Блог компании Аладдин Р.Д. – Режим доступа: <https://habr.com/ru/company/aladdinrd/blog/342924/>. Дата обращения: – 24.09.2019.
12. Волков, А. TrustZone: аппаратная реализация в ARMv7A // Блог компании Аладдин Р.Д. – Режим доступа: <https://habr.com/ru/company/aladdinrd/blog/340912/>. – Дата обращения: 24.09.2019.

Actual Trusted Execution Environment Technologies Based on Basic Input-Output System

Markin D. O.²²⁰, Umbetov T. K.²²¹, Arkhipov M. A.²²², Minachev V. M.²²³

Abstract. *The work is devoted to the trust problems of foreign-made firmware platforms and how to solve these problems using trusted runtimes. The authors present the analysis of legislation requirements for on computer systems protection based on trusted boot technologies. The work contains investigation of the modern technologies implementation features for building trusted application runtimes used at the level of the basic input-output system. The main problems of trust in modern software and hardware platforms of foreign production are formulated. The authors formulated main trust problems of foreign software and hardware platforms. Conclusions and development directions based on the analysis results are formulated.*

Keywords: *trusted boot, trustzone, ARM, TEE, TSM, BIOS.*

²²⁰ Dmitry Markin, candidate of technical sciences, The Academy of Federal Security Guard Service of the Russian Federation, Oryol, mdu@academ.msk.rsnet.ru

²²¹ Timur Umbetov, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

²²² Mihail Arkhipov, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

²²³ Vladislav Minachev, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

Эмулирование сети как метод исследования уязвимостей на примере протокола междоменной маршрутизации BGP

Маркова И.А.²²⁴

Аннотация: в данной статье рассмотрен принцип работы протокола междоменной маршрутизации BGP, проанализированы уязвимости данного протокола для конечных пользователей, представлена структура лабораторного стенда для эмуляции работы сети организации.

Ключевые слова: Border Gateway Protocol, уязвимость, маршрут, сеть, «угон» адресов, «человек посередине», виртуальные сети, лаборатория, эмуляция.

Введение

В связи с постоянным развитием технологий высокоскоростного доступа сети Интернет одной из основных тенденций является рост количества и сложности атак на сетевую инфраструктуру. На сегодняшний день BGP, как и DNS, является одним из главных механизмов, обеспечивающих функционирование Интернета. Дефектные, некорректно настроенные или преднамеренно искаженные источники маршрутной информации могут внести существенные искажения в работу сети Интернет путем вставки ложной информации в распространяемые базы маршрутных данных. Источниками ложной информации могут служить как внешние хосты, так и проверенные партнеры.

В настоящее время в сети насчитывается более 700 000 маршрутов и протокол BGP постоянно следит за актуальностью всех маршрутов. Обеспечивать безопасность такой топологии очень проблематично. Если внутри автономной системы администраторы следуют единой политики безопасности, то контролировать соседнюю автономную систему невозможно. При необходимости соединения с другой автономной системой встает вопрос о ее безопасности: не подвергалась ли она взломам или не «сливает» ли данные конкурентам [1-2]. Даже крупные провайдеры не застрахованы от «утечек» маршрутов.

Так, 28 апреля 2017 года сервис BGPmon, отслеживающий информацию о маршрутах следования интернет-трафика по всему миру, сообщил о «множественных аномалиях» в работе сети ПАО «Ростелеком». По предоставленным данным, «Ростелеком» осуществил «BGP-перехват», то есть проанонсировал по всей сети Интернет ложные данные о маршрутизации до некоторых интернет-ресурсах. Такими оказались сайты Visa, MasterCard, Norvik Banka, Приватбанк, Альфа-банк, HSBC, Федеральная служба охраны РФ, РосНИИИРОС и др. В результате, сайты на какое-то время были недоступны для клиентов ПАО «Ростелеком» и, возможно, для клиентов других провайдеров.

Другой яркий пример случился в 2010 году. Pakistan Telecom, получив от властей указание заблокировать YouTube, добавил соответствующий маршрут и начал анонсировать его другим провайдерам, в результате чего трафик большинства абонентов по всему миру стал перенаправляться в Пакистан и YouTube оказался для них недоступен.

На рис.1 представлено количество пострадавших автономных систем за 2016 год. Из графика видно, что пиковые значения поражений достигают более 9000 инцидентов.

²²⁴ Маркова Ирина Александровна, МГТУ им. Н.Э. Баумана, Москва, gurina.irina.94@gmail.com

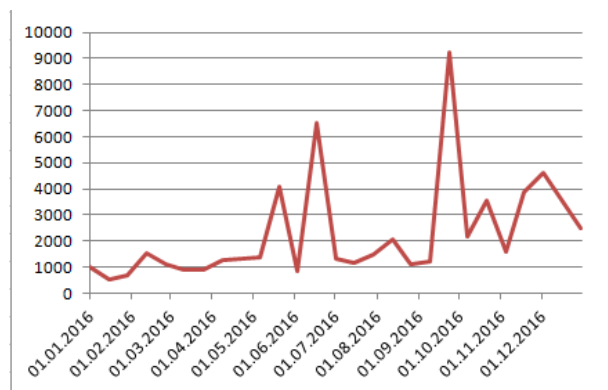


Рис.1

пострадавших автономных систем

Количество

Криптографическая защита TCPMD5 и защита устройств не позволяют исключить ложную информацию, полученную от легитимного соседа. Сами узлы могут включать ложные маршруты, выдавая себя за другой легитимный узел или рассылать маршрутную информацию от своего имени без должных на то полномочий. Риск нарушений, вызываемых легитимными соседями BGP, является реальным и должен приниматься во внимание [3].

Протокол междоменной маршрутизации BGP

Протокол BGP (Border Gateway Protocol) - основной протокол обмена маршрутной информацией между автономными системами Интернета. Автономная система — это группа маршрутизаторов, находящаяся под единым техническим управлением. Внутри автономной системы работают внутренние протоколы маршрутизации, а связь между автономными системами обеспечивается внешним протоколом маршрутизации BGP (рис.2) [3].

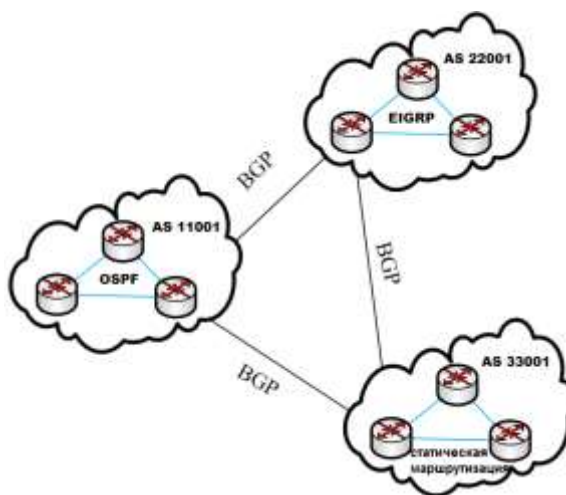


Рис.2. Схема

BGP

работы протокола

Вместе с маршрутной информацией так же передаются и различные атрибуты, с помощью которых протокол BGP выбирает наилучший маршрут и настраивает свои политики маршрутизации.

Один из основных атрибутов, который передается с информацией о маршруте — это список автономных систем, через которые прошла эта информация [4]. Эта информация позволяет BGP определить, где находится сеть относительно автономных систем,

исключить петли маршрутизации, а также может быть использована при настройке политик.

Маршрутизация осуществляется пошагово от одной автономной системы к другой. Все политики BGP настраиваются, в основном, по отношению к внешним (соседним) автономным системам. То есть, описываются правила взаимодействия с ними.

Ложные маршрутные данные могут оказывать различное влияние на картину маршрутизации. В таблице 1 представлены последствия ложной маршрутизации.

Таблица 1.

Неисправности сети в результате нарушения маршрутизации

№ п/п	Тип нарушения	Действия, происходящие в сети
1.	потеря пакетов	трафик, предназначенный для абонента, пересылается в ту часть сети, которая не может его доставить
2.	перегрузка	через определенный участок сети пересылается трафик больше, чем эта сеть способна обработать
3.	«черная дыра»	весь трафик направляется для пересылки через маршрутизатор, который не способен справиться с возросшим уровнем трафика и будет отбрасывать часть или весь трафик
4.	задержка	преднамеренное увеличение хостов в маршруте сети
5.	петли	данные передаются по замкнутому пути и удаляются по истечении времени жизни пакета, так и не достигнув абонента
6.	перехват	данные пересылаются через нелегитимный узел или сеть, которые не должны получать эти данные; данные при такой пересылке могут просматриваться
7.	отключение или разделение сети	некоторые части сети кажутся отрезанными, хотя на самом деле реально подключены
8.	нестабильность	не удастся достичь схождения картины маршрутов в связи с нестабильной работой протокола BGP

Виды атак на протокол BGP

BGP HiJacking – это случайный или преднамеренный захват чужих IP-адресов. В классическом виде, эта атака выглядит как анонс чужого префикса автономной системой, к которой он не принадлежит. Соседи нарушающей автономной системы принимают его и начинают распространять в сети Интернет. Одной из причин анонсирования является то, что отсутствует фильтрация на стыке автономных систем (либо это ошибка конфигурации, либо халатное отношение провайдеров).

MiTM – атака или атака «человек посередине» в BGP используется злоумышленниками для прослушки чужого трафика. Для жертвы это может оказаться совершенно незаметно: трафик проходит через узел злоумышленника и направляется в пункт назначения по измененному маршруту. Если нарушитель находится физически между адресатами, то жертва даже не заметит увеличения задержки в пакетах из-за изменения маршрута следования пакетов [5-6].

Стенд виртуальной сетевой инфраструктуры

В связи со сложностью построения большой топологии сети из реального оборудования на помощь инженерам приходят среды эмулирования сети. Такое программное обеспечение становится прекрасной лабораторной средой, позволяя моделировать сети любой сложности [7-10]. На рис.3 изображена исследуемая топология сети предприятия,

включающая в себя сети головного офиса «AS 11001», сети филиалов «AS 33001», «AS 44001» и «AS 44101», сеть провайдера «AS 11111» и сеть злоумышленника «AS 27001».

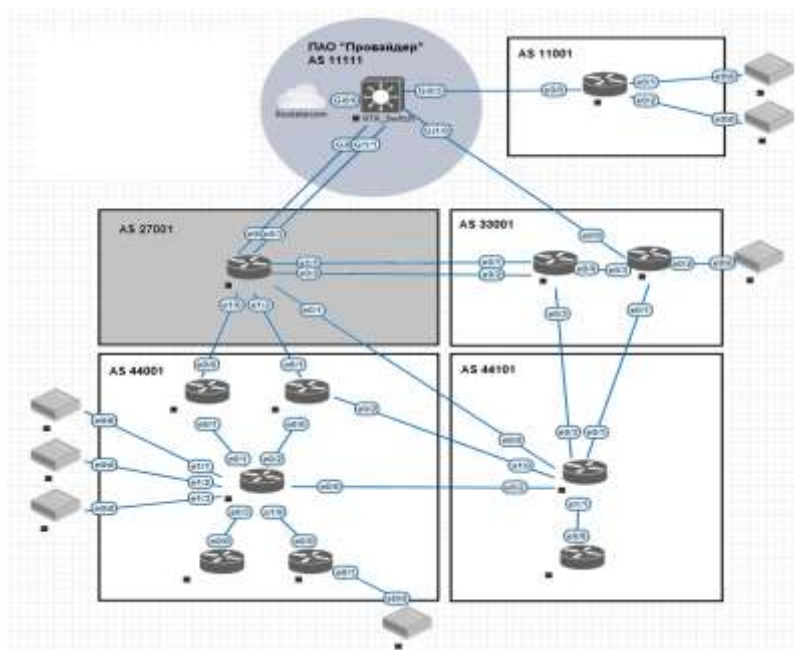


Рис. 3 Схема исследуемой сети, построенной на основе протокола BGP

На рис.4 и рис.5 показаны результаты реализации MiTM-атаки. Из результатов видно, что при совершении атаки изменяется маршрут следования пакетов. Из-за прохождения нелегитимных узлов также увеличивается и время ICMP-ответа от опрашиваемых устройств.

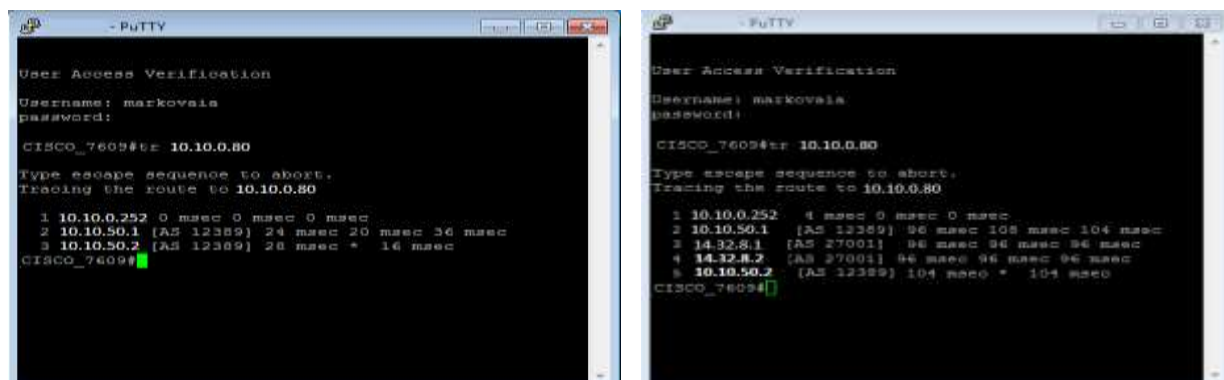


Рис. 4 Трассировка маршрута от AS 11001 до AS 33001

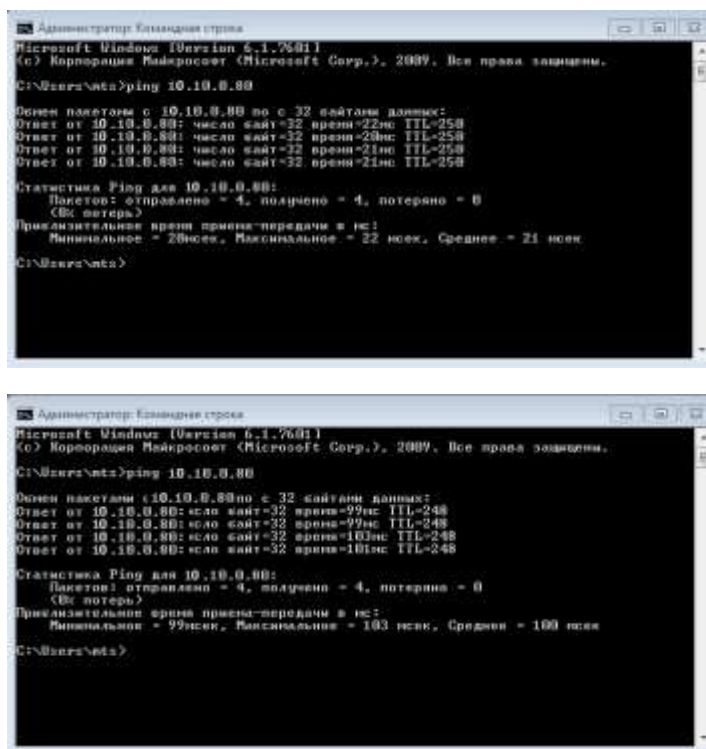


Рис. 5 Результаты ICMP запроса к AS 33001

Вывод

В данной статье был рассмотрен основной принцип работы протокола BGP, описаны нарушения работы в сети при атаках и уязвимости данного протокола. Так же был представлен лабораторный стенд виртуальной сетевой инфраструктуры предприятия и результаты успешно реализованной MiTM-атаки. С помощью технологий эмуляции сетей стало возможно исследовать уязвимости проектируемых топологий без колоссальных затрат на создание лабораторных стендов из реального оборудования. Это увеличивает эффективность применения средств защиты информации уже на этапе планирования топологии сети, увеличивая показатели защищенности и исключая затраты на приобретение неэффективных средств защиты.

Литература

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2017. 992 с.
2. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.
3. Желенков Б.В. Маршрутизация в глобальных сетях. Протокол BGP. М.: МИИТ, 2011. 182 с.
4. Нечаев А.Н., Авербах В.С. Особенности функционирования и основные свойства протокола динамической маршрутизации BGP // Известия института систем управления СГЭУ. 2017. №1 (2). С. 255-258.
5. Козачок А.В. Обеспечение безопасности BGP // Информация и безопасность. 2014. №4 (14). С 553-560.

6. Пирогов Н.С. Оценка уязвимостей протокола BGP // Инновации в науке. 2018. №12(88). С. 16-18.
7. Басков А. А. Сеть и виртуализация. Часть II // Журнал сетевых решений LAN. 2013. №4. С. 25-60.
8. Панфилов К.В. Система виртуализации EVE-NG // Форум молодых ученых. 2018. №2(30). С. 1149-1151.
9. Тарасов Я.В., Макаревич О.Б. Моделирование и исследование низкоуровневых DOS-атак на BGP-инфраструктуру // Известия ЮФУ. Технические науки. 2013. №12 (149). С. 101-111.
10. Ахмедзянова Р.Р. Задачи исследования проектирования центров обработки данных (ЦОД) для массового обучения IT-специалистов // Наука и образование: новое время. 2017. №4. С. 256-259.

Научный руководитель Быков Александр Юрьевич, к.т.н., доцент, МГТУ им. Баумана, Москва, abykov@bmstu.ru

Network emulation as a method of vulnerability research on the example of the cross-domain routing Protocol BGP

Markova I. A.²²⁵

Abstract: *this article describes the principle of operation of Protocol BGP, analyzes the vulnerabilities of this Protocol for users, and presents the structure of the laboratory stand for emulation of the network.*

Keywords: *Border Gateway Protocol, vulnerability, route, network, hijacking, "man in the middle", virtual networks, laboratory, emulation.*

²²⁵ Irina Markova, MSTU, Moscow, gurina.irina.94@gmail.com

Метод защиты персональных данных в «ЕНР – электронная медицинская книжка»

Марченко А.В.²²⁶

В данной работе разработан и описан метод защиты персональных медицинских данных пациента, позволяющий повысить их стойкость к компрометации за счёт комбинированного использования алгоритмов шифрования SHA-256 и AES-256. Шифрование персональных медицинских данных пациента производится с использованием уникального ключа пациента, который создаётся на этапе регистрации для каждого пациента с помощью алгоритма вычисления контрольных сумм персональных данных.

Ключевые слова: метод, защита, персональные, данные

Введение

В век информационных технологий одним из самых ценных объектов является информация. Она обладает свойствами товара: создаётся, обновляется, продаётся и покупается. Ценность информации зависит от её уникальности и полезности, другим словами, если файл содержит в себе описание и принцип создания лазерного оружия и существует в рамках узкого круга лиц, он имеет высокую ценность, с каждой покупкой его ценность уменьшается, так как увеличивается число его владельцев.

К сожалению, наравне с обычными рынками существуют и «чёрные», на которых покупаются и продаются персональные данные, конфиденциальная и секретная информация [1]. Основными потребителями данного рынка являются следующие лица:

- конкуренты, покупающие и продающие информацию о конкурирующих организациях;
- лица, приобретающие информацию о банковских картах, занимающиеся изготовлением банковских карт и их обналичиваем (кардеры) [2];
- рекламные компании для «холодных звонков»;
- лица, покупающие медицинские данные;
- и другие.

Персональные данные

Среди товаров персональных данных наиболее ценной является информация, связанная со здоровьем человека. Анализ данной информации позволяет злоумышленнику шантажировать [3] потенциальную жертву для получения выгоды, заключения более выгодных соглашений, партнёрстве и т.д.

Информационные товары на чёрном рынке появляются в результате утечек информации, которые возникают по причине халатности и невыполнения требований федеральных законов: «О персональных данных» [4], «Об информации, информационных технологиях и о защите информации» [5], а также других положений и приказов регуляторов.

Нередко наблюдается в медицинских учреждениях потеря медицинской амбулаторной карты, неправильная утилизация самих амбулаторных медицинских карт, которая производится обычным выбросом на свалку, а также незашифрованные данные в базах данных медицинского учреждения.

Метод комбинированного использования алгоритмов шифрования

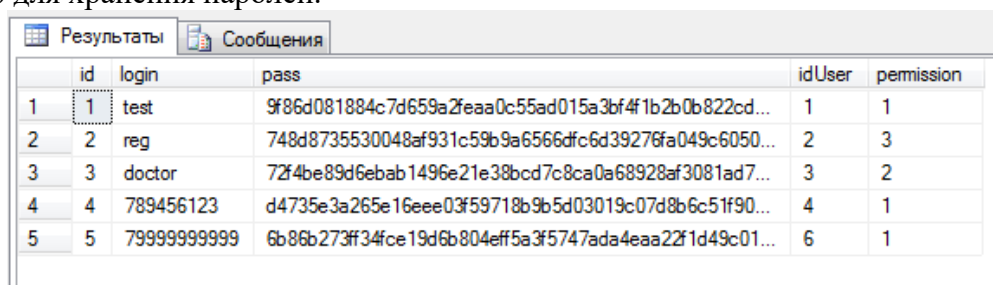
²²⁶ Марченко Антон Васильевич, студент, МГТУ им. Н.Э. Баумана, Москва, mart0n@mail.ru

Для предотвращения компрометации медицинских персональных данных необходимо:

- 1) выполнять рекомендации, предложенные автором М. А. Никитиным, в статье «Обработка персональных данных в информационных системах персональных данных медицинских учреждений» [6], которые разработаны, согласно федеральным законам и приказам регуляторов, относящимся к персональным данным;
- 2) Шифровать данные в базе данных.

В первую очередь необходимо понимать, что не существует не взламываемых систем, любая защита направлена на время, которое злоумышленник должен затратить, чтобы получить данные. Использование ключа размером 256 бит позволит очень сильно увеличить время грубого перебора (bruteforce). Для понимания число возможных комбинаций будет длиной 78 знаков. Ни один компьютер в мире не способен перебрать такое количество вариантов. Однако, стоит помнить, что если ключ будет потерян, то риск потери данных возрастёт.

В автоматизированной информационной системе «EHR – электронная медицинская книжка используется комбинация алгоритмов шифрования SHA-256 [7] для создания хэш-функций пароля. На рисунке 1 приведён пример использования и реализации алгоритма SHA-256 для хранения паролей.



	id	login	pass	idUser	permission
1	1	test	9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd...	1	1
2	2	reg	748d8735530048af931c59b9a6566dfc6d39276fa049c6050...	2	3
3	3	doctor	72f4be89d6ebab1496e21e38bcd7c8ca0a68928af3081ad7...	3	2
4	4	789456123	d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90...	4	1
5	5	79999999999	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01...	6	1

Рисунок 1 – Результат применения SHA-256

Преимущество использования хэш-алгоритмов в том, что они не имеют функции расшифрования, а аутентификация [9] пользователей происходит при помощи сравнения хэшей между собой. Порядок работы функции сравнения следующий: пользователь вводит логин и пароль, если пользователь прошёл первичную проверку на логин (существование данного пользователя в системе), то происходит переход на создание хэш введенного пользователем пароля и сравнение его с тем, который храниться в базе данных.

Для шифрования данных пациентов первоначально генерируется уникальный ключ пользователя с помощью алгоритма вычисления контрольных сумм персональных данных. После чего с помощью данного ключа происходит шифрование только его данных с использованием алгоритма AES-256. Если база данных будет скомпрометирована, то время её расшифрования будет стремиться к бесконечности.

Для наглядности на рисунке 2 представлен результат, как выглядят открытые данные и зашифрованные данные.

Результаты		Сообщения	
id	FName	LName	OName
1	Григорий	Григорьев	Григорьевич
2	Илья	Ильин	Ильин
3	Павел	Павленков	Павленкович
4	Иванов	Иванов	Иванович
5	Петр	Петров	Петрович
6	Антон	Antonov	Antonovich
7	Петр	Петров	Петрович
8	Алексей	Алексеев	Алексеевич
9	Анастасия	Настасьева	Анастасьевна
10	Ольга	Александрова	Павловна
11	12	71+110+102+85+21+12+221+212+68+159+83+250+1+118+...	127+181+123+189+20+197+41+154+123+236+40+181+250... 44+150+150+26+158+179+161+142+67+143+147+136+13...

Рисунок 2 – Открытые и зашифрованные данные

Симметричное шифрование AES-256 выбрано не случайно, для работы в системе необходима процедура расшифрования для того, чтобы пользователи с правами регистратор и врач могли видеть информацию о пациенте. В силу того, что .NET Framework 4.0 на котором ведётся разработка, есть встроенная поддержка AES, что позволяет, на данный момент, сократить время разработки и отладки в разы.

Стоит отметить, что выбор генерации уникального ключа имеет свои недостатки, в силу потенциальной известности всех персональных данных пациента, снижает криптостойкость [10] шифрования.

Существует альтернативный вариант, который способен решить эту проблему, если генерировать уникальный ключ алгоритмом псевдослучайных чисел и их выдавать пациентам в виде физических носителей. При таком решении доступ к данным пациентам будет осуществляться только при их физическом присутствии, что несёт в себе неудобство для персонала и медицинского учреждения в целом. Поэтому на данный момент продолжается поиск эталонного варианта и варианты повышения криптостойкости шифрования.

Вывод

В рамках проделанной работы была решена одна из главных задач по защите персональных медицинских данных пациента в амбулаторной карте благодаря комбинированному использованию криптоалгоритмов SHA-256 и AES-256. Благодаря использованию шифрования количество снизится динамика утечек медицинских данных. Данный метод можно использовать не только в области защиты медицинских данных, но и данных в целом, используя как предложенные алгоритмы шифрования, так и другие. В дальнейшем планируется внедрение отечественного блочного шифра «Магма» ГОСТ 34.12—2015 взамен AES-256.

Литература

1. Вардanian М.В. Черный рынок в экономике // Российское общество и экономика: исторический опыт и современность. 2017. С. 27-28.
2. Артеменко Н.А. Кардинг как вид мошеннической деятельности // Гуманитарные, социально-экономические и общественные науки. 2018. № 8. С. 77-80.
3. Никитин Ю.А. Объективная сторона шантажа как разновидности вымогательства // Библиотека уголовного права и криминологии. 2016. № 3 (15). С. 40-43.
4. Барановский С.Л., Трофимова О.М. Федеральный закон "О персональных данных" как регулятор структуры базы данных // Государство, политика, социум: вызовы и стратегические приоритеты развития. 2017. С. 213-215.

5. Шакалов М.С. Система защиты персональных данных при их обработке в информационной системе персональных данных // Педагогическое образование на Алтае. 2014. № 2. С. 453-454.
6. Никитин М.А. «Обработка персональных данных в информационных системах персональных данных медицинских учреждений» // Управление качеством медицинской помощи. 2014. № 1. С. 17-21.
7. Коренева А.М. Оценка характеристик перемешивания хэш-функций семейства MD. // Прикладная дискретная математика. Приложение. 2019. № 12. С. 107-110.
8. Cui J., Zhao K., Xie Z. Algebraic cryptanalysis scheme of aes-256 using gröbner basis. // Journal of electrical and computer engineering. 2017.
9. Жуков И.Ю., Мурашев О.Н. Защищенные процедуры взаимной аутентификации, формирования ключа фискального признака и защиты фискальных данных // Безопасность информационных технологий. № 25 (2). 2018. С. 63-70.
10. Гридин В.Н. Солодовников В.И. Исследование вопросов криптостойкости и методов криптоанализа нейросетевого алгоритма симметричного шифрования.

Научный руководитель или консультант: Веселов Юрий Геннадьевич, доцент, д-р техн. наук, преподаватель МГТУ им. Н. Э. Баумана, vesel_foto@mail.ru.

The method of protecting personal data in "EHR - electronic medical book" **Marchenko A.V.²²⁷**

Abstract. *In this work it is developed and described a method of protecting patients' personal medical data, which allows to increase its resistance to compromise due to the combined use of SHA-256 and AES-256 encryption algorithms. The patient's personal medical data is encrypted with using a unique patient key, which is created at the registration stage for each patient. The patient key is created with the help of the algorithm for calculating personal data checksums.*

Keywords: *method, security, personal, date*

²²⁷ Anton Marchenko, student, BMSTU, Moscow, mart0n@mail.ru

Применение средств поиска ключевых слов в слитной речи в DLP-системах

Мессерле А.А.²²⁸

В данной работе кратко рассмотрены перспективы использования средства поиска ключевых слов в слитной речи в системах предотвращения утечек информации (англ. Data Loss Prevention - DLP). Сделан обзор основных возможностей основных DLP-систем (по состоянию на конец 2017 года) по обработке речевых сигналов. Предложено использование систем поиска ключевых слов в слитной речи, которые могут существенно улучшить функциональность DLP-систем в области обработки речи, в том числе обеспечив распознавание ключевых слов в изолированных от сети интернет системах.

Ключевые слова: цифровая обработка речевых сигналов, информационная безопасность.

Введение

В современных условиях всё больше организаций уделяют внимание защите коммерчески значимой информации, например данных о договорах, персональных данных. Наиболее эффективным способом осуществления контроля за сотрудниками является внедрение систем защиты от утечек информации, или DLP-систем. Рассмотрим основные DLP-системы и системы контроля сотрудников, представленные на российском рынке в 2017 году с позиции оценки функционала в области перехвата (записи) и обработки речевых сигналов. Следует отметить, что в настоящее время социальные сети и мессенджеры (возможные каналы утечки информации [1, 2]) также позволяют обмениваться голосовыми сообщениями, причём данная технология набирает популярность.

Обзор DLP-систем с возможностью записи и анализа речевых сигналов

Ниже представлен краткий обзор основных DLP-систем (или их отдельных модулей) и систем контроля сотрудников, представленных на отечественном рынке, обладающих функционалом по работе с речевыми данными:

- КИБ СёрчИнформ. Имеет модуль SearchInform MicrophoneController, который позволяет записывать звук с рабочей станции пользователя с использованием любого доступного микрофона, в том числе с возможностью прослушивания в реальном времени. Имеются алгоритмы определения голосовой активности, подавления шума.
- StaffCop Enterprise. Позволяет записывать окружение с микрофона компьютера, автоматическое выключение при отсутствии звука.
- Zecurion Staff Control. Имеется возможность записи звука с микрофона и разговоров через VoIP. **Ошибка! Источник ссылки не найден..**
- Falcongaze SecureTower. Встроена функция аудио-мониторинга рабочего места.
- InfoWatch Traffic Monitor. В сотрудничестве с компанией «Центр Речевых Технологий» (система мониторинга голосового канала STC Voice Monitor), решение позволяет записывать голосовой трафик (например, при проведении видеоконференций, переговорах по Skype) с последующим преобразованием речи в текст и поиска в нём характерных ключевых слов по заранее настроенным политикам безопасности.

²²⁸ Мессерле Александр Алексеевич, соискатель, МГТУ им. Н.Э. Баумана, г. Москва, e-mail: nayca@mail.ru
 Консультант: Горшков Юрий Георгиевич, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э.Баумана, канд. техн. наук, доцент, e-mail: y.gorshkov@npo-echelon.ru

- «Стахановец» Голосовое DLP (также InfoWatch Person Monitor – тот же продукт, продаваемый под брендом InfoWatch). Система имеет возможность моментального реагирования на ключевые фразы (в основе лежит распознавание речи), записанных с микрофона компьютера или перехваченных в мессенджерах, ведение расшифровки переговоров и сохранение результатов распознавания речи в текстовые файлы.

В большинстве перечисленных систем имеется возможность прослушивания полученных записей и поиска записей по косвенным признакам (время записи, сотрудник и т. д.).

Тем не менее, очевидно, что при большом количестве записей:

- а) Отсутствует возможность качественного анализа, кроме как прослушивание оператором (представителем отдела безопасности) архива всех аудиозаписей или необходимость личного присутствия при прослушивании в режиме реального времени;
- б) Использование сервисов по распознаванию речи сопряжено с трудностями, возникающими при отправке записей на обработку (при использовании онлайн-сервисов – затраты на передачу данных, вопросы конфиденциальности) или при их анализе непосредственно внутри организации (дополнительные затраты вычислительных мощностей или невозможность автономной работы технологий распознавания речи без доступа к сети Интернет).

В таких условиях представляется рациональным сократить затраты человеческого труда и минимизировать потребляемые производственные мощности (при обеспечении конфиденциальности обработки полученной информации). В данном случае компромиссом может послужить средство поиска ключевых слов в слитной речи.

Средства поиска ключевых слов в слитной речи

Технология поиска ключевых слов в речи (англ. Speech Key-Word Spotting - KWS) позволяет существенно облегчить труд оператора при поиске информации среди множества аудиозаписей. Сущность технологии заключается в поиске только заранее предопределённых ключевых слов непосредственно в аудиоданных. Для реализации подхода не требуется переводить речь в текст, а необходимо создание небольшого словаря, содержащего несколько образцов звучания для каждого ключевого слова, подлежащего отслеживанию в соответствии с принятой политикой безопасности организации.

Средство поиска ключевых слов может быть как программным, так и программно-аппаратным решением. Одним из преимуществ средств поиска ключевых слов является возможность работы в автономном режиме (в том числе на изолированных сегментах внутренней сети организации). На конец 2017 года существует несколько систем поиска ключевых слов в речи (в том числе с возможностью анализа речи в режиме реального времени) с поддержкой русского языка. К таким системам можно отнести:

- 1) Продукция компании ООО «Центр Речевых Технологий» (ЦРТ):

- а) Модуль поиска ключевых слов в составе коммерческой системы многоканальной записи, регистрации и архивирования звуковых сигналов Незабудка II.

Данная технология является в определённой мере дикторозависимой и обладает правильностью распознавания почти в 80%. Основа алгоритма – распознавание через синтез.

- б) Система поиска информации в аудиозаписях по ключевым словам Voice Digger и настольное решение Voice Digger Swift. Данное программное обеспечение, судя по заявленным характеристикам, верно находит слово в 85-90% случаев. Основа ПО – скрытые Марковские модели, появилось в 2008 году. Скорость работы составляет около 1 секунды на 6 секунд звучания аудиофайла.

в) Система управления качеством и автоматизации работы контактного центра Speech Analytics Lab. Система работает по фонограммам звонков, основа работы – распознавание речи на большом словаре с последующим кластерным анализом данных.

Следует отметить, что данные решения созданы отечественной компанией и соответственно заточены под русский язык, однако существует возможность добавления любого другого языка.

2) Вторая система поиска ключевых слов в аудиозаписях – ANALYZE от компании Speech Drive, появилась в 2012 году. Точные характеристики продукции не указываются, зато отмечается наличие таких клиентов, как Сбербанк и Ростелеком; основой ПО [3] является CMU Sphinx (см. п. 4)).

3) Комплекс программных средств (КПС) «Голос», компания «Стэл – Компьютерные Системы» [4-6]. Комплекс позволяет в поточном режиме определять появление важных ключевых слов и словосочетаний на 7 языках, границы начала и конца слова выделяются. Комплекс поддерживает поиск 1000 слов одновременно. Основа – речевые модели языка (распознавание слитной речи с большим словарём), фонемный распознаватель. Скорость обработки составляет: в программной реализации 8 минут речи обрабатываются за минуту, а при аппаратной реализации на графических процессорах за одну минуту может быть обработано до 50 минут речи (при словаре до 2000 ключевых слов).

4) Комплекс свободного программного обеспечения CMU Sphinx (англ. Carnegie Mellon University, университет Карнеги Меллон, США под лицензией BSD (англ. Berkeley Software Distribution license — программная лицензия университета Беркли) для распознавания речи, в частности Pocketsphinx – библиотека распознавания, написанная на языке C. Основа алгоритма – скрытые Марковские модели (с использованием объёмных словарей и языковых моделей). Поскольку разработка и поддержка ведётся сообществом и энтузиастами, в том числе создание и модификации языковых моделей, то существует несколько неисчерпывающих словарей и звуковых моделей для русского языка. Разумеется, качество таких моделей оставляет желать лучшего, однако при определённых ограничениях можно добиться достаточно высокого быстродействия и качества работы.

5) Kaldi – написанный на языке C++ комплекс программного обеспечения под лицензией Apache License v2.0, предназначенный для исследователей речи. Разрабатывается и поддерживается несколькими разработчиками из разных организаций, содержит возможности поиска ключевых слов. Основа – распознавание речи на большом словаре.

6) Множество исследовательских и иных (в том числе на основе свободного ПО) приложений, разработанных в различных университетах и организациях по всему миру с целью изучения технологий поиска ключевых слов в речи (напр. [7, 8]), а также коммерческие продукты (напр. от компании Phonexia).

Отмечается, что построение системы полного распознавания речи для русского языка – очень тяжёлая задача, которая не может быть полностью решена без задействования больших вычислительных затрат и затрат на обучение такой системы. Для обучения средства поиска ключевых слов новому слову, в общем случае, достаточно потратить несколько минут.

Выводы

Внедрение возможностей систем поиска ключевых слов в речи в представленные на отечественном рынке DLP-системы позволит эффективно дополнить функционал последних. Использование автономного программного средства поиска ключевых слов решает проблемы при работе DLP-систем в локальной сети организации (данные не покидают пределов организации), а также позволяет обрабатывать записи с речью с привлечением незначительных вычислительных ресурсов (например, архив аудиозаписей

может быть обработан на одном компьютере за несколько часов, в то время как прослушивание всех данных записей займёт оператора на длительный срок).

Автором в 2017 г. были проведены исследования в области разработки и использовании средств поиска ключевых слов в речи (научно-исследовательская работа «Исследование методов поиска ключевых слов в речи» была отмечена дипломом II степени Всероссийского конкурса научно-исследовательских работ в области инженерных и гуманитарных наук, посвящённого 170-летию со дня рождения Н.Е. Жуковского в номинации «Информационно-телекоммуникационные технологии и моделирование»), в том числе адаптация решения CMU Sphinx – Pocketsphinx для использования в качестве самостоятельного модуля DLP-системы (при анализе аудиоархивов и в режиме реального времени). Данный инструмент показал приемлемые результаты при анализе обычной речи (в среднем 76% верно найденных ключевых слов) и удовлетворительные – при анализе шепотной речи (система обнаруживает до 36% ключевых слов).

Литература

1. Горшков Ю.Г. Тестирование средств засекречивания речи // Вопросы кибербезопасности. 2015. № 2 (10). С. 26-30.
2. Дворянкин С.В., Макаров Ю.К., Хорев А.А. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам // Защита информации. Инсайд. 2007. № 2 (14). С. 18-25.
3. Smirnov V. A. Russian Keyword Spotting System Based on Large Vocabulary Continuous Speech Recognition and Linguistic Knowledge // Journal of Electrical and Computer Engineering Volume 2016 (2016), Article ID 4062786, 9 pages, 2016. DOI: <http://dx.doi.org/10.1155/2016/4062786>.
4. Устюгов С. В. и др. Использование современных информационных технологий для обработки речевых материалов // Журнал Речевые технологии №3-4, 2014. — С. 72-76.
5. Андреев М. Ю. и др. Программный комплекс обработки данных, содержащих речевую информацию "Голос". Версия 1.0 // свидетельство о государственной регистрации программы для ЭВМ от 03.10.2016; URL: <https://elibrary.ru/item.asp?id=39355174> (дата обращения: 11.11.2019).
6. Андреев М. Ю. и др. Программа распознавания слитной речи "ristretto". Версия 1.0 // свидетельство о государственной регистрации программы для ЭВМ от 08.08.2016; URL: <https://elibrary.ru/item.asp?id=39352382> (дата обращения: 11.11.2019).
7. Кожирбаев Ж. М. и др. Поиск разговорного термина на казахском языке // Известия кыргызского государственного технического университета им. И.Раззакова №2 (38), 2016 С. 47-52.
8. Raghav Menon et al. Feature exploration for almost zero-resource ASR-free keyword spotting using a multilingual bottleneck extractor and correspondence autoencoders // INTERSPEECH 2018, 2018. DOI:10.21437/interspeech.2019-1665.

Консультант: Горшков Юрий Георгиевич, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э.Баумана, канд. техн. наук, доцент, e-mail: y.gorshkov@npo-echelon.ru

Application of Speech Keyword Spotting Tools in DLP-systems Messerle A.²²⁹

In this paper author briefly discuss the prospects for application an KWS tool in continuous speech in a modern DLP (Data Loss Prevention) systems. Presented review of the main capabilities of the DLP-systems (as of the end of 2017), which can process voice signals. KWS-systems, which may significantly improve the functionality of DLP systems in the field of speech digital processing (including providing keyword recognizing in an isolated from internet systems), are proposed.

Keywords: digital speech processing, information security.

²²⁹ Aleksandr Messerle, BMSU, Moscow, nayca@mail.ru

Ресурсно-временная модель повышения защищенности конфиденциальных данных

Минаков В.Ф.²³⁰, Шепелёва О.Ю.²³¹, Лобанов О.С.²³²

Аннотация. Разработана математическая модель интегральной оценки вероятности обеспечения безопасного состояния информационных ресурсов компании в условиях угроз и опасностей несанкционированного доступа к коммерческой конфиденциальной информации. Модель отличается учетом влияния ресурсных факторов обеспечения информационной безопасности, а также фактора времени. На основе предложенной математической модели построена зависимость вероятности обеспечения защищенного состояния информационных ресурсов компании в заданном диапазоне временных и ресурсных показателей. Установлена высокая эффективность совместного использования факторов времени и ресурсов для повышения вероятности безубыточной работы компании посредством снижения рисков возникновения ущерба в результате несанкционированного доступа к конфиденциальной коммерческой информации. Обоснована возможность использования модели в задачах стратегического управления деятельностью компании.

Ключевые слова: угрозы, опасности, несанкционированный доступ, модель, эффективность.

Введение

Современные процессы цифровизации распространяются не только на локальные технологические операции предприятий, но и на взаимодействие субъектов экономики [1]. Это процедуры формирования предложений товаров, работ и услуг производителями, их выбор потребителями и формирование запросов на их приобретение. Таким образом, посредством цифровых ресурсов обеспечивается управление потоками материальных и трудовых ресурсов [2, 3]. Оплата товаров и услуг также производится чаще безналичным расчетом (электронными платежами). Для этого используются как банковские услуги: платежные системы, дистанционное банковское обслуживание в системах клиент-банк, посредством банковских карт и т.д., так и сервисы замкнутых платежных систем Яндекс-Деньги, Web-Money и др. Доля безналичных расчетов примерно равна доле наличных, причем у обладателей банковских карт эта доля составляет 90% (по данным Центробанка России). Важно также, что цифровые технологии трансформировали экономические процессы [3-5]. Информационно-коммуникационные технологии (ИКТ) играют системообразующую роль. Так, финансовые, транспортные, маркетинговые агрегаторы стали фактором сближения и конвергенции участников экономических процессов. Именно цифровые платформы агрегаторов обеспечивают согласование интересов потребителей и производителей товаров и услуг, обеспечивая принятие и исполнение решений о сделках, запуске бизнес-процессов, управлении ресурсами хозяйственной деятельности.

В таких условиях растут возможности несанкционированного доступа к материальным и финансовым ресурсам, а соответственно, число компьютерных преступлений в отношении управления перечисленными ресурсами [6-8]. Следовательно, актуальность обеспечения информационной безопасности в экономике возрастает. Не случайно так растет интерес к прорывным информационным технологиям, например

²³⁰ Минаков Владимир Федорович, доктор технических наук, профессор, Санкт-Петербургский государственный экономический университет, Санкт-Петербург, m-m-m-m@mail.ru

²³¹ Шепелёва Ольга Юрьевна, ассистент, Санкт-Петербургский государственный экономический университет, Санкт-Петербург, shepeleva-olga@list.ru

²³² Лобанов Олег Сергеевич, кандидат экономических наук, Санкт-Петербургский государственный экономический университет, Санкт-Петербург, thelobanoff@gmail.com

распределенных реестров (блокчейн) и криптовалютам, их эмитентам и платежам с их использованием. Аналогичные процессы наблюдаются в системах смарт контрактов.

Модель ресурсного обеспечения безопасности в цифровой экономике

Надежность системы безопасности информационных ресурсов экономической системы предопределяется функционированием средств защиты в условиях угроз и опасностей несанкционированного доступа [9, 10]. Известно, что показатель надежности – вероятность безотказной работы системы защиты описывается зависимостью от объема ресурсного обеспечения средствами безопасности: программным и аппаратным обеспечением, разработкой новых методов, организационными механизмами и пр. Это можно выразить формулой:

$$p(R) = p_{max1} \cdot (1 - e^{-R/R_0}), \quad (1)$$

где: $e \approx 2,71828$,

p, p_{max1} – вероятности (текущее значение и максимально возможная) успешного противодействия угрозам и опасностям совершения компьютерного преступления, а соответственно – вызванного им экономического ущерба при базовом варианте обеспечения информационной безопасности.

Очевидно, что использование дополнительных средств защиты в виде инновационных решений, для которых не созданы средства взлома в силу неизвестности принципа действия и характеристик нововведения, повышает вероятность состояния защищенности на некоторую величину p_{max2} , причем $p_{max1} + p_{max2} = p_{max}$. Иначе: $p_{max} = p_{max1} \cdot (a_1 + a_2)$. В [11, с. 54, рис. 2] получена «зависимость вероятности обеспечения защиты» во времени в форме сигмоиды. Представим сигмоиду вероятностей функцией вида

$$p(t) = \frac{p_{max2}}{1 + e^{d-t/T}} \quad (2)$$

где: T – постоянная времени снижения эффекта защиты в условиях эксплуатации средства безопасности;

$e \approx 2,71828$,

d – число постоянных времени смещения медианного значения сигмоиды относительно начала времени отсчета.

Теперь с учетом одновременного влияния ранее использованных средств защиты и инновационных решений получим результирующую вероятность обеспечения защиты в виде суммы компонент (в качестве примера использованы: постоянная времени $T=2$ года как средний период между обновлениями программного обеспечения в системе информационной безопасности, $R_0=4$, $a_1 = 0,5$; $a_2 = 0,5$):

$$p(t, R) = 0,5 \cdot \frac{0,5}{1 + e^{4-t/2}} + 0,5 \cdot (1 - e^{-R/4}), \quad (3)$$

На рис. 1 визуализирован эффект повышения вероятности противодействия ущербам от несанкционированных доступов к коммерческой конфиденциальной информации. Как видно из рисунка, рост вероятности защищенности цифровых ресурсов существенно зависит от соотношения времени и ресурсного обеспечения информационной безопасности. Это позволяет закладывать проектные решения на основе решения задачи обеспечения требуемого уровня рисков, определяя такое соотношение ресурсов, а, следовательно, затрат, и времени реализации проекта, которое в наибольшей степени отвечает целям компании, возможностям реализации проекта в соответствии со стратегией ее деятельности. Более того, полученная зависимость является инструментом построения поля сценариев для принятия управленческих решений по обеспечению безопасного состояния не только информационных, но и финансовых, а также материальных ресурсов компании. Очевидно, что соотношение между эффектами повышения вероятности предотвращения несанкционированного доступа a_1 и a_2 может на основе полученной модели выбираться и оптимизационным путем, когда модель может использоваться в интегральных показателях деятельности компании в течение определенного времени.

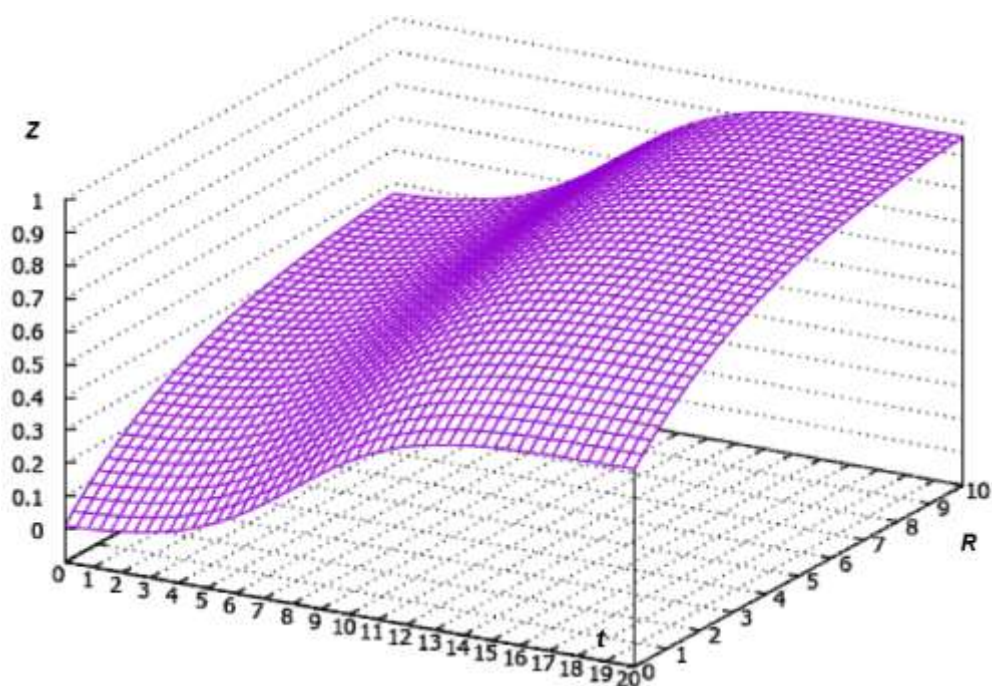


Рис. 1. Влияние ресурсов (R) и времени (t) на вероятность обеспечения безопасного состояния

Выводы

Предложена модель интегральной оценки вероятности обеспечения безопасного состояния информационных ресурсов компании в условиях угроз и опасностей несанкционированного доступа к коммерческой конфиденциальной информации. Отличительной особенностью модели является учет фактора времени при использовании инновационных решений обеспечения информационной безопасности в дополнение к ресурсным факторам ее повышения, основанных на повышении затрат. Установлено достаточно высокая степень повышения вероятности безубыточной работы компании, превышающая в конкретном рассмотренном примере эффект от ресурсного подхода к снижению рисков. Показана возможность использования модели в задачах стратегического управления деятельностью компании, управления проектами обеспечения информационной безопасности, а также оптимизации издержек. Достоверность предложенной модели подтверждается доказательством справедливости модели строгими математическими выкладками.

Литература

1. Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In Proceedings of the 2017 IEEE II International Conference on Control in Technical Systems, IEEE, CTS, 2017, pp. 96-99. DOI: 10.1109/CTSUS.2017.8109498.
2. Глинский В.В., Серга Л.К., Булкина А.М. Дифференциация муниципальных образований как фактор экономического развития территорий // Вопросы статистики. 2016. № 8. С. 46-52.
3. Ивантер В.В., Белоусов Д.Р., Блохин А.А., Борисов В.Н., и др. Структурно-инвестиционная политика в целях модернизации экономики России // Проблемы прогнозирования. 2017. № 4 (163). С. 3-16.
4. Glinskiy V., Serga L., Chemezova E., Zaykov K. Clusterization economy as a way to build sustainable development of the region // В сборнике: Procedia CIRP 13. Сер. "13th Global Conference on Sustainable Manufacturing - Decoupling Growth from Resource Use" 2016. С. 324-328.
5. Glinskiy V., Serga L., Khvan M. Assessment of environmental parameters impact on the level of sustainable development of territories // В сборнике: Procedia CIRP 13. Сер. "13th Global Conference on Sustainable Manufacturing - Decoupling Growth from Resource Use" 2016. С. 626-631.

6. Maximov R., Krupenin A., Sharifullin S., Sokolovsky S. Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines // Вопросы кибербезопасности. 2019. № 1 (29). С. 10-17.
7. Petrenko S. La Administración de la Ciberseguridad. Industria 4.0. Oviedo, Asturias. University of Oviedo, 2019, 294 p.
8. Dorofeev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city // Communications in Computer and Information Science. 2016. Т. 674. С. 441-449.
9. Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. -London: IntechOpen, 2018. 278 p.
10. Александров А.А., Ларионов В.И., Суцев С.П. Анализ и управление техногенными и природными рисками. – М.: МГТУ им.Н.Э. Баумана, 2019, 357 с.
11. Мальцев Г.Н., Панкратов А.В., Лесняк Д.А. Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. 2015. № 1 (74). С. 50-58.

Resource-time model to increase the security of confidential data

Minakov V.F.,²³³ Shepeleva O.Yu.²³⁴, Lobanov O.S.²³⁵

Abstract. *A mathematical model has been developed for the integrated assessment of the probability of ensuring a safe state of the company's information resources in the face of threats and dangers of unauthorized access to commercial confidential information. The model is distinguished by taking into account the influence of resource factors for ensuring information security, as well as the time factor. Based on the proposed mathematical model, the dependence of the probability of providing a protected state of the company's information resources in a given range of time and resource indicators is constructed. The high efficiency of the joint use of time and resource factors was established to increase the likelihood of a company breaking even by reducing the risk of damage resulting from unauthorized access to confidential commercial information. The possibility of using the model in the tasks of strategic management of the company.*

Keywords: *threats, dangers, unauthorized access, model, efficiency.*

²³³Minakov V.F., Dr.Sc., Professor, Saint-Petersburg State University of Economics, St. Petersburg, m-m-m-m-m@mail.ru

²³⁴ Shepeleva O.Yu., Saint-Petersburg State University of Economics, St. Petersburg, shepeleva-olga@list.ru

²³⁵ Lobanov O.S, Ph.D., Saint-Petersburg State University of Economics, St. Petersburg, thelobanoff@gmail.com

Исследование основных криптовалют на рынке и их сравнение с точки зрения информационной безопасности

Нечаев О.В.²³⁶

В данной работе были исследованы основные принципы работы системы Bitcoin, принципы стабильности компонентов ее технической составляющей и некоторые из угрожающих ее стабильности атак. Также рассмотрены альтернативные технологии «электронных денег» и произведено их сравнение с точки зрения информационной безопасности, конфиденциальности и анонимности.

Ключевые слова: биткоины, «электронные деньги», транзакции, альткоины, конфиденциальность, стабильность, анонимность.

Введение

Обоснование актуальности темы

Электронные деньги получают всё более широкое распространение, ввиду удобства расчётов за покупки товаров и услуг в Интернет-магазинах, высокой скорости проведения транзакций, применения современных технологий для обеспечения безопасности сделок [1]. Одним из наиболее перспективных видов электронных денег является криптовалюта. Однако даже самая главная криптовалюта на рынке не защищена от наличия уязвимостей, способных привести к потере денег конечного пользователя данной валюты.

Исходные данные НИРС

В качестве исходных данных для НИРС использовались ресурсы сети Интернет и материалы открытых источников, таких как:

- научные статьи;
- публикации;
- книги по тематике.

Цели и задачи НИРС

Целью настоящей НИРС является исследование принципа работы Bitcoin, его недостатков и угроз стабильности. Вследствие их наличия появились альтернативные криптовалюты, каждая из которых пробует исправить один или несколько из данных уязвимостей различными способами, и в данной работе будут также рассмотрены их принципы работы и каким образом они пытаются исправить уязвимости системы Bitcoin.

Основная часть

1. Bitcoin

Техническую составляющую криптовалюты Bitcoin можно разбить на три основных компонента:

- транзакции и скрипты;
- протокол консенсуса;
- сеть связи.

1.1 Транзакции и скрипты

²³⁶ Нечаев Олег Владимирович, Москва, nechaevolegiu@gmail.com

Работа Bitcoin основана на серии сообщений, называемых транзакциями.

Транзакция содержит массив входных данных (входов) и массив выходных данных (выходов). Вся транзакция хэшируется с использованием SHA-256, и этот хэш, в конечном итоге, служит глобальным уникальным идентификатором транзакции.

Входные данные транзакции ссылаются на предыдущие транзакции по их хэшу транзакции и индексу вывода в выходном массиве этой транзакции. Они также должны содержать фрагмент кода, который «погашает» тот вывод транзакции, который называется scriptSig.

1.2 Консенсус и майнинг

Валютная система на основе транзакций была бы небезопасной, если бы транзакции отправлялись напрямую между пользователями для перевода средств. В Bitcoin журнал реализован в виде последовательности блоков транзакций, каждый из которых содержит хэш предыдущего блока, фиксируя этот блок в качестве единственного предшествующего элемента. Это называется блокчейн.

Биткойн устанавливает консенсус по блокчейну посредством децентрализованного, псевдонимного протокола, получившего название консенсуса Накамото. Это можно считать основным нововведением биткойна и, возможно, самым важным компонентом его успеха.

1.3 Сеть связи

Последним ключевым компонентом Bitcoin является его коммуникационная сеть. По сути, это децентрализованная, специализированная одноранговая широковебчатая сеть, используемая для объявления новых транзакций и предлагаемых блоков. Как правило, это наименее инновационный из трех компонентов, и лишь немногие альткойны внесли существенные изменения.

1.4 Стабильность

Стабильность для Биткойна была определена многими расплывчатыми, а иногда и противоречивыми способами, но в широком понимании это означает, что система будет продолжать вести себя так, чтобы облегчать функциональную валюту по мере ее роста, и участники предпринимают новые атаки.

1.4.1 Стабильность правил достоверности транзакций

Основной философией, согласно которой устанавливается как участники экосистемы Биткойн достигают консенсуса в отношении правил достоверности транзакций, является канонизм. Он заключается в непоколебимости правил установленных самим Сатоши.

Тем не менее, канонизм не может полностью объяснить текущие правила Биткойна, так как изменения уже были внесены для добавления новых функций (например, pay-to-script-hash [2]).

В настоящее время управление де-факто обеспечивается основными разработчиками Биткойн, которые поддерживают bitcoind, а фонд Bitcoin Foundation обеспечивает базовую организационную структуру и привлекает средства за счет пожертвований для поддержки команды разработчиков.

1.4.2 Стабильность протокола консенсуса

В различных анализах [3-6] были предприняты различные попытки описать свойства консенсусного протокола, которые должны выполняться, чтобы можно было сказать, что блокчейн считается стабильным. В итоге их можно попробовать систематизировать в пять основных:

- Возможный консенсус.

- Экспоненциальная сходимость.
- Живучесть.
- Корректность.
- Честность. .

В общем случае, один майнер, добывающий биткойны не по стандартным правилам и контролирующий большую часть вычислительной мощности, может подорвать несколько из свойств стабильности.

Даже в отсутствие майнера, обладающего большей частью вычислительной мощности, майнеры меньшего размера могут вступить в сговор, чтобы, по сути, сформировать картель, контролирующей большую часть мощности майнинга.

Но у майнера могут быть другие стимулы, кроме получения прибыли с добычи биткойна: тогда можно отметить как минимум две атаки, теоретически угрожающие стабильности протокола консенсуса:

- атака Голдфингера
- атака под названием «feather-forking»

1.5 Безопасность со стороны клиента

Теперь рассмотрим пользование Биткойнами с точки зрения безопасности со стороны клиента – где, по сути, самое важное это управление ключами. Ведь пользователи понесут немедленные и безвозвратные денежные потери, если ключи будут потеряны или скомпрометированы. Это можно сделать несколькими способами:

- Хранение пула ключей на диске
- Чтобы избежать единой точки отказа и повысить безопасность, биткойны могут храниться с использованием мультисигнатурного сценария k-of-n, который задает n открытых ключей.
- Клиент Bitcoin может позволить зашифрованному файлу пула ключей (называемому кошельком) быть зашифрованным ключом, полученным из выбранного пользователем пароля.
- Пулы ключей могут быть детерминированно получены из одного выбранного пользователем секрета, что позволяет использовать его на нескольких устройствах, если секрет хранится в памяти.
- Кошельки, хранящиеся в автономном режиме на пассивных портативных носителях, таких как бумага или флэш-накопитель USB, улучшают защиту от кражи от вредоносных программ и предоставляют знакомую интеллектуальную модель физической безопасности.
- Хранилище «с воздушным зазором» (air-gapped storage)
- Сторонние веб-службы предлагают функции хранения

2. Альтернативы

Изменения, которые можно осуществить в системе Биткойн для попытки исправления описанных в предыдущих частях недостатков и уязвимостей, делятся следующим образом:

- «жесткое» ответвление (hard fork)
- «мягкое» ответвление (soft fork)
- обновление политики ретрансляции.

2.1 Альткойны

Из-за ограничений на то, что можно изменить в биткойнах без хард-форка, возникли сотни производных систем, называемых альткойнами, с альтернативными подходами к проектированию. Альткойны должны запустить первоначальное распределение валюты,

чтобы побудить пользователей к участию, что может быть достигнуто несколькими способами:

- альткойны могут просто начать новый блокчейн с нуля, выделяя средства первоначальным майнерам
- альткойн может намеренно ответвиться от Биткойн в какой-то определенный момент, принимая историю предыдущих транзакций и владение денежными средствами.
- «proof-of-burn», при котором пользователи должны уничтожить определенное количество биткойнов

Альткойны также должны конкурировать с биткойнами за майнеров и избегать атак Голдфингера майнерами биткойнов, что может быть затруднительно до того, как валюта достигнет ненулевого обменного курса.

2.2 Альтернативы в протоколе консенсуса

Как было рассмотрено ранее, протокол консенсуса Биткойна – наиболее обсуждаемый его компонент из-за открытых вопросов о стабильности, опасений по поводу производительности и масштабируемости протокола и волнений, что вычислительная головоломка является тратой ресурсов.

Протокол консенсуса включает в себя множество «магических констант», которые были жестко запрограммированы на основе первоначальных догадок. Почти каждый альткойн изменил, по крайней мере, некоторые из этих параметров, но модификации часто противоречивы, и есть только несколько четких рекомендаций о том, как их выбирать и как они могут повлиять на стабильность.

Например: ограничения на размер блоков и транзакций, или то, что Биткойн автоматически корректирует сложность своей вычислительной задачи, чтобы решения находились (в среднем) с интервалом в десять минут.

Можно попробовать пойти по пути смены вычислительной задачи. Было сделано предложение – ASIC-устойчивые головоломки. До сих пор самой популярной подобной головоломкой (используемой в Litecoin и Dogecoin, среди прочего) была хэш-функция scrypt [7], изначально разработанная для стойкого к взлому хэширования паролей.

Также распространенным предложением является использование функции поиска в приложениях для научных исследований, например проект Folding@Home [8].

Primescoin [9] представил первую полезную головоломку в успешном альткойне. Его загадка требует поиска последовательностей больших простых чисел, представляющих математический интерес и которые могут быть использованы в качестве параметров для криптографических протоколов.

Есть подход, который называется виртуальным майнингом. Его также иногда называют «proof-of-stake».

Виртуальный майнинг предлагает два основных преимущества:

- во-первых, злоумышленнику может быть сложнее приобрести достаточно большое количество цифровой валюты, чем приобрести достаточно мощное вычислительное оборудование.
- во-вторых, избегается потребление реальных ресурсов (т. е. вычислительных циклов), никакие реальные ресурсы не тратятся впустую.

На сегодняшний день было предложено несколько вариантов виртуального майнинга, которые в основном зависят от критериев, по которым обладание определенным количеством валюты дает право выбрать следующий блок:

- Proof-of-coin-age.
- Proof-of-deposit.
- Proof-of-burn.
- Proof-of-activity.

2.3 Альтернативы в анонимности и приватности

Биткойн предоставляет ограниченную форму несвязанности: пользователи могут в любое время создавать новые псевдонимы (адреса). В первоначальной спецификации наличие подобного доказывалось для обеспечения строгой конфиденциальности, однако быстро стало ясно, что из-за публичного характера блокчейна иногда можно отследить поток денег между псевдонимами и сделать вывод, что они, вероятно, контролируются одним и тем же человеком.

2.3.1 Деанонимизация

Связывание может применяться транзитивно для получения кластеров адресов; это пример анализа графа транзакций. Основная проблема для злоумышленника заключается в том, что эти идиомы хрупкие: они могут давать ложные срабатывания и со временем терять точность по мере развития реализаций. Также могут появиться новые методы связывания.

Для деанонимизации злоумышленник должен предпринять дальнейший шаг, связав кластеры адресов с реальными идентичностями.

Другой основной целью усилий по де-анонимизации является P2P сеть.

2.3.2 Предложения

Существует три основных класса предложений в области анонимности, их сравнение относительно свойств безопасности и совместимости с Bitcoin приведено в табл.1.

В P2P протоколах микширования, группа держателей биткойнов совместно создает серию транзакций, которые переставляют владение своими монетами, делая каждого участника анонимным в этой группе. Этот процесс может повторяться между разными пользователями для увеличения анонимности.

Таблица 1 – Сравнение трех основных классов предложений в области анонимности

Название	Класс	Безопасность			Совместимость с Bitcoin
		Внутренняя несвязанность	Защита от краж	Защита от DoS	
CoinJoin	P2P	–	+	–	+
Shuffle Net	P2P	–	+	–	+
Fair Exchange	P2P	–	+	–	+
CoinShuffle	P2P	+	+	частично	+
MixCoin	распр.	частично	частично	+	+
BlindCoin	распр.	+	частично	+	+
Zerocoin	альткойн	+	+	+	–
Zerocash	альткойн	+	+	+	–

Простым механизмом для достижения этого является CoinJoin [12]. Для надежной внутренней несвязанности используется CoinShuffle [13].

Примером использования распределенной микс сети является Mixcoin [14].

Blindcoin [15] расширяет Mixcoin, используя слепые токены. Ценой двух дополнительных транзакции для публикации и получения слепых токенов, это не позволяет честному, но любопытному миксу изучить соответствие между входами и выходами, и затем перейти на полную внутреннюю несвязанность

Zerocoin – это предлагаемый альткойн со встроенной несвязываемостью, использующий базовую валюту, похожую на биткойны, и анонимную теневую валюту, называемую зерокоинами. PinnocchioCoin [16] представляет собой аналогичное предложение, использующее другую криптографическую конструкцию.

ZeroCash - еще более сильное предложение для анонимного альткойна. Транзакции ZeroCash - это особый тип доказательств с нулевым разглашением, называемых SNARKs, которые не раскрывают вообще никакой информации о сумме или получателях (за исключением возможной комиссии за публичные транзакции), позволяя создать полностью не отслеживаемый регистр, в котором информация не раскрывается публично.

Заключение

В данной работе были:

- исследованы принципы работы Bitcoin, а также недостатки и угрозы стабильности данной криптовалюты;
- произведена попытка разбить ее техническую составляющую на три части, классифицировать правила стабильности;
- упомянуты атаки, имевшие место быть на практике, угрожающие стабильности Bitcoin;
- рассмотрено какую техническую часть или какую уязвимость пробует изменить\исправить в своей реализации та или иная альтернативная криптовалюта;
- произведен сравнительный анализ трех основных классов предложений в области анонимности пользования валютой.

Список использованных источников

1. Захаров Д.Н., Иванов В.Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. 2017. № S2 (20). С. 30-38.
2. G. Andresen. Pay to Script Hash. BIP 16, 1 2012.
3. J. Garay, A. Kiayias, and N. Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive Report 2014/765, 2014.
4. J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In WEIS, 2013.
5. A. Miller and J. J. LaViola Jr. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin, 2014.
6. S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. <http://bitcoin.org/bitcoin.pdf>, 2008.
7. C. Percival and S. Josefsson. The scrypt Password-Based Key Derivation Function, 2012.
8. S. M. Larson, C. D. Snow, M. Shirts, et al. Folding@ Home and Genome@ Home: Using distributed computing to tackle previously intractable problems in computational biology. Technical report, arXiv preprint, 2002.
9. S. King. Primecoin: Cryptocurrency with prime number proof-of-work, 2013.
10. S. King and S. Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, August 2012.
11. J. Kwon. TenderMint: Consensus without Mining, August 2014
12. G. Maxwell. CoinJoin: Bitcoin privacy for the real world. bitcointalk.org, August 2013.
13. T. Ruffing, P. Moreno-Sanchez, and A. Kate. CoinShuffle: Practical decentralized coin mixing for Bitcoin. In ESORICS, 2014.
14. J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten. Mixcoin: Anonymity for Bitcoin with accountable mixes. In Financial Cryptography, 2014.
15. L. Valenta and B. Rowan. Blindcoin: Blinded, Accountable Mixes for Bitcoin. In Workshop on Bitcoin Research, 2015.
16. G. Danezis, C. Fournet, M. Kohlweiss, and B. Parno. PinocchioCoin: building Zerocoin from a succinct pairing-based proof system. In PETShop, 2013

Study of the main cryptocurrencies in the market and their comparison

Nechaev O.V.²³⁷

In this work, we studied the basic principles of the Bitcoin system, the principles of stability of the components of its technical component, and some of the attacks that threaten its stability. Alternative technologies of “electronic money” are also considered and compared in terms of information security, confidentiality and anonymity.

Keywords: bitcoins, “electronic money”, transactions, altcoins, confidentiality, stability, anonymity.

²³⁷ Nechaev Oleg Vladimirovich, Moscow, nechaevolegiu@gmail.com

Классификация программ на языке Javascript по признаку обфусцированности при помощи искусственной нейронной сети с механизмом внимания

Пономаренко Г.С.²³⁸ Ключарёв П.Г.²³⁹

В работе исследовалось применение искусственной нейронной сети с механизмом внимания для решения задачи классификации по признаку обфусцированности программ на языке Javascript, приведённых к общему представлению на основе путей. Результатом работы стало создание нейросетевой модели с механизмом внимания, адаптированной для решения задачи классификации программ по признаку обфусцированности. Полученные качественные характеристики модели показывают, что рассмотренный подход имеет потенциал для применения в реальных программных продуктах, например, для обнаружения и классификации вредоносного кода, создания цифровых отпечатков и профилей и др., при условии доработки с учётом изложенных предложений.

Ключевые слова: обнаружение обфускации, обфусцированный код, распознавание обфускации

Введение

По мнению исследователей Н.П. Варновского и др. [1], обфускация впервые неявно упоминается ещё в 1976 году в работе Диффи и Хэллмана [2]. Они предложили вставлять в программу шифрования секретный ключ, и затем инициализированная секретным ключом программа шифрования запутывается так, чтобы извлечение из неё секретного ключа было очень трудной задачей. В явном виде понятие обфускации было введено в 1997 году в работе Коллберга, Томборсона и Лоу [3]. По определению К.Ю. Никольской и А.Д. Хлестова [4], обфускация программы — это приведение исходного текста программы к виду, сохраняющему его функциональность, но затрудняющему анализ при обратной разработке. Обфусцированная программа — программа, полученная из другой путём применения обфускации [5]. Исходная программа называется необфусцированной.

Формальная постановка задачи

Проблема различения обфусцированных и необфусцированных программ неразрывно связана с проблемой классификации исходных текстов программ. Для формализации задачи воспользуемся определениями, введёнными Сильвео Сезаром и Янгом Ксьянгом в первой главе книги «Классификация и схожесть программ» [6].

Признак r программы p называется стойким, если r остаётся неизменным при всех возможных способах исполнения программы p . Программа q называется обфусцированной копией программы p , если q является результатом преобразований, сохраняющих семантику (смысл) алгоритмов и структур данных. Программы p и q похожие, если они построены на базе одной и той же программы.

Пусть P — множество исходных текстов программ, $f_1, \dots, f_k$ — функции, выделяющие признаки из программы, т.е. $f_i: P \rightarrow D_i$, где D_i — i -е множество признаков. Пусть $\{p_1, \dots, p_n\} \subset P$ — обучающая выборка, $\{0,1\} = Y$ — метки классов (1 ставится в соответствие обфусцированной программе, 0 — необфусцированной). Необходимо найти при помощи обучающей выборки $\{p_1, \dots, p_n\}$ отображение $s: D_1 \times \dots \times D_k \rightarrow \{0,1\}$, с наименьшей ошибкой классифицирующее элементы из всего множества P .

²³⁸ Пономаренко Григорий Сергеевич, студент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, gs.ponomarenko@yandex.ru

²³⁹ Пётр Георгиевич Ключарёв, доцент кафедры «Информационная Безопасность» МГТУ им. Н.Э. Баумана, кандидат технических наук, pk.iu8@yandex.ru

Подготовка набора данных

Для создания тренировочной и тестовой выборок использовался репозиторий программ github.com. Были выгружены 100 самых популярных проектов на языке Javascript (49612 файлов с расширением «.js», исключая файлы с расширением «.min.js»).

Чтобы упростить создание образцов обфусцированного кода, из скриптов были выделены функции при помощи библиотеки Esprima. Библиотека позволяет строить для любой Javascript-программы, соответствующей стандарту ECMAScript 2016, абстрактные синтаксические деревья (АСД).

Для всех полученных скриптов с расширением «.js» (49612 штук) построены АСД, для каждого элемента класса «FunctionDeclaration» код сохранялся в отдельный файл (всего 126276 файлов).

Для генерирования образцов обфусцированного кода требовались специальные программы, реализующие обфускацию. Источником программ стал репозиторий github.com. Были использованы 6 проектов: «javascript-obfuscator/javascript-obfuscator», «zswang/jfogs», «anseki/gnirts», «mishoo/UglifyJS2», «alexhorn/defendjs», «wearefractal/node-obf».

Чтобы образцы программ могли быть поданы на вход искусственной нейронной сети, их нужно заранее специальным образом преобразовать. Использовалось общее представление на основе путей, предложенное Алоном и др. в 2018 году [7] для исследования свойств программ методами машинного обучения. Для выделения признаков из программ на Javascript была применена библиотека PigeonJS. Она позволяет получить список путей заданной длины на АСД. Путь из k вершин имеет формат:

$$(\text{вершина}_1 \wedge \text{вершина}_2 \dots \text{вершина}_{k-1} \vee \text{вершина}_k) \quad (1)$$

Вершины (1) отделяются знаками $\wedge$ и $\vee$ в зависимости от того, происходит подъём или спуск по дереву при проходе от первой до k -й вершины.

Архитектура искусственной нейронной сети с механизмом внимания

Идея, лежащая в основе механизма внимания, может быть представлена как выбор «наиболее интересной» части получившегося набора [8]. Механизмы внимания используется для решения разных прикладных задач при помощи искусственных нейронных сетей, например, анализа тональности текстов (Тащилин и др. [9]) или предсказания названий функций в программном коде (Алон и др. [10]). Полученная итоговая модель построена на базе сети Алон и др. [11], чьё решение было адаптировано для классификации скриптов по признаку обфусцированности.

Контекст $c_i = (x_s, p, x_t)$ — это кортеж из трёх элементов: начальной вершины, пути и конечной вершины. Начальные и конечные вершины $x_s, x_t \in T$, где T — множество начальных и конечных вершин, путь $p \in P$, где P — множество всех путей. Каждый скрипт s_j описывается множеством контекстов (2):

$$s_j = \{ (x_s, p, x_t) \mid x_s, x_t \in T, p \in P \} \quad (2)$$

Каждому элементу $x \in T$ сопоставлено векторное представление $v_x \in \text{Vect}_T \subset \mathbb{R}^{128}$. Аналогично, каждому элементу из $p \in P$ сопоставлено векторное представление $v_p \in \text{Vect}_P \subset \mathbb{R}^{128}$. Векторное представление одного контекста i имеет размерность $3 * 128 = 384$:

$$v_{ci} = (v_{xt}, v_p, v_{xt}) \in \text{Vect}_T \times \text{Vect}_P \times \text{Vect}_T \subset \mathbb{R}^{128*3} \quad (3)$$

Каждый скрипт (2) описывается набором векторных контекстов из (3):

$$s_j = \langle (v_{xt}, v_p, v_{xt}) \mid v_{xt}, v_{xs} \in \text{Vect}_T, v_p \in \text{Vect}_P \rangle \quad (4)$$

Была задана верхняя граница для числа контекстов (4) на один скрипт — 200 контекстов. Если мощность множества контекстов, описывающих скрипт, меньше 200, то к нему добавляются нулевые контексты: $v_{c0} = (0^{128}, 0^{128}, 0^{128})$.

На рисунке 1 дана схема использованной искусственной нейронной сети. Первым идёт полносвязный слой, для которого применён метод регуляризации дропаут, т.е. на каждом шаге обучения случайно выбранные 75% связей исключались.

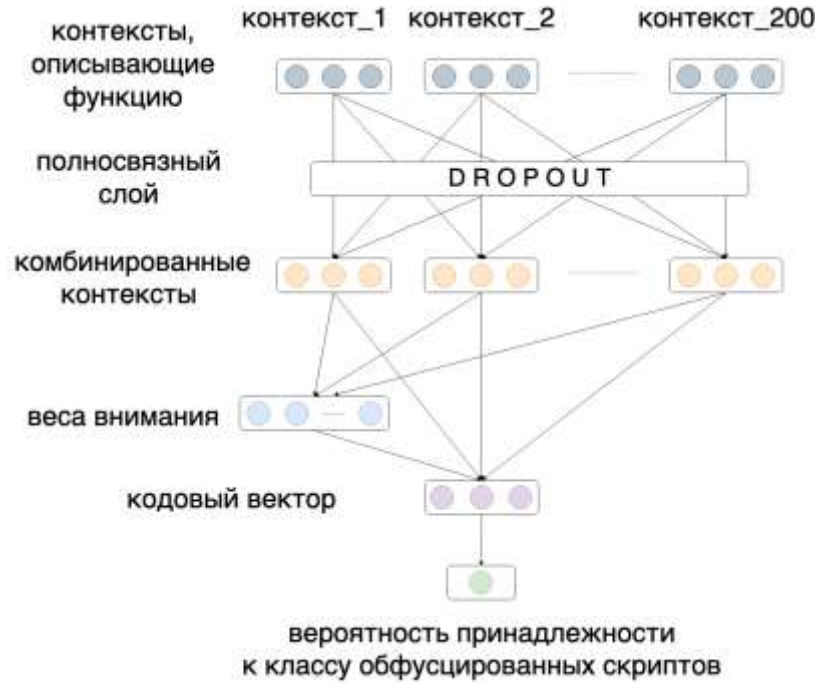


Рисунок 1 — Структура искусственной нейронной сети

Полносвязный слой имеет функцию активации $\tanh$:

$$\tilde{c}_i = \tanh(W * c_i) \quad (5)$$

где $c_i \in \mathbb{R}^{384}, i = \overline{1,200}$ — контексты, описывающие скрипт, $\tilde{c}_i \in \mathbb{R}^{128}, i = \overline{1,200}$ — комбинированные контексты, $W \in \mathbb{R}^{128 \times 384}$ — матрица весов полносвязного слоя.

На основе комбинированных контекстов $\{\tilde{c}_1, \dots, \tilde{c}_{200}\}$ и вектора внимания α подсчитываются веса внимания α_i для каждого $\tilde{c}_i$:

$$\alpha_i = \frac{\exp(\tilde{c}_i^T * \alpha)}{\sum_{j=1}^{200} \exp(\tilde{c}_j^T * \alpha)} \quad (6)$$

После подсчёта весов α_i (6) вычисляется кодировый вектор v по формуле (7):

$$v = \sum_{i=1}^{200} \alpha_i * \tilde{c}_i \quad (7)$$

Все веса внимания α_i неотрицательные, их сумма равна 1. Можно рассматривать вычисление кодирового вектора как вычисление взвешенного среднего по всем комбинированным контекстам $\tilde{c}_i$.

На последнем шаге при помощи векторов $y_{obf} \in \mathbb{R}^{128}$ и $y_{not\_obf} \in \mathbb{R}^{128}$ вычисляется итоговое решение: обфусцированный скрипт или нет. Значения y_{obf} и y_{not_obf} подбираются в процессе обучения. Вероятность принадлежности скрипта к классу обфусцированных $q(v)$ рассчитывается по формуле (9) на основе кодирового вектора v (7):

$$q(v) = \frac{\exp(v^T * y_{obf})}{\exp(v^T * y_{obf}) + \exp(v^T * y_{not\_obf})} \quad (9)$$

Если $q(v) > 0.5$, то скрипт признаётся обфусцированным. Вероятность того, что скрипт необфусцированный, равна $1 - q(v)$.

Для одного скрипта функция потерь (кросс-энтропии) вычисляется как:

$$H(p, q) = -p(v) * \log(q(v)) - (1 - p(v)) * \log(1 - q(v)) \quad (12)$$

где $p(v) = 1$ тогда, когда скрипт принадлежит классу обфусцированных, иначе $p(v) = 0$. Для минимизации функции потерь в качестве алгоритма оптимизации использовался метод адаптивной оценки моментов.

Обучение искусственной нейронной сети

Обучение искусственной нейронной сети проводилось на компьютере с 8-ядерным процессором Intel Core i7-7700 (3.6 ГГц), 16 Гб оперативной памяти, видеокартой NVIDIA GeForce GTX 1080.

Тренировочная выборка была сформирована следующим образом: 115504 наборов контекстов, описывающих необфусцированные функции, и 117990 наборов, описывающих обфусцированные функции, из них 36000 случайно выбрано из обфусцированных «javascript-obfuscator», 36000 случайно выбрано из обфусцированных «jfofs», 36000 случайно выбрано из обфусцированных «UglifyJS2», 9990 из обфусцированных «defendjs». Всего 233494 наборов. По тренировочной выборке было получено множество самых популярных наименований начальных и конечных вершин T ($|T| = 776830$), и множество наиболее часто встречающихся путей P ($|P| = 1008102$) таким образом, чтобы для каждого скрипта s хотя бы один контекст c состоял из двух элементов из T и одного из P .

Тестовая выборка состояла из 8444 наборов контекстов, описывающих обфусцированные функции (обфусцированы «gnirts» или «node-obf»). Модель обучалась на 9 эпохах. Численные оценки качества: точность — 84.9 %, полнота — 85.1 %, $F1$ — 85.0 %. Представленная модель имеет потенциал для улучшения: кодовый вектор v (7) может быть подан на вход дополнительному классификатору, например, алгоритму на основе метода опорных векторов. Аналогичный подход Ндичу и др. использовали для решения задачи детектирования вредоносных программ на Javascript [11]. Также улучшить качество модели может добавление второго полносвязного слоя и замена функции активации.

Выводы

В работе исследовалось применение искусственной нейронной сети с механизмом внимания для решения задачи классификации по признаку обфусцированности программ на языке Javascript, приведённых к общему представлению на основе путей [7]. Был получен набор образцов обфусцированного и необфусцированного кода, модель искусственной нейронной сети с механизмом внимания [10] была адаптирована для решения задачи классификации программ по признаку обфусцированности. Характеристики полученной модели показывают, что рассмотренный метод имеет потенциал для применения в программных продуктах, использующих классификацию программ по признаку обфусцированности (для обнаружения и классификации вредоносного кода, создания цифровых отпечатков и др.) при условии доработки с учётом изложенных предложений.

Литература

1. Н.П. Варновский, В.А.Захаров, Н.Н. Кузюрин, А.В. Шокуров. Современное состояние исследований в области обфускации программ: определения стойкости обфускации. . Труды Института системного программирования РАН, том 26, вып. 3, 2014, стр. 167-198.
2. Diffie W., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory, IT-22(6), 1976, p.644-654.
3. Collberg C., Thomborson C., Low D. A Taxonomy of Obfuscating Transformations // Technical Report, N 148, Univ. of Auckland, 1997.
4. К.Ю. Никольская, А.Д. Хлестов. Обфускация и методы защиты программных продуктов // Вестник УРФО. Безопасность в информационной сфере. 2015. No2 (16). С. 7-10.
5. Козачок А.В. Теоретическое обоснование стойкости неразличимой обфускации / А.В. Козачок, М.В. Бочков, Л.М.Туан // Вопросы кибербезопасности. -2016. № 1 (14). - С. 36-46.
6. Silvio Cesare, Yang Xiang. Software Similarity and Classification. Springer-Verlag, 2012.
7. Alon, Uri, Meital Zilberstein, Omer Levy, Eran Yahav. A general path-based representation for predicting program properties. ACM SIGPLAN Notices, vol. 53, no. 4, pp. 404-419. ACM, 2018.
8. Малых, В.К вопросу о классификации шумных текстов / В. Малых, В. Лялин // Труды ИСА РАН. Специальный выпуск. — 2018.
9. С.П. Тащилин, М.Ю. Косенко. Применение механизмов внимания в нейронных сетях для анализа тональности текста на русском языке. // Colloquium-journal. 2019. № 10-2 (34). С. 208-214.
10. Uri Alon, Meital Zilberstein, Omer Levy, Eran Yahav. Code2vec: Learning Distributed Representations of Code. Proc. ACM Program. Lang.3, POPL, 2019, 40, P. 1-29
11. Ndichu, S., Kim, S., Ozawa, S., Misu, T. and Makishima, K., 2019. A machine learning approach to detection of JavaScript-based attacks using AST features and paragraph vectors. *Applied Soft Computing*, 84, p.105721.

Javascript programs classification based on obfuscation using artificial neural networks with attention mechanism

Ponomarenko G.S.²⁴⁰, Klyucharev P.G.²⁴¹

In this paper, we consider javascript code obfuscation detection using artificial neural network with attention mechanism as classifier algorithm. Before being fed to the network, Javascript program is converted to the general path-based representation. Obfuscated Javascript code samples were created based repositories and obfuscators found on Github.com. According to results of experiments, evaluated model potentially can be implemented with some improvements in malicious code detection systems, browser or mobile device fingerprint collection systems etc.

Keywords: *obfuscation detection, obfuscated code, obfuscation recognition*

²⁴⁰ Grigory Ponomarenko, student, BMSTU, Moscow, gs.ponomarenko@yandex.ru

²⁴¹ Petr Klyucharev, Ph.D., BMSTU, Moscow, pk.iu8@yandex.ru

**Риск – ориентированный подход
в разработке безопасного программного обеспечения
Райкова Н.О.²⁴²**

В данной статье представлено описание риск-ориентированного подхода в концепции системы менеджмента разработки безопасного программного обеспечения, основанное на требованиях международных стандартов в области информационной безопасности (далее ИБ). Подробно рассмотрены процедуры управления рисками ИБ. Решена задача выбора методов оценки рисков ИБ в сфере разработки безопасного программного обеспечения. В результате делается вывод о возможности использования процедур управления рисками ИБ, применяемых в системе менеджмента ИБ.

Ключевые слова: система менеджмента разработки безопасного программного обеспечения, методы оценки рисков, системы менеджмента, уязвимость программного обеспечения.

Введение

1. Использование Системы менеджмента разработки безопасного программного обеспечения (далее СМРБПО), основанной на ГОСТ Р 56939, в качестве самостоятельной единицы или подсистемы Системы менеджмента информационной безопасности (далее СМИБ), поможет организациям разрабатывать программное обеспечение, отвечающее требованию по безопасности информации на всех стадиях жизненного цикла [1-5]. В данной статье рассмотрим риск-ориентированный подход применительно к использованию в СМРБПО.

Из-за отсутствия единой трактовки термина «риск информационной безопасности» или «информационный риск», необходимо условиться, что под риском будем понимать комбинацию вероятности возникновения рискового события и возникающего при этом ущерба [6].

Нормативная база

Риск-ориентированный достаточно широко представлен в международных методологиях и стандартах. Кратко рассмотрим, какие стандарты могут использоваться для управления рисками ИБ при разработке безопасного программного обеспечения (далее РБПО).

ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» обеспечивает рекомендации для менеджмента риска информационной безопасности в организации, в соответствии с требованиями СМИБ. Но не обеспечивает определенной методологией для управления рисками ИБ.

ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска» является общим для всех областей риска и предназначен для различных целей организации в зависимости от сферы деятельности. Стандарт содержит в себе описание 31 метода оценки риска.

Существующие методики и инструментарий для оценки риска можно разделить на следующие группы:

²⁴² Райкова Наталья Олеговна, аспирант кафедры ИУ8 МГТУ им. Н.Э. Баумана, Москва,
E-mail: natalya_raykova@mail.ru

- методики, использующие оценку риска на качественном уровне. К таким методикам, в частности, относятся FRAP, OCTAVE;
- количественные методики. К этому классу относится методика RiskWatch;
- методики, использующие смешанные оценки (такой подход используется в CRAMM, CORAS и т.д.).

На рисунке 1 представлена схема процесса управления рисками в соответствии с вышеперечисленными стандартами. Таким образом, относительно цикла Деминга, система управления рисками включает в себя следующие процессы:

1. Оценка рисков: инвентаризация активов, идентификация бизнес-требований и требований законодательства, оценка ценности активов, анализ угроз и уязвимостей, определение величины риска, оценивание и ранжирование рисков;
2. Обработка рисков: выбор способов обработки рисков и вариантов контрмер, принятие решения по контрмерам, реализация контрмер;
3. Контроль и пересмотр: аудит и анализ со стороны руководства, оценка эффективности контрмер, мониторинг и анализ риска;
4. Совершенствование: реализация превентивных и корректирующих мер.

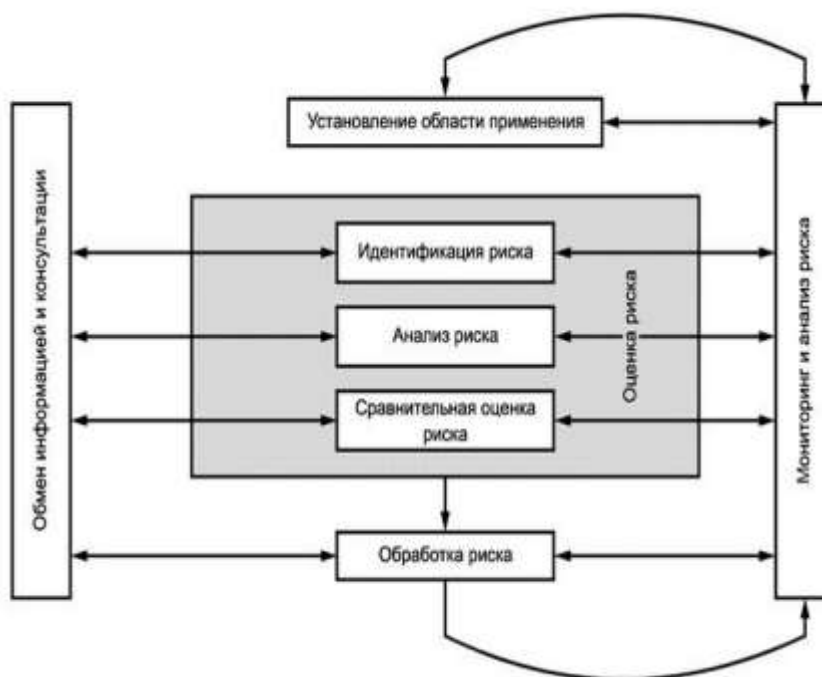


Рис. 1. Схема процесса управления рисками

Разработка безопасного программного обеспечения

При РБПО необходимо проводить управление рисками ИБ. Исходя из возможности интегрирования СМРБПО в качестве подсистемы СМИБ подход должен быть аналогичным [7]. Говоря о рисках в контексте СМИБ, вычисление и определение рисков выполняется для активов организации. В контексте РБПО активом является сама программа (код программы, обрабатываемая информация, сведения об архитектуре и т.п.).

Управление рисками ИБ должно включать в себя:

- разработку методики по управлению рисками организации в области РБПО и их анализу;
- анализ информационных ресурсов организации с целью выявления угроз и уязвимостей защищаемых проектов (разрабатываемого программного обеспечения);

- инвентаризацию проектов всех стадий жизненного цикла;
- проведение консультаций для специалистов организации и оценку соответствия фактического и необходимого уровня безопасности;
- расчет рисков, определение текущего и допустимого уровня риска для каждого конкретного проекта;
- ранжирование рисков, выбор комплексов мероприятий по их снижению и расчет теоретической эффективности внедрения.

Выбор метода оценки рисков

Задача выбора метода для проведения оценки рисков в СМРБПО состоит из трех этапов [8]:

1. Из тридцать одного метода, описанного в ГОСТ Р ИСО/МЭК 31010 выбираются пригодные для управления рисками при РБПО;
2. Из выбранных методов выбираются оптимальные;
3. Выбирается наиболее предпочтительное сочетание методов оценки рисков.

Таблица 1.

Показатели методов оценки риска ИБ при РБПО

Показатель	Смысловое значение показателя
$P_{сл}$	Сложность проблемы и методов, необходимых для оценки риска
P_n	Характер и степень неопределенности оценки риска, основанной на доступной информации и соответствии целям
$P_{рес}$	Необходимые ресурсы: временные, информационные
P_k	Возможность получения количественных оценок выходных данных
$P_{обл}$	Область применения метода к заданной сфере
$P_{пр}$	Применимость к определенному процессу оценки риска (идентификация риска, анализ риска, сравнительная оценка риска)

Расчет частных показателей ($P_{сл}$, P_n , $P_{рес}$, P_k , $P_{обл}$, $P_{пр}$) осуществляется на основе эвристических методов путем определения адекватности метода предъявляемым к нему требованиям на основе анализа описательных данных, представленных в приложениях ГОСТ Р ИСО/МЭК 31010.

Пусть

1. Каждое i –ое свойство j -ого метода, $i = \overline{1, n}$, $j = \overline{1, m}$ описывается переменной p_i^j , которая отображает определенное существенное свойство метода. Показатель p_i^j может принимать значение из множества допустимых значений $\langle p_i^{доп} \rangle$.

2. Вектор $P^j = \langle p_1^j, p_2^j, \dots, p_n^j \rangle$ – обобщенный показатель качества j -ого метода, компоненты которого являются показателями его отдельных свойств.

3. $P^* = \langle p_1^*, p_2^*, \dots, p_n^* \rangle$ – вектор идеального метода, тогда область адекватности показателя качества метода определяется

$$\delta \subseteq |P^{доп} / P^*| / |P^*| \quad (1)$$

Тогда критерии можно выразить следующим образом:

Этап 1. Критерий пригодности метода

$$K^{приг}: (\forall_i)(p_i^j \in \delta | \delta_i \rightarrow p_i^{доп}, i = \overline{1, n}) \quad (2)$$

Согласно этому выражению j -ый метод является пригодным, если значение всех i -х частных показателей p_i^j этого метода принадлежит области адекватности δ , а радиус этой области соответствует допустимым значениям всех частных показателей.

Этап 2. Критерий оптимальности метода

$$K^{\text{опт}}: (\exists_i)(p_i^j \in \delta | \delta_i \rightarrow \delta^{\text{доп}}) \quad (3)$$

Согласно этому выражению j -ый метод является оптимальным, если существует хотя бы один частный показатель p_i^j , значение которого принадлежит области адекватности, а радиус этой области по этому показателю оптимален.

Этап 3. Критерий превосходства метода

$$K^{\text{прев}}: (\forall_i)(p_i^j \in \delta | \delta_i \rightarrow \delta^{\text{опт}}, i = \overline{1, n}) \quad (4)$$

Согласно этому выражению j -ый метод превосходит другие, если все значения частных показателей p_i^j принадлежат области адекватности, а радиус этой области оптимален по всем показателем.

Таблица 2.

Результаты выбора метода оценки рисков ИБ

Этап оценки риска	Пригодные	Оптимальные	Предпочтительные
Идентификация риска	B.1, B.2, B.4, B.5, B.6, B.7, B.8, B.9, B.10, B.11, B.13, B.14, B.15, B.16, B.17, B.18, B.20, B.22, B.23, B.24, B.29, B.30, B.31	B.1, B.2, B.4	B.1, B.2
Анализ риска	B.6, B.7, B.8, B.9, B.10, B.11, B.12, B.13, B.14, B.15, B.16, B.17, B.18, B.19, B.20, B.21, B.22, B.24, B.26, B.29, B.30, B.31	B.9, B.11, B.12, B.13, B.15, B.17, B.18, B.19, B.20, B.22, B.23, B.28, B.29	B.28, B.29
Сравнительная оценка риска	B.6, B.7, B.8, B.9, B.10, B.11, B.12, B.13, B.14, B.16, B.19, B.20, B.21, B.22, B.25, B.26, B.29, B.30, B.31	B.14, B.16, B.19, B.20, B.21, B.22, B.25, B.26, B.29	B.29

Перечислим наименование методов в соответствии с Приложением В ГОСТ Р ИСО/МЭК 31010 с указанием индексов (Таблица 2): B.1 Мозговой штурм; B.2 Структурированные или частично структурированные интервью; B.3 Метод Дельфи; B.4 Контрольные листы; B.5 Предварительный анализ опасностей (РНА); B.6 Исследование опасности и работоспособности (HAZOP); B.7 Анализ опасности и критических контрольных точек (НАССР); B.8 Оценка токсикологического риска; B.9 Структурированный анализ сценариев методом "Что, если?" (SWIFT); B.10 Анализ сценариев; B.11 Анализ воздействия на бизнес (BIA); B.12 Анализ первопричины (RCA); B.13 Анализ видов и последствий отказов (FMEA); B.14 Анализ дерева неисправностей (FTA); B.15 Анализ дерева событий (ETA); B.16 Анализ причин и последствий; B.17 Причинно-Следственный анализ; B.18 Анализ уровней защиты (LOPA); B.19 Анализ дерева решений; B.20 Анализ влияния человеческого фактора (HRA); B.21 Анализ "галстук-

бабочка"; В.22 Техническое обслуживание направленное на обеспечение надежности; В.23 Анализ скрытых дефектов (SA); В.24 Марковский анализ; В.25 Моделирование методом Монте-Карло; В.26 Байесовский анализ и сети Байеса; В.27 Кривые FN; В.28 Индексы риска; В.29 Матрица последствий и вероятностей; В.30 Анализ эффективности затрат (CBA); В.31 Мультикритериальный анализ решений (MCDA).

Вывод

В ходе рассмотрения риск-ориентированного подхода при РБПО, была решена задача по выбору метода оценки рисков ИБ на основе критериев пригодности, оптимальности и превосходства. Выбранные методы аналогичны используемым при управлении рисками ИБ в СМИБ. Таким образом, возможно использовать аналогичные СМИБ процедуры управления рисками ИБ [9, 10], а также СМРБПО может быть интегрирована в СМИБ, что не противоречит общей концепции.

Литература

1. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения/А. В. Барабанов, А. С. Марков, В. Л. Цирлов//Вопросы кибербезопасности. 2015. № 5 (13). С. 2-10.
2. Гришин М.И., Марков А.С., Цирлов В.Л. Практические аспекты реализации мер по разработке безопасного программного обеспечения // ИТ-Стандарт. 2019. № 1.
3. Петренко С.А., Курбатов В.А. Политики безопасности компании при работе в Интернет. - СПб.: ДМК Пресс, 2011. - 396 с.
4. Barabanov A., Fadin A., Tsirlov V., Markov A., Shakhlov I. Synthesis of Secure Software Development Controls. In: ACM International Conference Proceeding Series 8. Ser. "Proceedings of the 8th International Conference on Security of Information and Networks, SIN 2015" 2015. P. 93-97.
5. Barabanov A., Grishin M., Markov A., Tsirlov V. Current Taxonomy of Information Security Threats in Software Development Life Cycle. In: 2018 IEEE 12th International Conference Application of Information and Communication Technologies (AICT). IEEE (17-19 Oct 2018, Almaty, Kazakhstan). 2018. P. 356-361. DOI: 10.1109/icaict.2018.8747065.
6. Petrenko S. La Administración de la Ciberseguridad. Industria 4.0. Publicado según la decisión del consejo de redacción de la Universidad de Innopolis. Universidad de Oviedo, Universidad de Innopolis. Oviedo, Asturias, 2019.
7. Райкова Н.О. Анализ нормативной базы в области разработки безопасного программного обеспечения // Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 152-156.
8. Райкова Н.О. Современные методы анализа рисков применительно к решению задач информационной безопасности // Труды международного симпозиума Надежность и качество. 2015. Т. 1. С. 85-86.
9. Дорофеев А.В., Менеджмент информационной безопасности: управление рисками// Вопросы кибербезопасности. 2014. № 2(3). С. 66-73.
10. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий. - М.: ДМК Пресс, 2017. 224 с.

Научный руководитель: Марков Алексей Сергеевич, доктор технических наук, профессор МГТУ им. Н.Э. Баумана, a.markov@bmstu.ru

Risk-based Approach in the Concept of Developing Secure Software

Raykova N.O.²⁴³

²⁴³ Raykova Natalya Olegovna, Information Security Department, BMSTU, Moscow, e-mail: natalya_raykova@mail.ru

This article describes risk-based approach in the concept of secure software management system based on the requirements of international standards in the field of information security. We examined the information security risk management procedures in detail. We have solved the problem of choosing methods for assessing information security risks in the field of developing secure software. As a result, we conclude that risk management procedures are similar to those used in the information security management system.

Keywords: *secure software development management system, risk assessment methods, management systems, software vulnerability.*

Вероятностный анализ риска воздействия кибератак на системы электронного банкинга

Ревенков П.В.²⁴⁴, Бердюгин А.А.²⁴⁵

Обращается внимание на факторы работы в киберпространстве, повышающие уровни банковских рисков. Проанализированы взаимосвязи кибератак на банковские автоматизированные системы и возможных последствий для банка. Делаются попытки сформулировать математическую модель вероятностного анализа инцидентов информационной безопасности для оптимизации алгоритма реагирования на инциденты. Расчёты на основе предложенной модели позволили определить продолжительность эксплуатации уязвимости электронной банковской системы, когда вероятность предотвращения инцидента превышает вероятность его реализации. Вклад исследования в науку заключается в повышении эффективности оценки риска для решения текущих задач, с учётом инновационных систем и технологий, ожидающих нас в будущем. Результаты работы могут быть использованы для научных исследований рисков нарушения информационной безопасности в системах электронного банкинга.

Ключевые слова: киберпреступность, риск воздействия кибератак, система электронного банкинга, инцидент информационной безопасности

Введение

Эрих Фромм, немецкий философ и социальный психолог XX века, отмечал, что война качественно изменилась. Враги перестали смотреть друг другу глаза в глаза: «Современная война в воздухе следует принципам современного автоматизированного производства, в котором и рабочие, и инженеры полностью отчуждены от своего труда. В соответствии с общим планом производства и управления они выполняют технические задания, не видя конечного продукта. Но даже если они видят готовую продукцию, она их прямо не касается, они за неё не отвечают, она лежит вне сферы их ответственности. От них никто не ждёт, что они спросят, что несёт эта продукция – пользу или вред. Это решают управляющие. Что же касается управляющих, то для них «полезно» все то, что «выгодно» (и что приносит пользу предприятию), а это не имеет ничего общего с объективной оценкой полезности продукта. В войне «полезно» то, что служит уничтожению противника, и решения о том, что в этом смысле полезно, часто принимаются на основе весьма приблизительных данных» [1].

Подобный процесс мы наблюдаем, когда говорим о киберпреступности. Снимая деньги с карточки, мошенник никогда не видит в глаза свою жертву, он свободен от созерцания последствий своего поступка. Слезы и отчаяние жертвы не тронут его, он просто их не увидит. Но делает ли это его поступок более этичным?

Другая аналогия, которая прослеживается между войной прошлого века и современной киберпреступностью, массовые жертвы среди мирного населения: современные преступники не охотятся исключительно на богатых бизнесменов. Они работают «в толпе», списывая по мелочи и у старушки-пенсионерки, и у студента, и у служащего.

²⁴⁴ Ревенков Павел Владимирович, доктор экономических наук, профессор кафедры «Информационная безопасность», Финансовый университет при Правительстве Российской Федерации, город Москва, e-mail: pavel.revenkov@mail.ru. orcid.org/0000-0002-0354-0665

²⁴⁵ Бердюгин Александр Александрович, аспирант кафедры «Информационная безопасность», Финансовый университет при Правительстве Российской Федерации, город Москва, e-mail: a40546b@gmail.com. orcid.org/0000-0003-2301-1776

В данной статье (применительно к кредитно-финансовой сфере) авторы используют термин «риск воздействия кибератак» (РВКа), под которым понимается мера возрастания типичных банковских рисков (включая финансовые потери), возникающие вследствие реализации кибератак на банковские автоматизированные системы (БАС) [2, 3].

Цель исследования состоит в том, чтобы проанализировать причинно-следственные связи при влиянии компьютерных атак на типичные банковские риски и разработать новые (применимые на практике в кредитно-финансовой сфере) подходы к оценке РВКа, за счёт которых можно значительно повысить качество обеспечения кибербезопасности в организациях кредитно-финансовой сферы.

Расширение профилей типичных рисков банка за счёт кибератак

Работа в киберпространстве, в первую очередь, повышает техническую составляющую всех типичных банковских рисков (рис. 1), среди которых в большей степени можно выделить операционный, правовой, стратегический, репутационный и риск ликвидности²⁴⁶ [4-7].

Основные виды кибератак на БАС, отмеченные в ежегодных отчётах ФинЦЕРТ Банка России и компании Group-IB – это:

- атаки на автоматизированное рабочее место клиента Банка России (АРМ КБР);
- атаки на автоматизированное рабочее место клиента международной системы передачи финансовой информации SWIFT (АРМ SWIFT);
- атаки на автоматизированное рабочее место администратора систем электронного банкинга (АРМ СЭБ);
- атаки на устройства самообслуживания (Automated teller machine – банкоматы).

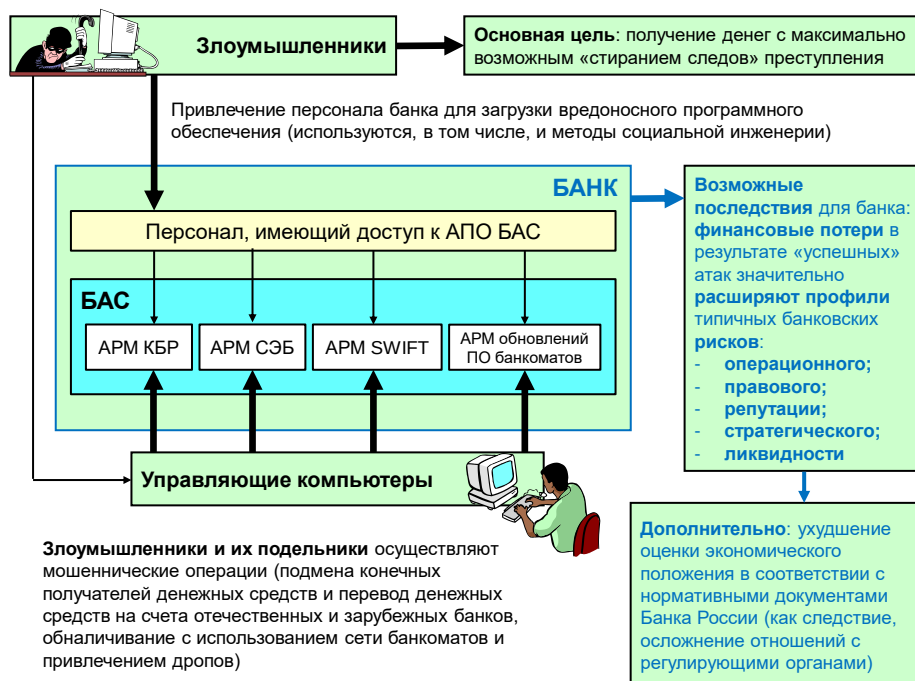


Рис. 1. Взаимосвязь кибератак на аппаратно-программное обеспечение (АПО) БАС и возможных последствий для банка²⁴⁷. Составлено авторами

²⁴⁶ Полный перечень типичных банковских рисков приведён в Письме Банка России от 23 июня 2004 года «О типичных банковских рисках» № 70-Т.

²⁴⁷ На рисунке ПО – программное обеспечение.

Оценка специалистами риск-подразделений проявлений РВКа должна проводиться своевременно, с последующим уведомлением руководства кредитной организации, чтобы руководство кредитной организации могло своевременно принимать превентивные меры [8, 9].

Формализация модели оценки РВКа на СЭБ

Представленный метод учёта РВКа может быть использован как специалистами риск-подразделений, так и сотрудниками служб внутреннего контроля. Использование этого отношения для менеджмента непрерывности деятельности кредитной организации может стать основой для оценки резервируемого капитала под РВКа на СЭБ.

Значительную часть пространственно-временного континуума (space-time) необходимо научно исследовать, если мы должны получить надёжные результаты. В противном случае можно прийти к ложным выводам [10-12]. Математическое представление РВКа может быть представлено в виде модели, которая лежит в основе классической для теории вероятностей «задачи о встрече» (в нашем случае встречаются киберпреступник и антихакер в сети). Противники действуют в киберпространстве независимо в любой период времени T , их нахождение в сети дискретно ввиду человеческого фактора. Допустим, что:

S_1 – событие 1 (заключается в проникновении хакера в локальную вычислительную сеть);

S_2 – событие 2 (заключается в эксплуатации уязвимости СЭБ);

S_3 – событие 3 (реализация компьютерного инцидента и кража денег).

Событие S_1 означает поступление сигнала системы кибербезопасности и запуск процесса реагирования. Моменты нахождения вышеуказанных лиц в сети обозначим через a и b соответственно и изобразим их на оси aOb (рис. 2).

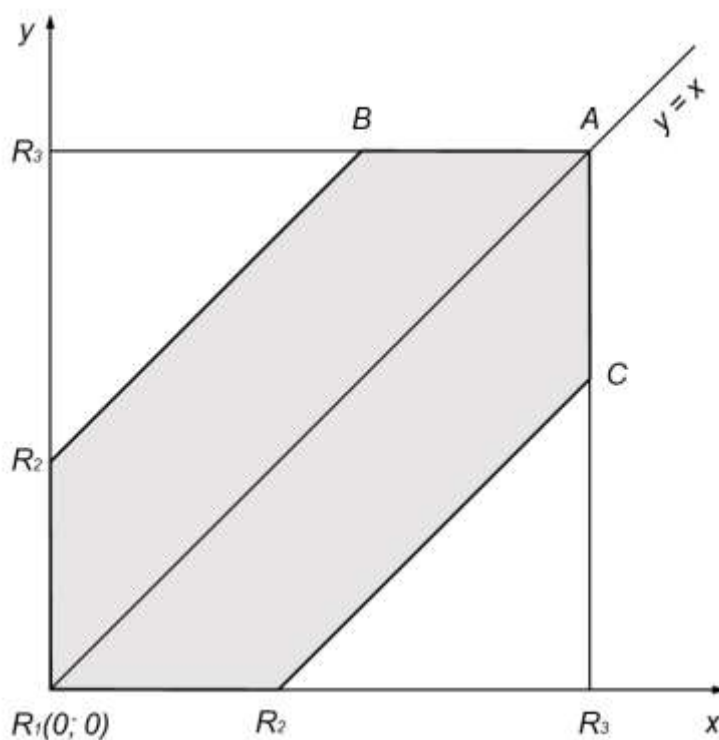


Рис. 2. Представление задачи о встрече в декартовой системе координат. Составлено авторами

Из условий задачи следуют двойные неравенства:

$$0 \leq a \leq S_3 \text{ и } 0 \leq b \leq S_3 \quad (1)$$

Неравенствам соответствуют координаты любой точки квадрата $S_1 S_3 A S_3$.

Обозначим этот квадрат фигурой F . Точки фигуры F имеют координаты, соответствующие значениям пребывания киберпреступника и антихакера online. Компьютерный инцидент может быть предотвращён до тех пор, пока разница между нахождением противников в сети меньше, чем S_2 . То есть

$$\begin{cases} b - a \leq S_2 \text{ при } b > a \\ a - b \leq S_2 \text{ при } a > b \end{cases} \quad (2)$$

По свойству абсолютной величины числа система равносильна неравенству:

$$|a - b| \leq S_2 \quad (3)$$

Координаты точек встречи противников попадают в фигуру $S_1 S_2 B A C S_2$. Назовём этот шестиугольник фигурой f . Тогда вероятность реализации РВКа равна:

$$P_{\text{РВКа}} = \frac{\text{площадь } f}{\text{площадь } F} = \frac{S_3^2 - (S_3 - S_2)^2}{S_3^2} = \frac{S_2 \cdot (2S_3 - S_2)}{S_3^2} \quad (4)$$

Соответственно вероятность противоположного события (предотвращения компьютерного инцидента – ПКИ) равна:

$$P_{\text{ПКИ}} = 1 - P_{\text{РВКа}} \quad (5)$$

Рассмотрим, как модель действует «в цифрах». Например, банк определил своей политикой информационной безопасности (или кибербезопасности) максимальное время реагирования на инцидент информационной безопасности – не более 90 минут. Исходя из этого $S_3 = 90$. Вычислим значения $P_{\text{РВКа}}$ и $P_{\text{ПКИ}}$ по формулам (5) и (6) для различных значений S_2 (табл. 1):

Таблица 1.

Определение параметров реагирования на компьютерную атаку

S_2	2	45	85
$P_{\text{РВКа}}$	$\frac{2 \cdot (2 \cdot 90 - 2)}{90^2} \approx 0,044$	$\frac{45 \cdot (2 \cdot 90 - 45)}{90^2} \approx 0,75$	$\frac{85 \cdot (2 \cdot 90 - 85)}{90^2} \approx 0,997$
$P_{\text{ПКИ}}$	0,956	0,25	0,003

Отсюда можно определить значение S_2 , при котором реализация и предотвращение РВКа равновероятны, т.е. $P_{\text{ПКИ}} = P_{\text{РВКа}} = 0,5$:

$$\begin{aligned} \frac{x \cdot (2 \cdot 90 - x)}{90^2} &= 0,5 \\ 180x - x^2 &= 0,5 \cdot 90^2 \end{aligned} \quad (6)$$

$$x^2 - 180x + 4050 = 0$$

Корнями уравнения являются $x_1 \approx 153,6$ и $x_2 \approx 26,4$. Но значение $x_1 \approx 153,6$ не удовлетворяет условию задачи, т.к. превышает $S_3 = 90$. Поэтому если уязвимость СЭБ

эксплуатируется не дольше $S_2 \approx 26,4$ минут, то вероятность предотвращения инцидента превышает вероятность его реализации. Другими словами, чем дольше сохраняется уязвимость в БАС (включая СЭБ), тем больше шанс кражи денег за счёт её использования.

Таким образом, предложенная авторами методика оценки РВКа позволяет проанализировать случившиеся ранее инциденты информационной безопасности для определения их относительной частоты с дальнейшим прогнозированием реагирования на инциденты и оптимизацией алгоритма реагирования. За счёт её внедрения в методики оценки рисков [13-15], используемые подразделениями по обеспечению кибербезопасности, можно значительно повысить эффективность мер, направленных на минимизацию возможных последствий проявления РВКа.

Заключение

- новые вызовы и вопросы кибербезопасности, которые возникают перед кредитными организациями и их клиентами, использующими СЭБ, требуют непрерывного совершенствования решений и нередко существенного пересмотра процедур риск-менеджмента, к которым относятся процедуры внутреннего контроля в условиях работы в киберпространстве;

- внедрение СЭБ позволяет кредитным организациям значительно сократить затраты на операционные расходы, но при этом работа банка в киберпространстве сопряжена с дополнительными источниками типичных банковских рисков, к которым относятся: операционный, правовой, стратегический риски, риск ликвидности, а также риск потери деловой репутации;

- проведение учёта и оценки РВКа на основе риск-ориентированного подхода должно подразумевать соответствие каждой причине реализации РВКа возможных последствий для банка (связанных с нарушением непрерывности предоставления банковской деятельности, снижением качества электронных банковских услуг, финансовыми потерями и др.) [16, 17];

- научно-исследовательские и опытно-конструкторские разработки учёных должны быть одним из «столпов» структуры управления РВКа на СЭБ [18].

Литература

1. Фромм Э. Анатомия человеческой деструктивности: Перевод / Авт. вступ. ст. П.С. Гуревич. – М.: Республика, 1994. 447 с.
2. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1 (25). С. 28-38.
3. Ревенков П.В., Пименов П.А., Ожеред И.В. Противодействие компьютерным атакам в условиях применения систем электронного банкинга: Учебное пособие. М.: Прометей, 2019. 158 с.
4. Бердюгин А.А. Разработка алгоритма оценки риска воздействия кибератак в условиях электронного банкинга. // Безопасность информационных технологий, 2019. Т. 26, N. 2, с. 86-94. DOI: 10.26583/bit.2019.2.06.
5. Бердюгин А.А. Подход к управлению защитой информации в системах электронного банкинга. В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 24-27.
6. Ревенков П.В., Крупенко Д.С. Оценка рисков информационной безопасности в условиях применения систем мобильного банкинга // Вопросы кибербезопасности. 2019. № 2 (30). С. 21-28.
7. Ярыгина И.З., Гисин В.Б. Методологические подходы к оценке стоимости банковских активов как методу управления финансовыми рисками // Банковские услуги. 2019. № 2. С. 20–26.
8. Козьминых С.И. Моделирование обеспечения информационной безопасности объекта кредитно-финансовой сферы // Финансы: теория и практика. 2018. Т. 22. № 5 (107). С. 105-121. DOI: 10.26794/2587-5671-2018-22-5-105-121.

9. Макеев С.А. Проблемы нейтрализации негативных информационных воздействий на бизнес-процесс кредитной организации // Вопросы кибербезопасности. 2015. № 5 (13). С. 51-54.
10. Шеремет И.А. Цифровая экономика и кибербезопасность ее финансового сегмента // Научные труды Вольного экономического общества России. 2018. Т. 210. № 2. С. 23-34.
11. Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In: Proceedings of 2017 IEEE 2nd International Conference on Control in Technical Systems, CTS 2017 2. 2017. P. 96-99.
12. Turing A.M., Neumann J.v. and Yanovskaya S.A. (2018) *Mozhet li mashina myslit'? Obshchaya i logicheskaya teoriya avtomatov. Per. s angl. 3-e izd.* [Can the machine think? General and logical theory of automata. Trans. from Eng. 3rd ed.], Lenand Publisher, Moscow, 232 p.
13. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
14. Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. -London: IntechOpen, 2018. 278 p.
15. Александров А.А., Ларионов В.И., Суцев С.П. Анализ и управление техногенными и природными рисками. – М.: МГТУ им.Н.Э. Баумана, 2019, 357 с.
16. Касперская Н.И. и др. К проблеме оценки и обеспечения корректности бизнес-процессов. // Безопасность информационных технологий, 2019, Т. 26, N. 3, с. 8-21. DOI: 10.26583/bit.2019.3.01.
17. Skinner C. (2018) Digital Human: The Fourth Revolution of Humanity Includes Everyone, Singapore: Marshall Cavendish International (Asia).
18. Шеремет И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере // Вопросы кибербезопасности. 2016. № 5 (18). С. 3-7.

Probabilistic analysis of risk of cyberattacks on electronic banking systems

Revenkov P.V.²⁴⁸, Berdyugin A.A.²⁴⁹

Attention is drawn to the factors of work in cyberspace that increase the levels of banking risks. The relationship of cyberattacks on banking automated systems and possible consequences for the bank is analyzed. Attempts are made to formulate the mathematical model of the probabilistic analysis of information security incidents to optimize the algorithm for responding to incidents. Calculations based on the proposed model made it possible to determine the duration of exploitation of vulnerability of electronic banking system, when the probability of preventing an incident exceeds probability of its realization. The contribution of research to science is to increase the effectiveness of risk assessment for solving current challenges, considering innovative systems and technologies that await us in the future. The findings may be useful for scientific research on the risks of information security breach in electronic banking systems.

Keywords: *cybercrime, risk of cyberattacks, electronic banking system, information security incident*

²⁴⁸ Revenkov Pavel Vladimirovich, Doctor of Economic sciences, Professor of the Department «Information Security», Financial University under the Government of the Russian Federation, Moscow, e-mail: pavel.revenkov@mail.ru. orcid.org/0000-0002-0354-0665

²⁴⁹ Berdyugin Alexander Alexandrovich, Post-graduate student of the Department «Information Security», Financial University under the Government of the Russian Federation, Moscow, e-mail: a40546b@gmail.com. orcid.org/0000-0003-2301-1776

Новые технологии: вызовы международной безопасности и стабильности Ромашкина Н.П.²⁵⁰

Аннотация. В статье представлены результаты анализа актуальных военно-политических вызовов и угроз в сфере международной информационной безопасности, которые носят глобальный, стратегический характер. Выявлены основные факторы глобального влияния информационно-коммуникационных технологий (ИКТ) на стратегическую стабильность. Представлен анализ современных подходов к определению понятия стратегической стабильности в эпоху ИКТ, а также новые характеристики нестабильности современной международной военно-политической системы. Обоснован вывод о необходимости развития механизмов международного управления в этой области, частью которых могут стать предложенные автором конкретные международные действия с участием России в ответ на актуальные глобальные вызовы международной безопасности и стратегической стабильности.

Ключевые слова: информационная безопасность, информационно-коммуникационные технологии (ИКТ), стратегическая стабильность, информационное оружие, информационная угроза, ИКТ-угроза, ИКТ-атака, кибер-электромагнитная деятельность, ядерное оружие.

Введение

В 21 веке информационно-технологическая революция поставила перед человечеством принципиально новые вопросы, которые уже носят международный, глобальный характер. Вместе с уникальными возможностями ускоренно развивающиеся информационно-коммуникационные технологии (ИКТ) несут глобальные вызовы и угрозы. Методы с использованием ИКТ превращаются в важный элемент военно-политического потенциала государств, дополняющий, а иногда и заменяющий традиционные политико-дипломатические средства и вооружения. Информационные войны одних государств против других могут оказаться не менее разрушительными, чем войны традиционные, а новые технологии могут стать детонатором развязывания межгосударственного военного конфликта с применением стратегического и даже ядерного оружия (ЯО). В настоящее время новые ИКТ уже активно применяются в военной организации и инфраструктуре, и это объективно создает новые проблемы. Важнейшим является блок ИКТ-угроз в сфере стратегических и, в частности, ядерных вооружений. Таким образом, ИКТ уже оказывают влияние на уровень стратегической стабильности. Поэтому в современную цифровую эпоху обеспечение международной безопасности и стратегической стабильности становится одной из важнейших задач мирового сообщества, требует развития и модернизации механизмов международного управления. При этом речь не идет о необходимости в корне менять основополагающие принципы управления, т.к. ИКТ-угрозы обостряют, осложняют, углубляют, усиливают и видоизменяют ранее существовавшие в этой области проблемы.

Глобальные военно-политические вызовы в сфере информационной безопасности

Современные информационные операции предоставляют уникальные возможности для создания деструктивного эффекта в военно-политической сфере. Угрозы применения новых технологий обусловлены развитием ИКТ-вооружений (средства борьбы с системами управления и контроля; разведывательное противоборство; электронное противоборство;

²⁵⁰ Ромашкина Наталия Петровна, кандидат политических наук, профессор, член-корреспондент АВН РФ, Руководитель подразделения проблем информационной безопасности ЦМБ ИМЭМО РАН, Москва, Romachkinan@yandex.ru.

военные средства, способствующие проведению информационных операций); использованием ИКТ для вмешательства во внутренние дела государств (ИКТ-воздействие на промышленные и финансовые объекты; пропагандистское иновещание, Интернет, мобильные приложения для подготовки и проведения массовых беспорядков, антиправительственных демонстраций, политических акций, государственных переворотов); развитием ИКТ-средств для вредоносного воздействия на объекты ВПК [1].

Угрозы международной безопасности дополнительно усиливаются в связи с развитием *ударных роботизированных средств* с дистанционным управлением [2], *искусственного интеллекта* в военных целях, машинного обучения, возможностями автономной работы различных систем и подсистем, автоматизированных систем принятия решений и т.д., которые могут подвергаться ИКТ-атакам [3], средств *кибер-электромагнитной деятельности*, которую активно развивают в США [4,5].

Помимо технологических характеристик существует еще и психологическая, которую можно сформулировать как утрату страха перед ядерной войной у общества и политических элит Запада, что может существенно снизить порог применения вооружений. При этом максимально опасной является убежденность в возможности локальной «небольшой» ядерной войны и победы в ней. Тенденция к распространению подобных взглядов возникла и при помощи современных ИКТ, позволяющих оказывать воздействие на огромную аудиторию за относительно короткие сроки и без серьезных экономических затрат.

При этом оценка ущерба и выработка мер противодействия существенно затруднены из-за «неосязаемости» ИКТ, а также широкого спектра источников возможных вредоносных технологий: государственных и негосударственных акторов, хакеров-одиночек. Все это повышает уровень неопределенности и нестабильности. Следовательно, одной из важнейших актуальных угроз, связанных с ИКТ, в сфере международной безопасности является снижение уровня стратегической стабильности.

Влияние ИКТ на уровень стратегической стабильности

В течение многих лет понятие *«стратегическая стабильность»* определялось как *состояние взаимоотношений ядерных держав, при котором устраняются стимулы к нанесению первого ядерного удара* [6]. ЯО по-прежнему существует, его разрушительные возможности постоянно совершенствуются, поэтому и сегодня это понятие также актуально, как и в период холодной войны. Однако за последние три десятилетия геополитическая и технологическая ситуация существенно усложнилась. Следовательно, учитывая общепринятые характеристики, необходимо выработать новые подходы к оценке уровня стратегической стабильности, и общих для ключевых акторов критериях оценки. Кроме того, речь идет уже не о двух глобальных полюсах противостояния, а об увеличении количества субъектов, влияющих на уровень стратегической стабильности. Поэтому необходимо оценивать характеристики военно-политической системы.

Стратегическая стабильность военно-политической системы – это *состояние мира (отсутствие широкомасштабной войны) в рамках этой системы, которое поддерживается даже при постоянно действующих возмущениях (дестабилизирующих факторах) в течение определенного (заданного) периода времени* [7].

Можно выделить основные факторы влияния ИКТ на стратегическую стабильность:

- использование ИКТ в деструктивных военно-политических целях;
- соблазн одержать победу в широкомасштабной войне, связанный с развитием новых технологий, подталкивающих к приобретению стратегических преимуществ;
- тенденция к исчезновению границ между мирным состоянием государств и переходом их в состояние войны, размытие границ между обороной и нападением в военном планировании;

- изменение логики глобального противоборства, когда комплексное применение невоенных методов с использованием вредоносных ИКТ приводит к достижению целей войны даже без вооруженной борьбы (рис. 1,2);
- сокращение «лестницы» эскалации конфликта, связанное с ростом вероятности ИКТ-атак на элементы военной ракетно-ядерной инфраструктуры [8].



Рис. 1. Этапы классического противоборства без комплексного применения ИКТ.



Рис. 2. Этапы противоборства с широкомасштабным применением ИКТ.

Анализ доказывает, что все факторы, дестабилизирующие современную систему стратегической стабильности, связаны с развитием ИКТ и усугубляются их использованием в деструктивных целях [9]. Поэтому соответствующие ИКТ-угрозы целесообразно

выделять в качестве отдельного дестабилизирующего фактора. Механизмы управления в этой сфере в настоящее время отсутствуют, что, в частности, сказывается на снижении уровня стратегической стабильности по сравнению с периодом биполярности.

Снижение уровня стратегической стабильности обусловлено влиянием вредоносных ИКТ на рост вероятности:

- ошибочного санкционированного запуска баллистических ракет (БР);
- получения ложной информации от СПРН о запуске БР со стороны противника из-за растущей изоэшелонности ИКТ-атак;
- повреждения или разрушения каналов коммуникаций, создания помех в системе управления, командования и контроля ВС;
- снижения уверенности военных, принимающих решения, в работоспособности систем управления, командования и контроля ВС [10, 11].

Выводы

1. Самые опасные ИКТ-угрозы международной безопасности и стабильности: применение информационного оружия в военно-политических целях для осуществления враждебных действий и актов агрессии; деструктивное ИКТ-воздействие на элементы критически важных объектов государственной инфраструктуры; вмешательство во внутренние дела суверенного государства, нарушения общественной стабильности, разжигание межэтнической, межнациональной розни посредством ИКТ. Наличие этих опасностей требует поиска дополнительных механизмов международного управления.
2. Ситуация в области стратегической стабильности может оцениваться как кризисная. В условиях угрозы военного столкновения между ядерными державами и отсутствия переговоров по ограничению и сокращению ЯО существующих механизмов международного управления в этой области недостаточно.
3. В контексте обеспечения стратегической стабильности особого внимания требует безопасность ракетно-ядерных вооружений. Все ядерные державы модернизируют ядерные системы, стремясь внедрять новые компьютерные технологии. Все больше компонентов военной ядерной инфраструктуры – от боеголовок и средств их доставки до систем управления и наведения, систем командования и контроля стратегических ядерных сил (СЯС) – зависят от сложного программного обеспечения, что делает их потенциальными мишенями для ИКТ-атак.
4. Особого внимания требует защита стратегических вооружений, система СПРН, противовоздушной (ПВО) и противоракетной обороны (ПРО), командования и контроля над ЯО. При этом в дополнение или вместо принципа сдерживания за счет неминуемого ответного удара, растет интерес к сдерживанию путем блокирования использования наступательных средств («блокирование пуска», "left of launch") с помощью ИКТ.
5. Самой опасной, не гипотетической, а уже реальной является угроза влияния ИКТ на принятие решения о применении ЯО, т.е. на рост вероятности ошибочного санкционированного запуска БР в результате получения неверной информации или отсутствия уверенности военных в правильности работы систем и восприятия каких-то действий в качестве начального этапа перехода к условиям гарантированного взаимного уничтожения. Это существенно снижает уровень стратегической стабильности.
6. В этих условиях целесообразны международные действия с участием России в ответ на актуальные глобальные вызовы международной безопасности и стратегической стабильности:

- возобновление переговоров РФ-США по ограничению и сокращению стратегических ракетно-ядерных вооружений; привлечение других ядерных держав к режиму ограничения и сокращения СЯС;
- выработка и фиксация общего (РФ, США, КНР) понимания критериев стратегической стабильности;
- выработка и фиксация общего (РФ, США, КНР) понимания опасности ИКТ-угроз для международной безопасности и стабильности;
- выработка общих подходов к оценке вероятности непреднамеренных и преднамеренных ИКТ-атак на СЯС;
- четкая фиксация вероятного ответа в случае обнаружения ИКТ-атак на СЯС в целях обеспечения сдерживания в применении ИКТ-вооружений.

Эти меры могут заложить основу для создания политики сдерживания в ИКТ-среде так, как это было сделано в период биполярности в отношении ядерных вооружений.

Параллельно целесообразно работать над созданием режима контроля над ИКТ-вооружениями, который мог бы включать:

- запрет на ИКТ-атаки на конкретные объекты, в первую очередь, в военной сфере (заявления, обязательства, соглашения, договоры);
- ограничение и/или отказ от наступательных ИКТ-возможностей;
- меры контроля за распространением ИКТ-вооружений;
- международные нормы в отношении средств и методов предотвращения и устранения киберконфликтов;
- разработку конвенции о запрещении вредоносного использования ИКТ в сфере ЯО.

Литература

1. Molander R., Riddile A., Wilson P. Strategic information warfare: a new face of war. Library of Congress Cataloging in Publication Data, RAND (Firm), 1996. 33 p. URL: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf.
2. Балыбин В.А., Высторобский С.Г., Ельцов О.Н., Сырбу И.А. Роботизированные комплексы РЭБ: перспективы создания и применения. Радиоэлектронная борьба в Вооруженных Силах Российской Федерации – 2018. Материалы от войск радиоэлектронной борьбы ВС РФ. 2018, URL: <https://reb.informost.ru/2018/pdf/1-5.pdf>.
3. Проблемы информационной безопасности в международных военно-политических отношениях. Под ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН, 2016, 183 с. URL: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf.
4. Cyber Electromagnetic Activities. Field Manual No. 3-38, Headquarters Department of the Army, Washington, DC, 12 February 2014. URL: <https://info.publicintelligence.net/USArmy-CEMA.pdf>.
5. Горбачев Ю.Е. Радиоэлектронная борьба в сложной электромагнитной обстановке. Радиоэлектронная борьба в Вооруженных Силах Российской Федерации – 2017. Материалы от войск радиоэлектронной борьбы ВС РФ. 2017, URL: <https://reb.informost.ru/2017/pdf/1-3.pdf>.
6. Арбатов А.Г. Роль ядерного сдерживания в стратегической стабильности. Гарантия или угроза. Московский Центр Карнеги, URL: <https://carnegie.ru/2019/01/28/ru-pub-78209>.
7. Ромашкина Н.П. Стратегическая стабильность в современной системе международных отношений. М.: Научная книга, 2008, 288 с., URL: <http://www.avnrf.ru/index.php/drugie-publikatsii/590-strategicheskaya-stabilnost-v-sovremennoj-sisteme-mezhdunarodnykh-otnoshenij>.
8. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1 (10). С. 2-9, URL: https://cyberrus.com/wp-content/uploads/2019/03/02-09-129-19_1.-Romashkina.pdf.
9. Information Security Threats during Crisis and Conflicts of the XXI Century / Eds.: N.P. Romashkina, A.V. Zagorskii. Moscow: IMEMO, 2016. URL: https://www.imemo.ru/files/File/en/publ/2016/2016_001.pdf.

10.Ромашкина Н.П. Перспективы международной информационной безопасности / Безопасность и контроль над вооружениями 2017–2018. Преодоление разбалансировки международной стабильности / отв. ред. А. Г. Арбатов, Н. И. Бубнова. – М.: ИМЭМО РАН; Политическая энциклопедия, 2018.

11.Sherman F. Aborting Unauthorized Launches of Nuclear-Armed Ballistic Missiles through Postlaunch Destruction // Science and Global Security, 1990, Volume 2, No. 1.

**New Technologies:
Challenges to International Security and Stability
Romashkina N.P.²⁵¹**

Abstract. *The article presents the results of the analysis of current politico-military challenges and threats in the field of information security, which are global, strategic in nature. The article describes the main factors of global effect of information and communication technologies (ICTs) on strategic stability. The analysis of modern approaches to define the concept of strategic stability in the ICT era as well as new characteristics of instability of the modern international politico-military system are presented. Arguments underlying the need to develop mechanisms of international governance in this area are provided. Suggested specific international actions performed together with Russia in response to current global challenges to international security and strategic stability may become one of such instruments.*

Keywords: *information security, information and communication technologies (ICTs), strategic stability, information weapons, information threat, ICT threat, ICT attack, cyber-electromagnetic activity, nuclear weapons.*

²⁵¹Nataliya Romashkina, PhD in Political Sciences, Professor, Corresponding member of the Russian Academy of Military Sciences (AMS), Head of the Informational Security Problems Group of the Primakov National Research Institute of World Economy and International Relations (IMEMO) of the Russian Academy of Sciences, Moscow, Romashkinan@yandex.ru

Анализ защищенности высокочастотных бесконтактных смарт-карт Mifare**Сафин И.Р.²⁵², Колосов Д.В.²⁵³**

Аннотация: Mifare является самым популярным чипом RFID, используемым в общественном транспорте, а также в системах контроля и управления доступом различного уровня организаций. В статье дается обзор оборудования и методик анализа защищенности с практическими реализациями, которые используются в атаках на данный чип. Данная статья включает в себя сочетание технических и исторических деталей. История чипа Mifare и компании NXP ярко отображает незащищенности закрытых технологий. Данный вопрос является актуальным, так как касается критических информационных инфраструктур.

Ключевые слова: NXP, Ghost, reverse engineering, Proxmark III, Replay атака, NFC

Введение

Mifare Classic является самой популярной бесконтактной смарт-картой, которая используется для защиты доступа к зданиям, информации в системе общественного транспорта и личной персональной информации. В течение более 20 лет информация об алгоритмах этих карт держалась в секрете. В 2008 году две группы исследователей (Нол и др, 2008 [1-4]; Де Конинг Ганс и др, 2008 [5-6]) с помощью обратной инженерии (reverse engineering) Mifare Classic обнаружили несколько очень серьезных уязвимостей, подробнее в Разделе 1. В результате, можно клонировать карту, если злоумышленник имеет доступ к радиочастотной связи с подлинным считывателем карт (который знает секретный ключ). Может ли система, которая уже содержит серьёзные уязвимости, содержать ещё больше уязвимостей в будущих изучениях? Ответ: Да, существуют незакрытые уязвимости, подробнее в Разделе 3[7-9].

Эта статья не только о криптографии. Речь идет о безопасности смарт-карт и систем контроля и управления доступа во реальной жизни. Основные проблемы данной тематики складываются в несколько вопросов:

- Какова роль секретности при разработке продуктов информационной безопасности в повседневной жизни?
- Существуют ли следы проведения атаки на самих чипах?
- Какие стандарты и законы регламентируют работу со смарт-картами?
- Стоимость атаки и защиты?
- Возможна ли альтернатива?

В разделе 2 обозревается аппаратное и программное обеспечения для проведения анализа. Раздел 4 раскрывает ситуацию с данным чипом на территории Российской Федерации.

Данная статья не способна ответить на все выше поставленные задачи, ввиду небольшого числа исследований. Однако полученные в ходе исследования результаты, раскрытые в Разделе 5, дают все основания полагать, что компании использующие смарт-карты слабо представляют масштабы проблем [10-11, 14].

Полученные результаты исследования

В качестве объекта исследования использовалась транспортная карта Мостраспорта «Тройка». Ознакомившись с результатами исследования энтузиастов [12], легко нашел 10 ключей из 32, открывая новые способы получения ключей. А точнее с помощью технических недостатков современных технологий NFC и приложений для работы с ними. Мостранспорт передавал ключи к шифру Crypto-1, большинству мобильных приложений.

²⁵² Сафин Ильнур Ришатович, студент ИУ8-31М, МГТУ им. Баумана, Москва, safinir@student.bmstu.ru

²⁵³ Колосов Денис Витальевич, студент ИУ7-32Б, МГТУ им. Баумана, Москва, kolosovdv@student.bmstu.ru

С помощью найденных ключей я получил данные транспортной карты, пример представлен на рисунке 1.

```

1  +Sector: 0
2  04306FFA445080084400120111002116
3  00000000000000000000000000000000
4  00000000000000000000000000000000
5  A0A1A2A3A4A57C178800-----
6  +Sector: 2
7  172B3D21230000001096640200000000
8  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
9  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
10 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
11 2AA05ED1056F787788FF-----
12 +Sector: 3
13 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
14 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
15 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
16 2AA05ED1056F787788FF-----
17 +Sector: 4
18 4713500A7558222A6B00000000001129
19 00000000000000000000000000000000
20 00000000000000000000000000000000
21 73060F118C13787788002B7F3253FA05
22 -----
23 +Sector: 6
24 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
25 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
26 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
27 2AA05ED1056F787788FF-----
28 +Sector: 7
29 4503D00A7558222A6B000000000001491
30 00000000000000000000000000000000
31 00000000000000000000000000000000
32 AE3D6A13AD4787788000F1C63D13DBA
33 -----
34 +Sector: 8
35 450B100A7558222A6B000000000000000
36 347C3E3592001D0028D210005AA23DF
37 347C3E3592001D0028D210005AA23DF
38 A73F9DC1D33378778800E3017349A81
39 -----
40 +Sector: 15
41 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
42 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
43 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
44 2AA05ED1056F787788FF-----

```

Рисунок 1 – Пример отображения памяти транспортной карты

В ходе ряда экскрементов было установлено, что сектора 6 и 15 отданы сервисам компании «РЖД» для электропоездов. Сектор 8 отвечает за мостранспорт. За целостностью данных отвечает 64-х битная имитовставка ГОСТ 28147-89 с циклами 3-16. Данной версии придерживается, и публикация 2009 года [13]. Подробнее в Разделе 5. Однако данная защита не помогает с атакой повторного воспроизведения (Replay-attack) и невозможно определить взломанную карту от оригинальной. До 21 ноября 2019 года данную атаку ежедневно эксплуатировали приблизительно 3000 пользователей данной транспортной системы. 21 ноября 2019 года, совместно с вводом МЦД, Мостранспорт впервые за 5 лет обновил ключи.

Целью одной из следующих исследований будет подтверждения или опровержения гипотезы, что другие транспортные системы РФ подвержены данной атаке или другим атакам.

Заключение

В целом, чипы Mifare остаются уязвимы к атакам, однако согласно исследованиям других аналогичных карт, карты Mifare остаются самыми защищенными и практика использования имитовставки отечественных алгоритмов шифрования повышает защиту данных. Однако существует вероятность увеличения пользователей взломанных карт до существенного уровня, где убыток будет критическим. Данная проблема является актуальной, так как в данный момент каждый четвертый пользователь мобильных телефонов является потенциальным злоумышленником.

Литература

1. Gerhard de Koning Gans. Analysis of the MIFARE Classic used in the OVChipkaart project. Master's thesis, Radboud University Nijmegen, 2008.
2. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A practical attack on the Mifare Classic. In Gilles Grimaud and Francois-Xavier Standaert, editors, Smart Card Research and Advanced Application (CARDIS '08), volume 5189 of Lecture Notes in Computer Science, pages 267–282. Springer, 2008.
3. Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling Mifare Classic. In Sushil Jajodia and Javier Lopez, editors, European Symposium on Research in Computer Security (ESORICS '08), volume 5283 of Lecture Notes in Computer Science, pages 97–114. Springer, 2008.
4. Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing borders: Security and privacy issues of the European e-Passport. In Advances in Information and Computer Security, number 4266 in Lecture Notes in Computer Science, pages 152–167. Springer, Berlin, 2006.
5. Karsten Nohl, David Evans, Starbug, and Henryk Plotz. Reverse-engineering a cryptographic RFID tag. In USENIX Security 2008, pages 185–193, 2008.
6. Karsten Nohl and Henryk Plotz. Mifare, little security despite obscurity. Presentation at Chaos Computer Congress, 2007.

7. Wee Hon Tan. Practical attacks on the Mifare Classic. Master's thesis, Imperial College London, 2009.
8. Nicolas Courtois. The dark side of security by obscurity - and cloning mifare classic rail and building passes, anywhere, anytime. In Eduardo Fern'andez-Medina, Manu Malek, and Javier Hernando, editors, SECRIPT, pages 331–338. INSTICC Press, 2009.
9. Keith E. Mayes and Carlos Cid. The Mifare Classic story. Information Security Technical Report, 15(1):8–12, 2010.
10. Márcio Almeida. Hacking Mifare Classic Cards. Материалы конференции BlackHat 2014. [Электронный ресурс] – url: <https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf> (Дата обращения 21.11.2019)
11. Carlo Meijer and Roel Verdult. Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards. [Электронный ресурс] – url: https://cs.ru.nl/~rverdult/Ciphertext-only_Cryptanalysis_on_Hardened_Mifare_Classic_Cards-CCS_2015.pdf (Дата обращения 10.11.2019)
12. Исследование защищенности карты Тройка .2016. [Электронный ресурс] – url: <https://sohabr.net/habr/post/301832/> (Дата обращения 10.11.2019)
13. Александр Симонов, Взлом метро: копирование и подделка билетов метрополитена. 2009 [Электронный ресурс] – url: <https://hacker.ru/2009/02/06/47074/> (Дата обращения 20.11.2019)
14. Рабинович А.С., Казарин О.В. Методика аутентификации пользователя в информационной системе с использованием технологии NFC // Вопросы кибербезопасности. 2013. № 2. С. 59-62.

Научный руководитель: Цирлов Валентин Леонидович, к.т.н., CISSP, CISM, AMBCI, доцент МГТУ им. Баумана, v.tsirlov@npo-echelon.ru.

Security Analysis of Mifare High Frequency Contactless Smart Cards

Safin I.R.²⁵⁴. Kolosov D.V.²⁵⁵

Abstract: *Mifare is the most popular RFID chip used in public transport, as well as in access control systems for various levels of organizations. The article provides an overview of equipment and security analysis techniques with practical implementations that are used in attacks on this chip. This article includes a combination of technical and historical details. The history of the Mifare chip and NXP clearly reflects the insecurity of proprietary technologies. This issue is relevant, as it relates to critical information infrastructures.*

Keywords: *NXP, Ghost, reverse engineering, Proxmark III, Replay attack, NFC*

²⁵⁴ Safin Ilnur Rishatovich, student IU8-31M, BMSTU, Moscow, safinir@student.bmstu.ru

²⁵⁵ Kolosov Denis Vitalvich, student IU7-32B, BMSTU, Moscow, kolosovdv@student.bmstu.ru

Определение стойкости шифрования методом гаммирования

Строгалева С. Ю.²⁵⁶, Ефремов Е. А.²⁵⁷

Аннотация: на сегодняшний день тексты, зашифрованные разными способами, иногда можно прочитать без особых усилий. Это касается и метода гаммирования. В представленной статье на примере частного случая проанализировано обеспечение стойкости защиты информации методом гаммирования при наложении одного и того же ключа для шифрования различных сообщений.

Ключевые слова: криптография, ключ, секретность, передача данных.

Введение

Вопросам защиты информации в настоящее время уделяется большое внимание, криптография все шире входит в нашу жизнь. Так, владельцы банковских карт, обращаясь через терминал к банку, сначала должны выполнить криптографический протокол аутентификации [1-11]. За последние годы информационные технологии стали частью нашей жизни, информация представляет существенную ценность и уязвима к различного рода злоупотреблениям.

Целью данной работы является изучение одного из методов шифрования – метода гаммирования, а также анализ обеспечения стойкости защиты информации методом гаммирования при использовании одной и той же гаммы для шифрования различных сообщений.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МЕТОДА ГАММИРОВАНИЯ

Гаммирование – простейшая и в то же время наиболее надежная из всех схем шифрования, изобретение, которое чаще всего связывают с именем Г.С. Вернама. В этом способе шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Процесс сложения исходного текста и ключа называется в криптографии *наложением гаммы*.

Если буквой X обозначить число, соответствующее исходному символу, а буквой K – число, соответствующее символу ключа, то правило гаммирования можно записать следующим образом:

$$Z = X + K(mod N) \quad (1)$$

где Z – закодированный символ, N – количество символов в алфавите.

Чаще всего на практике встречается двоичное гаммирование, где используется двоичный алфавит, а сложение производится по модулю два. Операция сложения по модулю 2 часто обозначается $\oplus$. Тогда запись будет выглядеть следующим образом:

$$Z = X + K(mod 2) = X \oplus K \quad (2)$$

Операция сложения по модулю два выполняется достаточно быстро, поэтому наложение гаммы даже на очень большой открытый текст выполняется практически

²⁵⁶ Строгалева Сергей Юрьевич, студент, МГТУ имени Н. Э. Баумана, Москва, sergeystrogalev@gmail.com

²⁵⁷ Ефремов Егор Андреевич, студент, МГТУ имени Н. Э. Баумана, Москва, e.efremov2014@gmail.com

мгновенно. Поэтому метод гаммирования широко применяется в современных технических системах.

ОПРЕДЕЛЕНИЕ СТОЙКОСТИ ШИФРОВАНИЯ ДЛЯ ЧАСТНОГО СЛУЧАЯ

Для определения стойкости шифрования при помощи наложения гаммы был проанализирован случай, в котором для шифрования двух разных сообщений использовалась одна и та же гамма:

С помощью формул режима однократного гаммирования получаются криптограммы обоих исходных текстов:

$$Z_1 = X_1 \oplus K \quad (3)$$

$$Z_2 = X_2 \oplus K \quad (4)$$

Задача нахождения открытого текста по известной криптограмме двух текстов, зашифрованных одним ключом, может быть решена, используя формулы (3) и (4). Для этого нужно сложить по модулю 2 оба равенства. Получаем следующее равенство:

$$Z_1 \oplus Z_2 = X_1 \oplus K \oplus X_2 \oplus K = X_1 \oplus X_2 \quad (5)$$

В том случае, если известна какая-то информация о содержании одного из открытых текстов, его тематике, используемых стандартных фразах, то можно попытаться использовать это для определения слов второго открытого текста, находящихся на тех же позициях, что и предполагаемые фразы в первом тексте с помощью свойства операции сложения по модулю 2:

$$Z_1 \oplus Z_2 \oplus X_1 = X_1 \oplus X_2 \oplus X_1 = X_2 \quad (6)$$

Если таким образом расшифрованные места второго открытого текста будут осмысленными, то можно, постепенно смещаясь по тексту сообщений, попытаться расшифровать как можно большее количество позиций в обоих открытых текстах.

Если совершенно неизвестна исходная информация, то задача сводится к подбору открытых текстов, сумма которых определяется по формуле 5, что, хоть и довольно затруднительно, но все-таки возможно.

Рассмотрим следующий пример. Имеются две шифрограммы, полученные наложением одной и той же гаммы:

Таблица 1. Шифрограмма 1

								0	0	0	0	0	1	1	0	0	0					0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	0	0	1	1	0	1	1
0	0	0	0	0	1	0	1																																				
Е								Ё									З								М								Ь										

Таблица 2. Шифрограмма 2

0	0	0	0	1	1	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Н								Й								В								П								А											

Складывая эти шифрограммы, получаем следующую последовательность:

Таблица 3.

0	0	0	0	1	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	1	0	0	0	1	1	0	1	1	
К								Л								Ё								Ъ								Ь							

С помощью кодировочной таблицы СР-1251, используя предположение, что символам исходного русского алфавита соответствуют числа от 0 (А) до 32 (Я), переводим текст криптограммы в буквенную форму.

Теперь попробуем найти все возможные пары букв русского алфавита, которые при сложении в двоичной форме образуют буквы этой последовательности, и среди этих пар найти те, которые образуют искомые слова. При этом «зеркальные» пары («АБ» и «БА») будем учитывать только один раз. В парах, образующих начальные буквы исходных слов, не будем учитывать те, которые содержат буквы Ъ, Ь, поскольку по правилам русского языка слова с них не начинаются, а из пар, образующих последние буквы слов, уберем содержащие Ь. Кроме того, очевидно, что в исходных словах нет буквы Я, поскольку для нее отсутствует второе слагаемое, необходимое для получения исходной шифрограммы. В итоге осталось 13 комбинаций букв для первых букв исходных текстов и 15 комбинаций для каждой последующей буквы.

Таблица 4. Первая буква

А	В	Г	Д	Е	Ё	Ж	Й	Р	С	Т	У	Ф
К	И	З	О	Н	М	Л	Б	Щ	Ш	Ч	Ю	Э

Таблица 5. Вторая буква

А	В	Г	Д	Е	Ё	Ж	М	П	Р	С	Т	У	Ф	Щ
Л	Н	О	З	И	Й	К	Б	Ы	Ь	Э	Ю	Ч	Ш	Х

Таблица 6. Третья буква

А	В	Г	Ж	З	И	Й	К	П	Р	С	Т	Ч	Ш	Щ
Ё	Д	Е	Б	Н	О	Л	М	Х	Ц	У	Ф	Э	Ю	Ы

Таблица 7. Четвертая буква

А	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
Ь	Ю	Э	Ш	Ч	Б	Щ	Ф	У	Ц	Х	Р	П	Т	С

Таблица 8. Пятая буква

А	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	Щ
Б	Ш	Ч	Ю	Э	Ы	Т	С	Р	П	Ц	Х	Ф	У	Б

Перебирая все возможные варианты, при этом на каждом уровне отбрасывая те, которые образуют нечитаемые сочетания, постепенно сужаем диапазон поиска и в итоге получаем два исходных слова.

Таблица 9.

0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	1	0	1	1
Ж								И								З								Н								Б							
0	0	0	0	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	
Л								Е								Н								Т								А							

Заключение

Метод гаммирования является достаточно надежной и простой схемой шифрования, что позволяет использовать его в современных технических системах. Кроме того, недостаточно надежно использовать одну и ту же гамму для шифрования различных текстов, поскольку информация не будет должным образом защищена и тексты можно будет легко прочесть, что подтверждает выводы, сделанные известным американским математиком и инженером Клодом Шенноном о таком необходимом и достаточном условии абсолютной стойкости шифра, как однократное использование ключа.²⁵⁸

Литература

1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
2. Алексеев А. П. Курсовое проектирование для криптографов. Учебное пособие. М.: СОЛОН-Пресс, 2018. – 100 с.

²⁵⁸ Шеннон. К. Теория связи в секретных системах // «Bell System Technical Journal». – 1949.

3. Бабаш А. В., Шанкин Г. П. Криптография. Под редакцией В. П. Шерстюка, Э. А. Применко / А. В. Бабаш, Г. П. Шанкин. – М.: СОЛОН-ПРЕСС, 2007. – 512 с.
4. Информационный мир XXI века. Криптография – основа информационной безопасности / Под ред. Э. А. Болелова; Московский государственный технический университет гражданской авиации. – 2-е изд. – М.: Издательство-торговая корпорация «Дашков и К°», 2018 – 126 с.
5. Рябко Б. Я., Фионов А. Н. Криптография в информационном мире. – М.: Горячая линия – Телеком, 2018. – 300 с.
6. Шеннон К. Теория связи в секретных системах» / «Bell System Technical Journal». – 1949.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003 – 816 с.
8. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.
9. Введение в криптографию / Под общ. ред. В. В. Яценко. – 4-е изд., до. М.: МЦНМО, 2012. – 348 с.
10. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. – М.: Аст, Астрель, 2006. 447 с.
11. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.

Научный руководитель: Троицкий Игорь Иванович, доцент, кандидат технических наук, зам. зав. кафедры «Информационная безопасность»

The determination of strength of the encryption using XOR cipher

Sergey Strogalev²⁵⁹, Egor Efremov²⁶⁰

Abstract. *At the present time once in a while some texts encrypted with many different algorithms can be effortlessly read. This also relates to XOR cipher. In this article the providing of strength of data protection with XOR cipher using one and the same key to encrypt different messages is analyzed on the example of particular case.*

Keywords: *cryptography, key, secrecy, data transmission.*

²⁵⁹ Sergey Strogalev, student, Informatics and Control systems department Bauman Moscow State Technical University, BMSTU, Moscow, sergeystrogalev@gmail.com

²⁶⁰ Egor Efremov, student, Informatics and Control systems department Bauman Moscow State Technical University, BMSTU, Moscow, e.efremov2014@gmail.com

Обзор подходов к применению технологий искусственного интеллекта в информационной безопасности

Титов А.Ю.²⁶¹

Технологии искусственного интеллекта и глубокого обучения позволяют по-новому подойти к решению задач информационной безопасности. Уже продемонстрированы значительные улучшения по сравнению с традиционными системами на основе сигнатур и правил и даже с классическими решениями на основе машинного обучения. Использование открытых наборов данных для обучения и тестирования позволяет провести сравнение подходов. Рассмотрены уязвимости, характерные для моделей машинного обучения.

Ключевые слова: глубокое обучение, искусственные нейронные сети.

Введение

Целью работы было исследование применения методов искусственного интеллекта в области информационной безопасности.

История развития искусственного интеллекта

Исторические вехи развития технологий искусственного интеллекта в России [1] и в мире [2] показаны на рис.1.

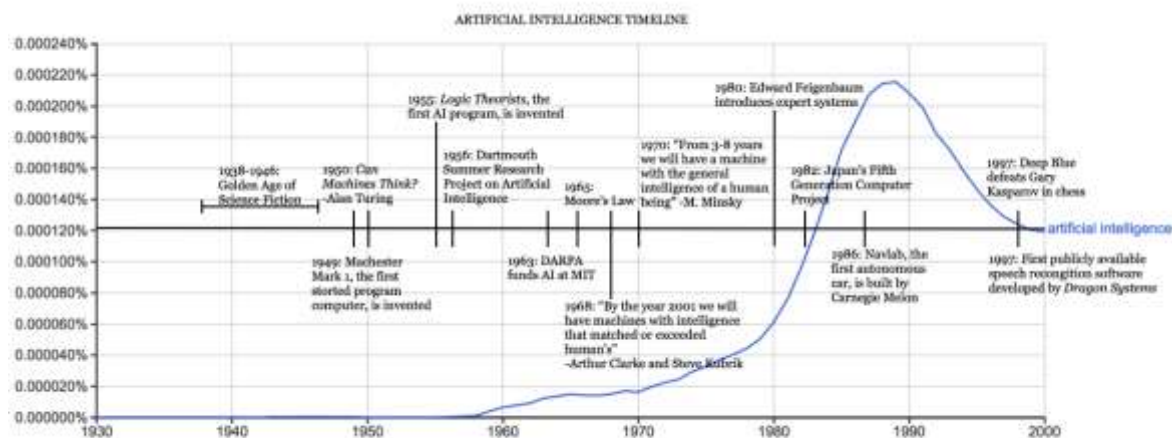


Рис.1. Хронология развития искусственного интеллекта [2].

Подходы и направления развития искусственного интеллекта

Описаны направления развития ИИ (см. рисунок 2), перечислены ключевые особенности технологий машинного обучения (рис. 3) [3].

²⁶¹ Титов Андрей Юрьевич, CISSP, CISM, студент группы ИУ8-45, МГТУ им. Н.Э. Баумана, г. Москва, titov@student.bmstu.ru

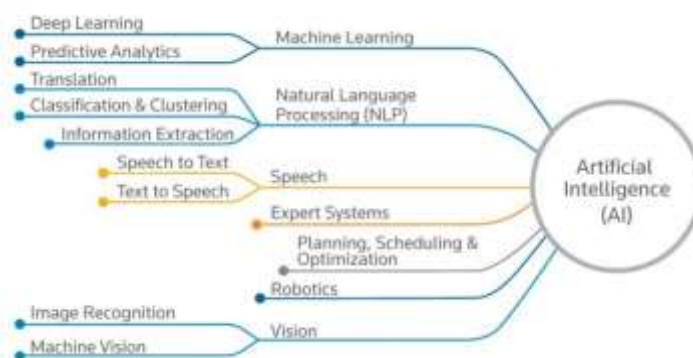


Рис.2. Направления развития искусственного интеллекта.



Рис.3. Классификация алгоритмов машинного обучения [4]

Наборы данных для машинного обучения в сфере ИБ

Таблица 1 – Открытые наборы данных из области информационной безопасности, используемые для тестирования методов машинного обучения.

Область ИБ	Набор данных	Ссылка на источник
Обнаружение сетевых вторжений	KDD99 Knowledge Discovery and Data Mining	[5]
	NSL-KDD	[6]
	CTU-13 (Czech Technical University)	[7]
	DARPA Intrusion Detection Evaluation	[8]
	AWID (Aegean WiFi Intrusion Dataset)	[9]
Обнаружение алгоритма генерации доменов	Alexa Top Sites	[10]
	OSINT DGA	[11]
	DGArchive	[12]
Вредоносное программное обеспечение	Google Play Store	[13]
	Contagio malware dump	[14]
	Comodo Anti-Malware Database	[15]
	VirusShare Repository of Malware Samples	[16]
	DREBIN (Android Malware)	[17]
	Microsoft Malware Classification	[18]
	CERT Insider Threat Data Dataset	[19]
Спам	Enron-Spam	[20]
	Spam-Assassin	[21]
	LingSpam	[22]

Показатели качества обучения

Существует несколько различных показателей качества (метрик) для задач бинарной классификации. Все эти показатели получаются из четырех значений, матрицы ошибок (confusion matrix), указанных в таблице 2.

Таблица 2 – Матрица ошибок

Confusion Matrix		Прогнозируемый класс ошибок	
		Положительный	Отрицательный
Фактический класс ошибок	Положительный	Истинно положительные (TP) = верно принятые	Ложно отрицательные (FN) = пропуск цели = ошибка II рода
	Отрицательный	Ложно положительные (FP) = ложная тревога = ошибка I рода	Истинно отрицательные (TN) = верно отвергнутые

Правильность классификации (acc) или доля правильных:

$$acc = \frac{TP+TN}{TP+TN+FP+FN}, \quad (1)$$

где $TP+TN$ – правильно классифицированные примеры;

$TP+TN+FP+FN$ – общий объем выборки.

Доля положительно предсказанных (PPV) или точность (p):

$$p = \frac{TP}{TP+FP}, \quad (2)$$

где TP – правильно классифицированные как класс X примеры;

$TP+FP$ – все примеры, классифицированные как класс X .

Чувствительность, коэффициент истинно положительных (TPR), вероятность обнаружения (P_D) или полнота (recall, r):

$$TPR = \frac{TP}{TP+FN}, \quad (3)$$

где TP – правильно классифицированные примеры из класса X ;

$TP+FN$ – все примеры класса X .

Доля истинно отрицательных (NPV):

$$NPV = \frac{TN}{TN+FN}, \quad (4)$$

где TN – примеры, правильно классифицированные как не принадлежащие к классу X ;

$TN+FN$ – все примеры, не принадлежащие к классу X .

Специфичность или коэффициент истинно отрицательных (TNR):

$$TNR = \frac{TN}{TN+FP}, \quad (5)$$

где TN – примеры, правильно классифицированные как не принадлежащие к классу X ;

$TN+FP$ – все примеры, которые не относятся к классу X .

Частота ложных тревог (FAR), коэффициент ложных срабатываний (FPR):

$$FPR = \frac{FP}{TN+FP}, \quad (6)$$

где FP – примеры, неправильно классифицированные как класс X ;

$TN+FP$ – все примеры, которые не относятся к классу X .

Мера F_1 — это гармоническое среднее между точностью (p) и коэффициентом истинно положительных (r):

$$F_1 = \frac{2}{\frac{1}{r} + \frac{1}{p}} = 2 \frac{p \cdot r}{p+r}, \quad (7)$$

где p – точность;

r – коэффициент истинно положительных.

Примеры применения методов машинного обучения в области ИБ

Таблица 3 – Алгоритмы машинного обучения в задачах ИБ

Область ИБ	Используемые методы ИИ	Достигнутые показатели	Ссылка на источник
	MLP/SOM		[23]
	MLP		[24]

Область ИБ	Используемые методы ИИ	Достигнутые показатели	Ссылка на источник
Обнаружение сетевых вторжений	DBN	Точность 81,26%, полнота — 99,34%	[25]
	ИНС		[26]
Обнаружение вторжений в сеть WiFi	Каскадный автокодировщик	Обнаружение — 92,18%, ложных срабатываний — 4,40%, точность — 86,15%.	[27]
Обнаружение аномалий протокола BGP	LSTM	Точность — 99,5%	[28]
Обнаружение ботнетов	LSTM	TPR — 96,01%, FPR — 1,95%	[29]
Ботнеты в IoT-устройствах	Двунаправленная LSTM	Точность от 91,95% до 99,999%	[30]
Обнаружение алгоритма генерации доменов	GAN, автокодировщик	TPR 70%	[31]
	GRU	TPR 98%, FPR 0,1%.	[32]
Атаки при загрузке	EDCNN	FPR на 47% ниже собычной CNN	[33]
Определение типа файла	DBN	Точность классификации — 97,44%.	[34]
Определение типа сетевого трафика	Каскад из автокодировщиков	Точность—91,74%, полнота — 90,9%	[35]
	Автокодировщик в паре с CNN	F ₁ -мера — 98%, точность — 93%.	[36]
Обнаружение внутреннего нарушителя	LSTM		[37]
Спам	DBN из 3-х RBM, +SVM	Точность—99,45%, 97,5% и 97,43%	[38]
	Автокодировщик	Точность более 95%	[39]
Проверка нажатия клавиш человеком	LSTM	Точность — 80%	[40]
Аутентификация пользователя WiFi	Автокодировщик +SVM	91% точность аутентификации	[41]

Уязвимости методов машинного обучения

Приведены виды уязвимостей, присущих различным методам искусственного интеллекта и наборам данных для их обучения.

Таблица 4 — Виды атак на модели машинного обучения [42]

Этап / Цель	Шпионаж	Саботаж	Мошенничество
Обучение (атака на алгоритм)	Изучение модели при помощи отравления данных	Отравление Трояны Backdoor	Отравление
Эксплуатация (атака на модель)	Атаки логического вывода (вывод об участии, инверсия модели и др.)	Состязательное переобучение Обход (пропуск цели)	Обход (ложная тревога)

Выводы

Технологии искусственного интеллекта и глубокого обучения позволяют по-новому подойти к решению задач информационной безопасности. Уже продемонстрированы значительные улучшения по сравнению с традиционными системами на основе сигнатур и правил и даже с классическими решениями на основе машинного обучения. RBM чаще всего использовались для обнаружения ВПО и обнаружения вторжений. RNN — метод, который использовался для устранения самого широкого набора угроз безопасности (т.е. вредоносных программ, доменных имен, вторжений в сеть и на ПК). RBM часто используются вместе с автокодировщиками, примерно в половине случаев, видимо, из-за недостатка размеченных данных, т.к. RBM и автокодировщики могут предварительно обучаться на неразмеченных данных и точно настраиваться на классы. RNN популярны, потому что многие данные, связанные с информационной безопасностью, можно рассматривать как задачи временных рядов, которые хорошо поддаются RNN.

Эффективность сильно различалась по разным направлениям информационной безопасности. Глубокое обучение наиболее стабильно работает при идентификации вредоносных доменных имен (DGA), где TPR варьируется от 96,01% до 99,86%, FPR — от 0,1% до 1,95%, а точность — от 0,9959 до 0,9999. Напротив, подходы к обнаружению сетевых вторжений имеют более широкие диапазоны: TPR от 92,33% до 100%, FPR от 1,58% до 2,3% и точность от 44% до 99%. Способность обнаруживать вторжения в сеть в значительной степени зависит от типа атаки и количества классов при классификации. Другим критическим фактором, который повлиял на показатели во всех направлениях, было отношение фоновых данных к «плохим» в обучающем наборе.

Исследования в этой области затруднены недостатком общедоступных наборов данных, которые являются либо слишком маленькими, старыми, либо внутрикорпоративными. Для увеличения доверия к методам глубокого обучения нужны большие, регулярно обновляемые эталонные наборы данных из области ИБ.

Указанные в работе уязвимости моделей ИИ не означают, что эти методы не подходят для целей информационной безопасности, а говорят о том, что эти риски необходимо минимизировать в соответствии с актуальными угрозами и возможностями.

Литература

1. Российская Ассоциация искусственного интеллекта. [Электронный ресурс]: Становление информатики в России. Д. А. Поспелов. URL: <http://www.raai.org/about/persons/pospелov/pages/stanovl.htm> (дата обращения: 01.11.2019).
2. Science in the News [Электронный ресурс]: The History of Artificial Intelligence. Rockwell Anyoha. 28.08.2017. URL: <http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/> (дата обращения: 01.11.2019).
3. Towards Data Science [Электронный ресурс]: Machine Learning for Cybersecurity 101. Alexander Polyakov, 04.10.2018. URL: <https://towardsdatascience.com/machine-learning-for-cybersecurity-101-7822b802790b> (дата обращения: 01.11.2019).

4. vas3k [Электронный ресурс]: Машинное обучение для людей, 23.07.2018. URL: https://vas3k.ru/blog/machine_learning/ (дата обращения: 01.11.2019).
5. UCI Knowledge Discovery in Databases Archive [Электронный ресурс]: KDD Cup 99. URL: <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html> (дата обращения: 01.11.2019).
6. Canadian Institute for Cybersecurity [Электронный ресурс]: NSL-KDD dataset URL: <https://www.unb.ca/cic/datasets/nsl.html> (дата обращения: 01.11.2019).
7. Stratosphere Research Laboratory [Электронный ресурс]: The CTU-13 Dataset. URL: <https://stratosphereips.org/category/dataset> (дата обращения: 01.11.2019).
8. MIT Lincoln Lab [Электронный ресурс]: DARPA Intrusion Detection Evaluation. URL: <https://www.ll.mit.edu/r-d/datasets> (дата обращения: 01.11.2019).
9. IEEE Xplore [Электронный ресурс]: Kolias, C.; Kambourakis, G.; Stavrou, A.; Gritzalis, S. Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. URL: <https://ieeexplore.ieee.org/document/7041170>. (дата обращения: 01.11.2019).
10. Alexa Top Sites [Электронный ресурс]: Amazon Web Services. URL: <https://aws.amazon.com/alexa-top-sites/> (дата обращения: 01.11.2019).
11. Bambenek Consulting [Электронный ресурс]: Master Feeds URL: <http://osint.bambenekconsulting.com/feeds/> (дата обращения: 01.11.2019).
12. Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie [Электронный ресурс]: DGArchive. URL: <https://dgarchive.caad.fkie.fraunhofer.de/> (дата обращения: 01.11.2019).
13. Google Play [Электронный ресурс]: Store. URL: <https://play.google.com/store> (дата обращения: 01.11.2019).
14. Contagio Malware Dump [Электронный ресурс]: Mila Parkour. URL: <http://contagiodump.blogspot.com/> (дата обращения: 01.11.2019).
15. Comodo [Электронный ресурс]: Anti-Malware Database URL: <https://www.comodo.com/home/internet-security/updates/vdp/database.php> (дата обращения: 01.11.2019).
16. VirusShare [Электронный ресурс]: Repository of Malware Samples. URL: <http://virusshare.com/> (дата обращения: 01.11.2019).
17. NDSS Symposium [Электронный ресурс]: Arp, D.; Spreitzenbarth, M.; Hubner, M.; Gascon, H.; Rieck, K. Drebin: Effective and Explainable Detection of Android Malware in Your Pocket. 2014. URL: <https://www.ndss-symposium.org/ndss2014/programme/drebin-effective-and-explainable-detection-android-malware-your-pocket/> (дата обращения: 01.11.2019).
18. Kaggle [Электронный ресурс]: Microsoft Malware Classification (BIG 2015) URL: <https://www.kaggle.com/c/malware-classification/data> (дата обращения: 01.11.2019).
19. Semantic Scholar [Электронный ресурс]: Lindauer, B.; Glasser, J.; Rosen, M.; Wallnau, K.C.; Generating Test Data for Insider Threat Detectors. 2014, URL: <https://pdfs.semanticscholar.org/090b/7a2802a7a6a077a7b712c3alecce19c6d35b.pdf> (дата обращения: 01.11.2019).
20. EnronSpam. [Электронный ресурс]: V. Metsis, I. Androustopoulos and G. Paliouras. URL: <https://labs-repos.iit.demokritos.gr/skel/i-config/downloads/enron-spam/> (дата обращения: 01.11.2019).
21. SpamAssassin [Электронный ресурс]: Public Mail Corpus URL: <https://spamassassin.apache.org/old/publiccorpus/> (дата обращения: 01.11.2019).
22. LingSpam [Электронный ресурс]: A mixture of spam messages. URL: <https://labs-repos.iit.demokritos.gr/skel/i-config/downloads/> (дата обращения: 01.11.2019).
23. Semantic Scholar [Электронный ресурс]: Cannady J & Mahaffey J. The application of Artificial Neural Networks to Misuse. URL: <https://pdfs.semanticscholar.org/6eff/11044a6b7b120b17294aa4b9cc14141fe9fb.pdf>. (дата обращения: 01.11.2019).
24. ScienceDirect [Электронный ресурс]: Cunningham R & Lippmann R Improving Intrusion Detection performance using keyword selection and neural networks. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1389128600001407> (дата обращения: 01.11.2019).
25. IEEE Xplore [Электронный ресурс]: Maimó, L.F.; Gómez, A.L.P.; Clemente, F.J.G.; Pérez, M.G. A self-adaptive deep learning-based system for anomaly detection in 5G networks.. URL: <https://ieeexplore.ieee.org/document/8283694> (дата обращения: 01.11.2019).

26. SANS Institute [Электронный ресурс]: Application of Neural Networks to Intrusion Detection. URL: <https://www.sans.org/reading-room/whitepapers/detection/application-neural-networks-intrusion-detection-336> (дата обращения: 01.11.2019).
27. Semantic Scholar [Электронный ресурс]: Aminanto, M.E.; Kim, K. Improving detection of Wi-Fi impersonation by fully unsupervised deep learning. URL: <https://www.semanticscholar.org/paper/Improving-Detection-of-Wi-Fi-Impersonation-by-Fully-Aminanto-Kim/74ec60ffc826b5254cc5ef78e2c41ea3006d9ce1> (дата обращения: 01.11.2019).
28. covert.io [Электронный ресурс]: Cheng, M.; Xu, Q.; Lv, J.; Liu, W.; Li, Q.; Wang, J. MS-LSTM: A multi-scale LSTM model for BGP anomaly detection. URL: <https://www.covert.io/research-papers/deep-learning-security/MS-LSTM%20-%20a%20Multi-Scale%20LSTM%20Model%20for%20BGP%20Anomaly%20Detection.pdf> (дата обращения: 01.11.2019).
29. Worcester Polytechnic Institute [Электронный ресурс]: Torres, P.; Catania, C.; Garcia, S.; Garino, C.G. An Analysis of Recurrent Neural Networks for Botnet Detection Behavior. URL: [https://users.wpi.edu/~kmus/ECE579M_files/ReadingMaterials/RNN_Botnet_Detection\[2093\].pdf](https://users.wpi.edu/~kmus/ECE579M_files/ReadingMaterials/RNN_Botnet_Detection[2093].pdf) (дата обращения: 01.11.2019).
30. ResearchGate [Электронный ресурс]: McDermott, C.D.; Majdani, F.; Petrovski, A. Botnet detection in the internet of things using deep learning approaches. URL: https://www.researchgate.net/publication/327017365_Botnet_Detection_in_the_Internet_of_Things_using_Deep_Learning_Approaches (дата обращения: 01.11.2019).
31. arXiv [Электронный ресурс]: Anderson, H.S.; Woodbridge, J.; Filar, B. DeepDGA: Adversarially-tuned domain generation and detection. URL: <https://arxiv.org/pdf/1610.01969.pdf>. (дата обращения: 01.11.2019).
32. arXiv [Электронный ресурс]: Woodbridge, J.; Anderson, H.S.; Ahuja, A.; Grant, D. Predicting domain generation algorithms with long short-term memory networks. URL: <https://arxiv.org/pdf/1611.00791.pdf>. (дата обращения: 01.11.2019).
33. IEEE Xplore [Электронный ресурс]: Shibahara, T.; Yamanishi, K.; Takata, Y.; Chiba, D.; Akiyama, M.; Yagi, T.; Ohsita, Y.; Murata, M. Malicious URL sequence detection using event de-noising convolutional neural network. URL: <https://ieeexplore.ieee.org/document/7996831>. (дата обращения: 01.11.2019).
34. ScienceDirect [Электронный ресурс]: Cox, J.A.; James, C.D.; Aimone, J.B. A signal processing approach for cyber data classification with deep neural networks. URL: <https://www.sciencedirect.com/science/article/pii/S1877050915029865>. (дата обращения: 01.11.2019).
35. BlackHat [Электронный ресурс]: Wang, Z. The Applications of Deep Learning on Traffic Identification. URL: <https://www.blackhat.com/docs/us-15/materials/us-15-Wang-The-Applications-Of-Deep-Learning-On-Traffic-Identification-wp.pdf> (дата обращения: 01.11.2019).
36. arXiv [Электронный ресурс]: Lotfollahi, M.; Shirali, R.; Siavoshani, M.J.; Saberian, M. Deep Packet: A Novel Approach for Encrypted Traffic Classification Using Deep Learning. URL: <https://arxiv.org/abs/1709.02656> (дата обращения: 01.11.2019).
37. arXiv [Электронный ресурс]: Tuor, A.; Kaplan, S.; Hutchinson, B.; Nichols, N.; Robinson, S. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. 2017. URL: <https://arxiv.org/abs/1710.00811> (дата обращения: 01.11.2019).
38. ResearchGate [Электронный ресурс]: Tzortzis, G.; Likas, A. Deep Belief Networks for Spam Filtering. in Tools with Artificial Intelligence. URL: https://www.researchgate.net/publication/4302287_Deep_Belief_Networks_for_Spam_Filtering (дата обращения: 01.11.2019).
39. SpringerLink [Электронный ресурс]: Mi, G.; Gao, Y.; Tan, Y. Apply stacked auto-encoder to spam detection. URL: https://link.springer.com/chapter/10.1007%2F978-3-319-20472-7_1 (дата обращения: 01.11.2019).
40. ResearchGate [Электронный ресурс]: Koboжек, P.; Saeed, K. Application of recurrent neural networks for user verification based on keystroke dynamics. URL: https://www.researchgate.net/publication/309531048_Application_of_recurrent_neural_networks_for_user_verification_based_on_keystroke_dynamics (дата обращения: 01.11.2019).
41. Semantic Scholar [Электронный ресурс]: Shi, C.; Liu, J.; Liu, H.; Chen, Y. Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT. 2017. URL:

<https://www.semanticscholar.org/paper/Smart-User-Authentication-through-Actuation-of-IoT-Shi-Liu/d6aa779d5ad81ae2e361e9900b0943247131e41c> (дата обращения: 01.11.2019).

42. Towards Data Science [Электронный ресурс]: How to attack Machine Learning (Evasion, Poisoning, Inference, Trojans, Backdoors). Alexander Polyakov. 06.08.2019. URL: <https://towardsdatascience.com/how-to-attack-machine-learning-evasion-poisoning-inference-trojans-backdoors-a7cb5832595c> (дата обращения: 01.11.2019).

Научный руководитель: Басараб Михаил Алексеевич, д-р физ.-мат. наук, профессор, заведующий кафедрой «Информационная безопасность» МГТУ им. Н. Э. Баумана, basarab.iu8@gmail.com

Review of Artificial Intelligence Applications to Information Security

Titov A.²⁶²

Abstract. *Artificial Intelligence and deep learning technologies enabled new approaches to problems in information security. Significant improvements were already demonstrated in comparison to traditional signature- and rule-based systems and even classic machine learning. Open-source datasets for machine learning will help to test and compare key metrics of different methods on the same data. Different categories of attacks on machine learning models were considered.*

Keywords: *deep learning, artificial neural networks, natural language processing.*

²⁶²Andrey Titov, CISSP, CISM, student of IU8-45 group, Bauman Moscow State Technical University, titov@student.bmstu.ru

Разработка алгоритма стегоанализа с использованием машинного обучения

Фомченко А.В.²⁶³

В работе была создана модель для обнаружения стеганографии в изображениях с использованием машинного обучения. Результатом статьи является программа, позволяющая определять наличие стеганографии в изображении при заданных условиях. Был успешно проведен эксперимент на тестовой выборке изображений.

Ключевые слова: стегоанализ, машинное обучение

Введение

Стеганография — это метод организации связи, который, собственно, скрывает само наличие связи [1, 2]. В отличие от криптографии, где точно можно определить, является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют передавать секретные сообщения так, чтобы невозможно было заподозрить их существование [3-6].

Постановка задачи и извлечение признаков из выборки

Для обучения и тестирования алгоритма будут использоваться полностью заполненные стегоконтейнеры методом LSB. Стегоконтейнерами будут являться 3700 изображений 100x100 формата png. Малый размер выборки изображений и самих изображений связан с тем, что для наглядности работы алгоритма в больших размерах нет необходимости. Для выбора пространства признаков будет использоваться алгоритм SPAM (Subtractive Pixel Adjacency Model of covers). Суть алгоритма в том, что по различным направлениям считается разность цветов соседних пикселей D , задаваемая формулой:

$$D_{\overline{i,j}} = I_{i,j} - I_{i,j+1}, \quad (1)$$

где $I_{i,j}$ — цвет пикселя в координате (i, j) .

Вектор признаков задается набором условных вероятностей:

$$M_{\overline{u,v}} = P(D_{\overline{i,j+1}} = u | D_{\overline{i,j}} = v), \quad (2)$$

где u, v принадлежат заданному множеству чисел.

Таким образом, получается вектор признаков для каждого изображения.

Обучение на тестовых данных

Перед началом обучения стоит разбить датасет на 2 части, одна часть будет изображениями со скрытой информацией, другая останется без изменений. После извлечения признаков получается таблица из 4000 строк. Классификация будет происходить с алгоритмом Random Forest. Этот алгоритм представляет из себя ансамбль множества решающих деревьев, что позволяет уменьшить проблему переобучения и значительно повысить точность в сравнении с одним деревом. С помощью подбора параметров получаем, что для наилучшей точности Random Forest должен содержать около 800 деревьев с глубиной не более 8.

Результат работы алгоритма

Результат программы представлен на графике (рис.1). Этот график называется ROC-кривой (от Receiver Operating Characteristic). Он показывает зависимость доли ложных срабаток от доли попадания в цель.

²⁶³ Фомченко Александр Валерьевич, МГТУ им. Н.Э. Баумана, Москва, alexvin364@mail.ru

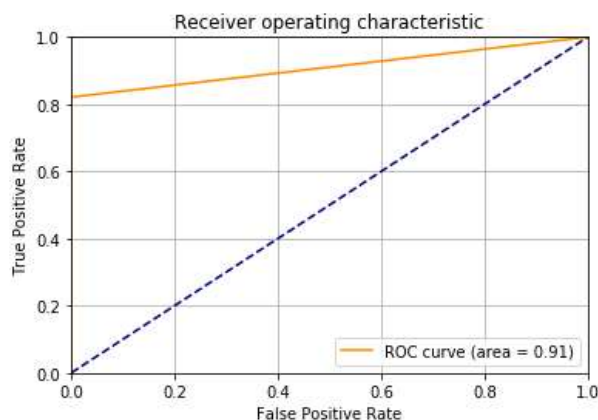


Рисунок 1 – результат работы алгоритма

Выводы

В данной статье была создана работающая модель для обнаружения стеганографии в изображениях. Был определен набор необходимых признаков для извлечения из стегоконтейнеров и подобраны параметры обучающей модели. В результате написана программа, позволяющая определять наличие стеганографии в изображении. Также был успешно проведен эксперимент на тестовой выборке изображений.

Литература

1. Макаренко С.И. Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии // Вопросы кибербезопасности. 2014. № 2 (3). С. 24-32.
2. Сивачев А.В., Прохожев Н.Н., Михайличенко О.В., Башмаков Д.А. Эффективность стеганоанализа на основе методов машинного обучения // Вопросы кибербезопасности. 2017. № 2 (20). С. 53-60.
2. Pevny T., Bas P., Fridrich J. Steganalysis by subtractive pixel adjacency matrix, Proc. 11-th ACM Multimedia Security Workshop, Princeton, 2009, 75-84. DOI: 10.1145/1597817.1597831
3. Lyu S., Farid H. Steganalysis using color wavelet statistics and one-class support vector machines / Lyu S., Farid H. // Proc. Security, Steganography, and Watermarking of Multimedia Contents. - 2004. - P. 35-45.
4. Steganalysis of LSB matching using differences between nonadjacent pixels / Z. Xia, X. Wang, X. Sun, Q. Liu, N. Xiong // Multimedia Tools and Applications. - 2016. - Vol. 75(4). - P. 1947-1962.
5. J. Friedrich, G. Miroslav, R. Du. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghamton, New York: SUNY, 2001.

Научный руководитель: Лебедев Анатолий Николаевич, доцент, кандидат физико-математических наук, МГТУ им Н.Э. Баумана, lebedevan@bmstu.ru

Development of Stegoanalysis Machine Learning Algorithm

Fomchenko A.V.²⁶⁴

Abstract. In this paper, the model for image steganography detection using machine learning has been created. Result of this paper is a program for determination of steganography presence in images under the certain conditions. An experiment on a test sample of images had been conducted.

Keywords: steganalysis, machine learning

²⁶⁴ Alexander Fomchenko, Bauman Moscow State Technical University, Moscow, alexvin364@mail.ru

Исследование обратимых клеточных автоматов с конечной решеткой**Чиликов А.А.²⁶⁵ Жуков А.Е.²⁶⁶ Верховский А.И.²⁶⁷**

В работе исследовались свойства обратимости клеточных автоматов. С помощью численных методов были явно получены локальные функции связи, обеспечивающие свойство обратимости клеточным одномерным и двумерным автоматам разных размеров. Были получены критерии обратимости для ряда простых случаев, а также свойства, при которых обратимость сохраняется.

Ключевые слова: клеточные автоматы, обратимые преобразования, нелинейные преобразования.

Введение

Впервые клеточные автоматы были упомянуты Джоном фон Нейманом в 40-х годах двадцатого века, и уже в 1985 г. Вольфрамом был описан первый поточный алгоритм шифрования на клеточных автоматах [1]. Классический клеточный автомат представляет собой упорядоченный набор ячеек памяти, образующих некоторую регулярную n -мерную решетку. Многие теоретические исследования, особенно касающиеся теории динамических систем рассматривают бесконечную решетку. На практике наибольшее распространение приобрели клеточные автоматы небольшой размерности – с одно-, двух- и трехмерными решетками, как правило бесконечными. В криптографии же, как показано в обзоре [2] – [3], пока нашли свое применение одномерные и двумерные автоматы с конечной решеткой, либо модели на основе обобщенных клеточных автоматов. На основе двумерного клеточного автомата был получен высокопроизводительный поточный шифр [4]. На основе второй модели недавно была получена хэш-функция [5]. Обратимый клеточный автомат – такой, что у каждого его состояния имеется лишь одно предшествующее.

В недавнем обзоре [6] показано, что основные результаты исследований обратимых клеточных автоматов затрагивают лишь автоматы с бесконечной решеткой.

С точки зрения криптографических приложений рассматривать такие автоматы смысла нет. Авторами были найдены примеры обратимых клеточных автоматов с конечной решеткой, а также были предложены направления теоретических исследований и получены некоторые результаты.

Данная работа была проведена с помощью Российского Научного Фонда Грант N 17-11-01377.

²⁶⁵ Чиликов Алексей Анатольевич, кандидат физико-математических наук, доцент кафедры «Информационная Безопасность» МГТУ им. Н.Э. Баумана, Москва, старший научный сотрудник Московского Физико-Технического Института, Москва, chilikov@passware.com

²⁶⁶ Жуков Алексей Евгеньевич, кандидат физико-математических наук, директор ассоциации «РусКрипто», доцент кафедры «Информационная Безопасность» МГТУ им. Н.Э. Баумана, Москва, aez_iu8@rambler.ru

²⁶⁷ Верховский Алексей Иванович, студент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, alexey.verkhovsky@mail.ru

Формальная постановка задачи

Клеточным автоматом $C(\Omega, X_1, X_2, \dots, X_d, \Psi_r, f)$ над множеством Ω с d -мерной решеткой размера $X_1 \times X_2 \times \dots \times X_d$, радиусом локальности r , окрестностью r и локальной функцией связи f задающей правила перехода, называется автономный конечный автомат (1):

$$AC(S, s_0, F), \quad (1)$$

где S – множество возможных состояний автомата, $s_0 \in S$ – начальное состояние автомата, F – функция переходов.

Для обозначения ячейки решетки клеточного автомата с координатами $(x_1, x_2, \dots, x_d)$ будет использоваться запись $m_{(x_1, x_2, \dots, x_d)}$, а в случае, если необходимо указать на ее значение в некоторый момент времени t – запись $m_{(x_1, x_2, \dots, x_d), t}$.

Каждое внутреннее состояние s автомата соответствует заполнению решетки клеточного автомата и описывается упорядоченным набором, компонентами которого являются значения ячеек памяти, как показано на формуле (2)

$$s = [\dots, m_{(x_1, x_2, \dots, x_d)}, \dots], 1 \leq x_i \leq X_i, 1 \leq i \leq d. \quad (2)$$

Рассмотрим одномерный клеточный автомат с коэффициентами из $\mathbb{Z}_2$.

Одномерным булевым клеточным автоматом C (3) с размером решетки X , радиусом локальности r , окрестностью Ψ_r и локальной функцией связи f называется клеточный автомат

$$C(\mathbb{Z}_2, X, \Psi_r, f) \quad (3)$$

описываемый автономным конечным автоматом AC (4):

$$AC(S, s_0, F), \quad (4)$$

где $S = \mathbb{Z}_2^X$ — множество внутренних состояний, $s_0 \in S$ – начальное состояние, $F : S \rightarrow S$ – функция переходов.

Внутреннее состояние описывается набором $s = [m_0, m_1, \dots, m_{X-1}]$. Действие функции f заключается в применении локальной функции связи к окрестности каждой ячейки клеточного автомата, как показано на формуле (5)

$$m_{x,t+1} = f, 0 \leq x < X \quad (5)$$

При условии конечности решетки становится непонятно, что является окрестностью для клеток у границ решетки. Мы будем рассматривать 2 случая, когда крайние клетки отождествлены, т.е. в одномерном случае соседом крайней правой является крайняя левая клетка.

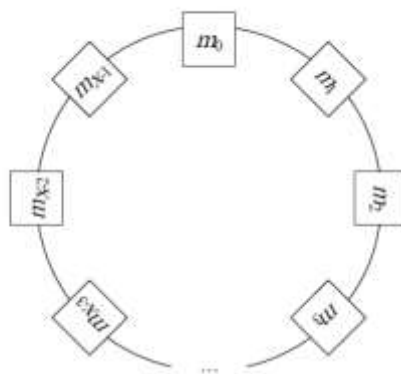


Рисунок 1. Отождествление крайних клеток одномерного клеточного автомата

И другой случай – считаем, что за границами конечной решетки находятся клетки, заполненные нулями, и они не меняются при работе автомата. Будем называть такие ситуации ненулевой и нулевой границей соответственно.

Клеточный автомат называют обратимым, если у каждого его состояния s существует единственное предшествующее состояние s' , такое что $F(s) = s'$. Стоит заметить, что данное условие эквивалентно периодичности клеточного автомата: для каждого s найдется такое t , что $F^{(t)}(s) = s$. С точки зрения криптографии интересен вопрос эффективности вычисления периода, либо его близости к максимальному.

Для конечной решетки и множества состояний клеток $\mathbb{Z}_2$ элементарную обратимость обеспечивает автомат с локальной функцией связи в виде сдвига. В двумерном случае клетка принимает значение своего соседа, либо его инверсию. То есть функция вида (6):

$$f(x_1, \dots, x_n) = x_i \oplus \alpha. \quad (6)$$

С целью выявить нетривиальные локальные функции связи на языке C++ была написана программа, методом полного перебора выявляющая функции, обеспечивающие обратимость клеточному автомату с заданным числом клеток. С исходным кодом, а также с полученными результатами можно ознакомиться в репозитории [7].

Автоматы, полученные путем перебора

В ходе работы программы было получено большое количество функций, обеспечивающих обратимость автоматам размерности 1 и числом клеток от 7 до 23 в случае функции от трех переменных, и до 19 для равновесных функций от 5 переменных. Среди них было большое количество вышеупомянутых функций сдвига, а также линейных функций.

Линейные функции – достаточно простой случай, они обеспечивают обратимость автомату тогда и только тогда, когда матрица соответствующего линейного оператора, действующая на вектор, представляющий текущее состояние автомата, не является вырожденной.

Помимо линейных функций, а также функций сдвига, было получено 542 функции с нелинейной локальной функцией связи. Среди них замечены следующие факты: инверсия каждой функции, обеспечивающей обратимость, также обеспечивает обратимость. Двойственная функция для ненулевой границы также обеспечивает обратимость, в нулевой случае найден контрпример.

В случае нулевой границы размерности 2 (функции от 5 переменных), получены 62 функции, которые обеспечивали обратимость всем проверяемым размерностям (от 7 до 19 клеток).

Теоретический анализ

Неочевидные результаты подтолкнули к подробному теоретическому анализу обратимого клеточного автомата как модели. Далее будут перечислены свойства, справедливые для клеточных автоматов.

Свойство 1. Если f – локальная функция связи, обеспечивающая обратимость то и $f \oplus 1$ также обеспечивает обратимость.

Доказательство простое, от противного. Для простоты рассмотрим одномерный случай ($d = 1$). Пусть есть некоторое состояние клеточного автомата $s_1 = [m_0, m_1, \dots, m_{x-1}]$. И пусть функция перехода переводит автомат в состояние $s_2 = [n_0, n_1, \dots, n_{x-1}]$, $m_i, n_i \in \mathbb{Z}_2$. Тогда $f \oplus 1$ переведет s_1 в $\bar{s}_2 = [\bar{n}_0, \bar{n}_1, \dots, \bar{n}_{x-1}]$ – состояние с инвертированными координатами. Предположим, что после применения инвертированной функции у состояния $\bar{s}_2$ появился еще один предшественник s^* . Но тогда в исходном автомате s^* будет переведен f в s_2 (свою же инверсию), а у него только один предшественник, и это s_1 . То есть s_1 совпадает с s^* . Аналогично доказывается и для больших размерностей.

Следующие 2 свойства по сути являются адаптацией классических результатов из [9] на случай с конечной решеткой.

Свойство 2. Отображение над векторным пространством является клеточным автоматом тогда и только тогда, когда оно коммутирует с оператором сдвига.

Для одномерных клеточных автоматов с ненулевой границей известен факт, также справедливый для автоматов и с бесконечной решеткой, а именно – коммутативность с операцией сдвига. То есть, если $F: \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ – отображение клеточного автомата, а $Sh(z), z \in \mathbb{Z}_2^n$ – отображение циклического сдвига вектора z , то $F(Sh(z)) = Sh(F(z))$. Данное утверждение достаточно очевидно, ведь при применении циклического сдвига содержание окрестности каждой клетки не поменяется, а значит не поменяется и ее значение при применении преобразования клеточного автомата. Верно и обратное, если отображение над векторным пространством коммутирует с оператором сдвига, то данное отображение является клеточным автоматом с ненулевой границей. Для этого покажем, что инвариантность при сдвиге означает однородность преобразования.

Пусть f_i – булева функция, показывающая изменение i -й координаты n -битного вектора при действии на него отображения F в зависимости от значения соседних координат. Так как работаем с двоичными векторами, можем получить ее явно, применяя F для каждого набора соседних координат (и ее самой). Получив столбец значений, запишем функцию f через АНФ:

$$f_k = \bigoplus_{v=(v_0, v_1, \dots, v_{n-1})} \alpha_v x_0^{v_0} * x_1^{v_1} * \dots * x_k^{v_k} * \dots * x_{n-1}^{v_{n-1}} \quad (7)$$

Так как значение после сдвига не меняется для любых таких координат, а также не меняются значения всех соседних клеток, то при сдвиге функция не меняется. Например, при сдвиге на l значение координаты $k + l$ (8):

$$f_{l+k} = \bigoplus_{v=(v_0, v_1, \dots, v_{n-1})} \alpha_v x_l^{v_0} * x_{l+1}^{v_1} * \dots * x_{l+k}^{v_k} * \dots * x_{l+n-1}^{v_{n-1}} \quad (8)$$

Таким образом, для любой координаты имеем одно и ту же функцию, зависящую от соседних координат вектора, а значит, данное отображение является клеточным автоматом. Стоит заметить, что функция может не быть локальной – она вполне может зависеть от всех значения всех клеток решетки. Влияние параметров локальной функции связи на распределение значений было изучено в [8].

Свойство 3. Для обратимого двоичного одномерного клеточного автомата с ненулевой границей существует обратный клеточный автомат. Запишем условие коммутативности со сдвигом в терминах отображений :

$$F \circ Sh = Sh \circ F \quad (9)$$

Применяя справа и слева F^{-1} , получим :

$$F^{-1} \circ F \circ Sh \circ F^{-1} = F^{-1} \circ Sh \circ F \circ F^{-1} = F^{-1} \circ Sh = Sh \circ F^{-1} \quad (10)$$

То есть обратное отображение тоже коммутирует со сдвигами, а значит является клеточным автоматом.

Теорема 1. Подстановочный полином, записанный с использованием нормального базиса будет иметь коэффициенты из поля F_2 .

Под нормальными базисами подразумеваем такие, что каждый элемент z поля F_{2^n} представим в виде $z = z_1 * \theta + z_2 * \theta^2 + \dots + z_n * \theta^{2^{n-1}}$. Условие сдвига в них записывается как

$$Sh(z) = z^2. \quad (11)$$

Обратимый клеточный автомат является подстановкой, запишем для него подстановочный многочлен в нормальном базисе :

$$F = \sum_i \alpha_i * z^i \quad (12)$$

Тогда условие коммутативности со сдвигом запишется как

$$F(z^2) = (F(z))^2 \quad (13)$$

Объединяя с (14), получаем:

$$\sum_i \alpha_i * z^{2i} = \left(\sum_i \alpha_i * z^i \right)^2 = \sum_i \alpha_i^2 * z^{2i}, \quad (14)$$

то есть, $\alpha_i = \alpha_i^2$ и $\alpha_i \in F_2$.

Указанный подход позволяет работать с клеточными автоматами как с отображениями над полем расширения, которые еще и представимы в виде многочленов. Подробнее о свойствах подобной конструкции написано в [10].

Определение 1. Пусть задана конечная группа G , и каждой вершине графа биективно сопоставлен некоторый элемент группы. Пусть также зафиксировано некоторое подмножество $\hat{G} = \{g_1, \dots, g_n\}$ (не обязательно подгруппа), и выполняется следующее свойство: ребро номер i , ведущее в вершину h , исходит из вершины hg_i . На описанном

таким образом графе можно задать клеточный автомат (как однородный, так и неоднородный). Такой автомат мы будем называть *групповым*, а группу G – *носителем*. Функция связи при этом примет вид $f_g(x_1, \dots, x_n)$, и уравнение, описывающее работу автомата, будет иметь вид:

$$m_g(t) = f_g(m_{gg_1}(t-1), \dots, m_{gg_n}(t-1)) \quad (15)$$

Квазигрупповой автомат можно определить аналогично, заменив слово "группа" на "квазигруппа". Напомним, в квазигруппе не обязательно свойство ассоциативности, в отличие от группы. Данное определение может оказаться очень полезным для изучения свойств периодичности клеточного автомата. Кроме того, рассмотренные классические автоматы могут быть рассмотрены как автоматы, носителем которых является циклическая группа, что естественным образом приводит к идее обобщения развитой теории путем переноса ее на более широкий класс групп (например, конечные абелевы).

Выводы

Обратимые клеточные автоматы представляют собой достаточно простое в описании преобразование, которое ко всему прочему может содержать свойства нелинейности и рассеивания (значение клетки на следующем такте влияет на всю окрестность), что может оказаться очень полезным при построении симметричных криптосистем. Кроме того, в [12] и [13] показаны способы построения асимметричных криптосистем на основе обратимых клеточных автоматов. Теоретическая база клеточных автоматов с конечной решеткой еще не вполне развита, авторами предприняты шаги в данном направлении. Полученные результаты вполне могут послужить началом построения теории, аналогичной теории по регистрам сдвига с линейной обратной связью (LFSR).

Литература

1. Wolfram S. Cryptography with cellular automata // Lecture Notes in Computer Science. 1986. Vol. 218. P. 429–432.
2. Жуков А.Е. Клеточные автоматы в криптографии. Часть 1 // Вопросы кибербезопасности. №3 (21). 2017. С. 70-76.
3. Жуков А.Е. Клеточные автоматы в криптографии. Часть 2 // Вопросы кибербезопасности. №4 (22), 2017. С. 47-66.
4. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. – 2010. – №2. – С. 34–41.
5. Ключарёв П.Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности. 2017. № 1 (19). С. 45-50.
6. Kari, J.: Reversible Cellular Automata: From Fundamental Classical Results to Recent Developments.: New Generation Computing 36, 145–172 (2018)
7. Bitbucket [Электронный ресурс]: репозиторий \ Дата обращения 05.12.2018. – Режим доступа: <https://bitbucket.org/KleshIvanovich/bruterca/src/master/>
8. Сухинин Б.М. О влиянии параметров локальной функции связи на распределение значений ячеек двоичных клеточных автоматов // Объединенный научный журнал. – 2010. – № 8. – С. 39–41.
9. Hedlund, G.A.: Endomorphisms and automorphisms of the shift dynamical systems. Math. Syst. Theory 3(4), 320–375 (1969)

10. Лидл Р., Нидеррайтер Г. J155 Конечные поля: В 2-х т. Т. 1. Пер. с англ. - М.: Мир, 1988. - 430 с.
11. Kari, J.: Representation of reversible cellular automata with block permutations. Math. Syst. Theory 29(1), 47–61 (1996)
12. Puhua Guan.: Cellular Automaton Public-Key Cryptosystem. Complex Systems 1 51- 57 (1987)
13. Xing Zhang, Rongxing Lu, Hong Zhang, and Chungen Xu: A New Public Key Encryption Scheme based on Layered Cellular Automata. KSII Transactions on internet and information systems. Vol. 8, No. 10 (2014)

The research of reversible cellular automata with a finite lattice

Chilikov A.A.²⁶⁸ Zhukov A.E.²⁶⁹ Verkhovsky A.I.²⁷⁰

Abstract. *The work contains a research about reversibility of cellular automata. Using computational methods, local connection functions, that provide a property of reversibility to cellular one-dimensional and two-dimensional automata of different dimensions, were explicitly obtained. Reversibility criteria were obtained for simple cases, as well as properties for which reversibility is preserved.*

Keywords: *cellular automata, reversible transformations, nonlinear transformations.*

²⁶⁸ Aleksey Chilikov, Ph.D (Math), BMSTU, MIPT, Moscow chilikov@passware.com

²⁶⁹ Aleksei Zhukov, Ph.D. (Math.), Associate Professor, Director at Association RusCrypto, BMSTU, Moscow, aez_iu8@rambler.ru

²⁷⁰ Aleksey Verkhovsky, student, BMSTU, Moscow, alexey.verkhovsky@mail.ru

Информационная безопасность и цифровая криминалистика: проблемы, решения и новые вызовы

Чиликов А.А.²⁷¹, Яковлев А. Н.²⁷²

В работе проведен анализ современного состояния дел в цифровой криминалистике. Разобраны ряд наиболее сложных задач, проведен анализ возникающих трудностей и возможных путей их решения. Разобран положительный практический опыт. Рассмотрены ключевые требования к компетенциям различных категорий специалистов в области цифровой криминалистике. Сформулирован ряд предложений по повышению качества взаимодействия специалистов различного профиля.

Ключевые слова: компьютерно-техническая экспертиза, мобильные устройства, криптографическая защита, извлечение данных

Введение

Под цифровой криминалистикой традиционно понимают ту часть криминалистической науки, которая сопряжена с исследованием криминалистически значимой информации, представленной в цифровой форме. Бурное развитие информационных технологий, начавшееся в конце прошлого века, и продолжающееся по сей день, привело к повсеместному проникновению цифровой техники. Как следствие, ежесекундно в различных информационных обрабатываются гигантские объемы данных, которые могут иметь важное значение для расследования преступлений (не обязательно в сфере компьютерной информации), а также иных инцидентов информационной безопасности. В связи с этим, естественным образом возник запрос на создание способов извлечения, анализа и интерпретации цифровой информации. С точки зрения криминалистики такие способы должны быть научно обоснованными, и обеспечивать полноту, достоверность и воспроизводимость полученных результатов.

Повсеместное распространение цифровых устройств, доступность современных коммуникационных сетей привели к нескольким важным эффектам. Во-первых, резко выросло количество преступлений и иных противоправных действий, при совершении которых используется компьютерная техника. Во-вторых, производители аппаратного и программного обеспечения стали уделять все большее внимание вопросам защиты информации. Это, в свою очередь, привело к появлению легкодоступных, но при этом весьма качественных решений в области информационной безопасности.

Последнее обстоятельство крайне положительно с точки зрения "рядового пользователя" информационных систем. Однако обратной стороной его является то, что задачи, стоящие перед экспертом, проводящим криминалистический анализ, значительно усложнились. Иными словами, лучше защищенным стал не только легитимный пользователь, но и злоумышленник. Простым, но показательным примером, иллюстрирующим вышеописанное явление, является эволюция систем шифрования. До 1999 года в США действовали экспортные ограничения, запрещавшие поставлять за рубеж средства шифрования (включая программные) с эффективной стойкостью ключа более 40 бит. После снятия указанных ограничений качество систем шифрования неуклонно повышалось. Сейчас обычным явлением стало 128- и даже 256-битное шифрование.

²⁷¹ Чиликов Алексей Анатольевич, к. ф.-м.н., МГТУ им. Н.Э. Баумана, Москва, МФТИ, Долгопрудный, Московская область, chilikov@passware.com

²⁷² Яковлев Алексей Николаевич, к. ю.н., доцент, МГТУ им. Н.Э. Баумана, Москва, ЦЭКИ, a_yakovlev@mail.ru

Общее наблюдение заключается в том, что специалистам по цифровой криминалистике необходимо не только хорошо понимать современные тенденции в области обеспечения информационной безопасности, но и уметь посмотреть на них "с другой стороны баррикады" - с позиции атакующего, а не защищающегося. В конечном итоге информационная безопасность и цифровая криминалистика преследуют общую цель - построение более безопасного мира, пресечение противоправных действий злоумышленников.

Следует отметить также поистине интернациональный характер возникающих задач и методов их решения. В самом деле, несмотря на существенные различия в традициях и правовых системах разных стран, информационные системы развиваются по схожим правилам, и методы исследования цифровых следов крайне похожи. А большинство особо опасных преступлений остаются таковыми вне зависимости от того, где они происходят, и против кого направлены. Это позволяет говорить о необходимости налаживания международного сотрудничества в области цифровой криминалистики, изучения и внедрения лучших мировых практик, использования самого совершенного инструментария.

Современные вызовы в цифровой криминалистике

Не претендуя на полноту, все же можно отметить ряд задач в области цифровой криминалистики, значение которых в последнее время неуклонно возрастает.

В первую очередь это задача исследования мобильных устройств. Бурное развитие мобильных сетей связи, удешевление услуг связи, рост объемов трафика привели к тому, что сейчас трудно встретить человека, не пользующегося мобильным устройством. Сами устройства превратились, по сути, в полноценные компьютеры, превосходящие по вычислительной мощности многие "настоящие" компьютеры недавнего прошлого. Таким образом, современный смартфон является неоценимым источником данных, которые могут быть использованы в процессе расследования. Однако доступ к этим данным становится все более сложной технической задачей. Это обусловлено, в первую очередь, уже упоминавшейся выше общей тенденцией к совершенствованию систем защиты. Разумеется, не упрощает задачу разнообразие типов мобильных устройств. Несмотря на некоторые общие принципы построения систем защиты, заложенные на уровне операционных систем, большое число нюансов различаются у различных производителей. Это приводит к тому, что исследование каждой новой модели устройства зачастую требует проведения отдельного исследования.

К счастью для практикующих экспертов, подобную работу в большинстве случаев, берут на себя производители специального программно-аппаратного инструментария, предоставляя уже готовые решения. Однако же, успеть за быстроразвивающимся рынком мобильных устройств удастся далеко не всегда.

Второй важной задачей является исследование криптографически защищенных объектов. Многие сложности при исследовании мобильных устройств связаны с применением в них достаточно качественных решений для шифрования пользовательских данных. Однако же данная проблематика, разумеется, не исчерпывается мобильными устройствами. Более того, в случае "классических" компьютеров она возникла гораздо раньше. В результате довольно длительной эволюции шифровальные средства, предлагаемые в современном программном обеспечении, стали надежными, дешевыми и удобными в применении даже для неподготовленного пользователя. Все современные операционные системы и многие приложения включают в себя встроенные возможности шифрования данных. Также присутствует ряд доступных специализированных решений. В качестве простой и наглядной иллюстрации сложности возникающей задачи можно привести простой расчет: современный компьютер с тактовой частотой 4ГГц может

произвести менее 2^{60} элементарных операций в течение года. Следовательно, для полного перебора 128-битного ключа потребуется работа 100 миллиардов таких компьютеров в течение примерно 2,5 миллиардов лет. Надежды на какие-либо "тайные алгоритмы взлома" также необоснованны. Достаточно сказать, что с момента публикации американского алгоритма DES до появления первых серьезных продвижений в его взломе прошло около 15 лет, а в случае с советским (а позже и российским) стандартом шифрования ГОСТ 28147-89 этот срок составил более 20 лет. Следует отметить, что практический взлом последнего алгоритма до сих пор представляется вычислительно неосуществимым. Однако после появления даже теоретических подходов к атакам, как в России, так и за рубежом были незамедлительно разработаны и введены в действие новые, более совершенные стандарты.

К счастью для практиков, задача обхода защит не всегда безнадежна. Большинство прикладных систем используют механизмы парольной защиты, что делает возможным переборные и словарные атаки на такие системы. Также существуют и иные методы, связанные, например, с анализом оперативной памяти, или же файлов гибернации.

Более классическими, но не менее актуальными задачами являются выявление и исследование вредоносного кода и восстановление поврежденных данных. Здесь следует отметить, что в последнее время подобные задачи также усложняются, в том числе и в связи с использованием механизмов шифрования и обфускации исполняемого кода.

Приятным для нас обстоятельством является наличие практически в каждом из упомянутых секторов серьезных отечественных производителей специализированного инструментария. При этом работа таких компаний, как Passware, Оксиджен Софт, Элкомсофт, Р-Лаб, Group-IB не ограничивается лишь российским рынком, все они хорошо известны и уважаемы и в мировом экспертном сообществе.

Профессиональное сообщество в цифровой криминалистике и смежных отраслях

К представителям профессионального сообщества следует, в первую очередь, отнести следующие категории специалистов: экспертов-практиков, непосредственно осуществляющих экспертизу в рамках следствия или же судебного процесса (как уголовного, так и гражданского), либо сопровождающих оперативные мероприятия при расследовании конкретных дел; производителей специализированного инструментария для решения конкретного круга экспертных задач; представителей научного сообщества. Требования к представителям данных категорий довольно существенно различаются. Однако именно их продуктивное взаимодействие позволяет существенно повысить эффективность работы, создавая лучшие технические решения и внедряя их в повседневную практику.

Ключевыми компетенциями для специалистов-производителей и исследователей являются, на наш взгляд: понимание современных технологий информационной безопасности; навыки программирования (включая системное и низкоуровневое) и реверс-инжиниринга, инженерная подготовка. Крайне полезным будет знание основ криптографии и общая математическая подготовка.

Для практикующих экспертов в большей степени важно знание особенностей исследований в конкретных классах дел, владение тактикой проведения экспертизы, уверенные знания специализированного инструментария, а иногда и готовность к его "творческой" доработке.

Также важным является упоминавшийся выше психологический: готовность встать на позицию "атакующего", при этом, не забывая об основной "позитивной" цели своей работы, и не вступая в противоречие с нормами закона и этики.

Организационные решения в области цифровой криминалистики

Организационные решения в области цифровой криминалистики необходимы для обеспечения постоянной и продуктивной коммуникации между различными категориями специалистов. Поскольку они решают различные задачи и обладают различным набором базовых компетенций, то первая из задач - научить их "говорить на одном языке", понимать потребности и возможности друг друга.

Очевидным решением здесь является регулярное проведение обучения практикующих экспертов специалистами-производителями, позволяющее практикам быть в курсе последних технологических достижений и применять имеющиеся инструменты максимально эффективно. Такое обучение может осуществляться как отдельными производителями или же поставщиками решений, так и в рамках мероприятий по повышению квалификации на базе учебных заведений.

Профессиональные научные конференции, выставки, также являются хорошим способом для повышения информированности о новейших достижениях, а также получения производителями обратной связи от практиков, обсуждения их насущных потребностей. Выявление и изучение лучших мировых практик экспертизы, совершенствование программ обучения, внедрение в учебный процесс лучшего доступного инструментария, разработка методик его использования — вот неисчерпывающий список возможных точек соприкосновения между практиками, производителями, представителями научного и вузовского сообщества.

Партнерство между производителями инструментария в смежных областях позволяет создавать высококачественные интегрированные решения, повышая эффективность работы пользователя, и достигая одновременно технологического и коммерческого успеха. Уже сейчас между ведущими производителями и поставщиками заключен ряд подобных партнерских соглашений. Также следует отметить, что в 2016 году в России была создана Ассоциация производителей программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий «ЭКСПИТ», объединившая ряд ведущих отечественных производителей.

Представляется интересной также идея повышения информированности о возможностях и ограничениях цифровой криминалистики нетехнических специалистов. В первую очередь это касается тех, кто ответственен за дальнейшее применение результатов экспертизы: следователей, судей, адвокатов.

Выводы

В настоящей работе проведен обзор современного состояния цифровой криминалистики и компьютерно-технической экспертизы, рассмотрены актуальные проблемы, стоящие перед отраслью и возможные пути их решения. Обзор основан на личном многолетнем опыте авторов в области цифровой криминалистики, компьютерно-технической экспертизы и разработки специализированного экспертного ПО, а также наиболее актуальных работах российских и зарубежных специалистов в данной области.

Данная работа была проведена с помощью Российского Научного Фонда Грант N 17-11-01377.

Литература

1. Яковлев А.Н. Цифровая криминалистика и её значение для расследования преступлений в современном информационном обществе. // В сб. Совершенствование следственной деятельности в условиях информатизации: сб. материалов междунар. науч.-практ. конф. (Минск, 12-13 апреля 2018 г.) / Следственный комитет Республики Беларусь; редкол.: С.Я. Аземша [и др.]. – Минск : Редакция журнала "Промышленно-торговое право", 2018. - 368 с. ISBN 978-985-6789-34-5. С. 357-362.
2. Мещеряков В.А., Яковлев А.Н. "Электронная" составляющая осмотра места происшествия. // Библиотека криминалиста. Научный журнал. 2015. № 5(22). ISSN 2224-0543. С. 280-291.

3. Мещеряков В.А. Цифровая криминалистика. // Библиотека криминалиста. Научный журнал. 2014. № 4 (15). ISSN 2224-0543. С. 231-241.
4. Мещеряков В.А. Цифровая криминалистика: становление и перспективы развития. В сборнике: Конституция Российской Федерации и ее влияние на практику государственного строительства и развитие правовой системы страны Материалы Международной научно-практической конференции, посвященной 55-летию юбилею юридического факультета Воронежского государственного университета. Сер. "Юбилеи, конференции, форумы" ФГБОУ ВПО "Воронежский государственный университет"; Юридический факультет; под редакцией Ю. Н. Старилова. 2014. С. 292-295.
5. Мещеряков В.А. Влияние информационного общества на развитие криминалистики. // Воронежские криминалистические чтения. 2015. № 17. С. 153-158.
6. Мещеряков В.А. Особенности специальных знаний, используемых в цифровой криминалистике. // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 87-92.
7. Мещеряков В.А. Криминалистика в цифровой век. // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2015. № 1. С. 9-12.
8. Яковлев А.Н. Цифровая криминалистика как фактор защиты цифровой экономики. // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) [Электронный ресурс] : сборник статей Международной научно-практической конференции. – Электронные текстовые данные (2,33 Мб). – М. : Академия управления МВД России, 2018. – 1 электр. опт.диск (DVD-R): 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц; ОЗУ 512 Мб; операц. система семейства Windows; AdobeReader v. 4.0 и выше; дисковод; мышь. – Загл. с титул. экрана. ISBN 978-5-906942-68-5. С. 325-331.
9. Adi Shamir and Nicko van Someren. Playing hide and seek with stored keys. \Lecture Notes in Computer Science, Vol. 1648, p. 118--124, 1998
10. Brian Kaplan. RAM is Key. Extracting Disk Encryption Keys From Volatile Memory. \Carnegie Mellon University. May 2007. Thesis Report
11. Алексеев Е.К., Чиликов А.А. Распознавание криптографических ключей в RAM // Системы высокой доступности. 2011. Т. 7, №2.
12. Чиликов А.А. Атаки по памяти. // Защита информации. Инсайд. №3, 2011
13. Чиликов А.А. Математические, инженерные и прикладные аспекты анализа содержимого RAM. // Труды Первой Межвузовской научно-практической конференции «Актуальные проблемы организации и технологии защиты информации» Санкт-Петербург: ИТМО, 2011.
14. Закаблук Д. В., Пикулин С. В., Чиликов А.А. Распределенная система восстановления паролей. // Second International Conference "Cluster Computing" CC 2013 (Ukraine, Lviv, June 3-5, 2013) \ <http://hpc-ua.org/cc-13/files/proceedings/55.pdf>
15. Хоруженко Г.И., Чиликов А.А. Восстановление ключевой информации, расположенной в образе оперативной памяти в зашифрованном виде. // Проблемы информационной безопасности. Компьютерные системы. Санкт-Петербург: Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого", 2015.
16. Чиликов А.А. О применении образов оперативной памяти для расшифрования защищенных данных при проведении криминалистического анализа. // Информатизация и информационная безопасность правоохранительных органов. Сборник трудов XXV Всероссийской научно-практической конференции \ Москва: Издательство: Академия управления Министерства внутренних дел Российской Федерации, 2016.

**Information Security and Digital Forensics:
problems, solutions and new challenges**
Chilikov A.A.²⁷³, Yakovlev A.N.²⁷⁴

Abstract. *In this paper we analyze current state and modern trends in digital forensics. We consider several hardest problems and discuss about difficulties and possible solutions. We talk about positive practical experience. Key requirements to digital forensic experts are considered/ Several ideas are proposed to make the communication between different experts more efficient/.*

Keywords: *computer forensics, mobile forensics, cryptography, encryption, data acquisition*

²⁷³ Chilikov Alexey, Ph.D/ (Math), Associate Professor of information Security Department, BMSTU, Senior Researcher, MIPT

²⁷⁴ Yakovlev Alexey, Ph.D/ (Law), Associate Professor of Jurisprudence Department, BMSTU

Угрозы информационной безопасности гражданского воздушного судна

Чичварин Н.В.²⁷⁵, **Медведев Н.В.**²⁷⁶

В докладе рассмотрена постановка проблемы обеспечения информационной безопасности (ИБ) комплексов связи и навигации гражданского воздушного судна (ГВС), с целью разработки аппаратуры, обеспечивающей комплексную безопасность полета. Анализ комплексных исследований, проводимых ведущими разработчиками Российской Федерации и развитых стран, показывает, что проблема безопасности полетов нарастает.

Ключевые слова: бортовая автоматизированная система, информационная уязвимость, бортовое радиоэлектронное оборудование

Введение

По мнению специалистов, в условиях возрастания сложности бортовых информационных систем всё более существенное значение приобретает проблема защиты автоматизированных систем авиационной техники от угроз информационной безопасности [1-7].

Хотя правила безопасности для подключенных к Интернету ВС в целом уже существуют и их требования внедряются на новых самолетах в виде так называемых особых условий сертификации, отрасль сейчас занята разработкой более всеобъемлющих систем обеспечения безопасности, с тем чтобы надежно защитить от злоумышленников растущие объемы передаваемых данных как в полете, так и на земле, включая обновления баз данных и загрузку информации о техническом состоянии ВС²⁷⁷. Ключевыми узлами передачи данных (а значит, и основными потенциальными мишенями кибератак²⁷⁸) являются роутеры или системные серверы, к которым сходятся различные шины данных и которые делают возможным интернет-соединение самолета с внешним миром.

2018 - 2019 годы отмечены кардинальными изменениями в отношении ведущих мировых авиатехнических корпораций и исследовательских центров к киберугрозам, смысл которых - свести воедино технологии и практические наработки специализирующихся на безопасности бортового радиоэлектронного оборудования (БРЭО²⁷⁹) и IT-секторов компаний, для исследования потенциальных информационных уязвимости продуктов авионики²⁸⁰. Основными целями исследований при этом являются:

- анализ источников атак на средства связи и навигации ЛА,
- анализ характера и последствий атак на ЛА,

Проведенные исследования показывают, что источниками угроз, как правило, являются:

- беспроводные информационно-телекоммуникационные устройства пассажиров, находящиеся на борту ЛА во время полета;
- атаки внешних злоумышленников по беспроводным радиоканалам каналам передачи данных, обеспечивающим доступ к бортовой вычислительной сети.
- помехи, случайно, либо умышленно поставленные с помощью средств радиоэлектронной борьбы (РЭБ)

²⁷⁵ Чичварин Николай Викторович, к.т.н., доцент кафедры ИБ, МГТУ им.Н.Э.Баумана, Москва

²⁷⁶ Николай Викторович Медведев, к.т.н., доцент кафедры ИБ, МГТУ им.Н.Э.Баумана, Москва, medvedevnick54@yandex.ru

²⁷⁷ Документы ИКАО. URL: airspot.ru/library/dokumenty-ikao.

²⁷⁸ www.aviasafety.ru/crash-stat

²⁷⁹ Воздушный кодекс РФ от 19.03.1997 N 60-ФЗ.

²⁸⁰ Анализ состояния безопасности полетов в гражданской авиации в 2013 году. URL: www.dvmtu-favt.ru/upload/medialibrary/

С большой степенью точности можно прогнозировать действия злоумышленников по вредоносному воздействию на ГВС. Участвовавшие локальные и региональные конфликты, в которых применяются современное высокоточное оружие и средства РЭБ угрожают почти напрямую ГВС находящихся в полете даже на значительном удалении от зоны боевых действий. Таким образом, вопросы проектирования средств обеспечения ИБ средств связи, управления и навигации ГВС следует считать актуальными.

Для достижения поставленных целей должны быть решены следующие задачи:

1. Анализ участков полета ГВС.
2. Анализ угроз ИБ на всех участках полета ГВС.
3. Анализ средств противодействия угрозам средствам связи ГВС.
4. Разработка технического облика средства обеспечения ИБ средств связи и навигации ГВС на критическом участке полета ГВС.

Несмотря на принимаемые меры для защиты автоматизированных систем управления АСУ воздушным движением (АСУ ВД), существуют значительные недостатки в обеспечении ИБ, связанные с навигационными системами и сетями. Значительное количество недостатков выявлено в системах контроля доступа, изменений конфигурации АСУ ВД. Выявлены недостатки межсетевого взаимодействия АСУ ВД и прочих информационных систем. На сегодняшний день выявлены следующие 12 угроз информационной безопасности в авиационной отрасли и системах управления воздушным движением.

1. *Процедуры идентификации и аутентификации субъектов доступа к объектам доступа выполняются не в полном объеме.* Несмотря на наличие политики безопасности, АСУ ВД не защищал границу своих сетей от возможных проникновений.

2. *Недостаточная изоляция сетей.* Реализованы многочисленные элементы разграничения АСУ ВД, но этого не всегда достаточно для защиты или ограничения взаимодействия между внешними и внутренними сетями. Чрезмерное межсетевое взаимодействие между рассмотренными системами увеличивает риск компрометации критически важных систем управления воздушным движением.

3. *Слабые пароли.* Все еще имеет место безграмотная реализация механизма управления идентификацией и аутентификацией пользователей, несмотря на политику безопасности и рекомендации компетентных структур. К серверам и приложениям, используемым в АСУ ВД применяли слабый пароль, что влекло за собой нежелательные последствия.

4. *Слабый контроль управления доступом.* Не всегда обеспечен тот факт, что доступ пользователей к ключевым системам управления воздушным движением был полномочен. В ряде случаев возможны ошибки в предоставлении прав доступа. Пользователи системы также имели больше полномочий, чем требовалось для осуществления своей работы.

5. *Отсутствие криптографической защиты информации.* Далеко не всегда данные были зашифрованы во время обработки или сохранения, как того требует политика безопасности или требования регуляторов. Например, сетевые устройства не всегда шифровали данные аутентификации при передаче по сети, а другие системы не всегда шифровали пароли. Из-за слабых мест атакующие могут просмотреть и изменить передаваемые данные.

6. *Мониторинг состояния ИБ и самооценка проводятся не в полном объеме.* Недостаточно реализованы процедуры мониторинга состояния текущего уровня ИБ и проведение самооценки. Например, не всегда проконтролирован сетевой трафик или системы АСУ ВД не всегда реагируют на важные события в системе информационной безопасности. В результате — невозможность обнаружения НСД в АСУ ВД.

7. *Отслеживание изменений в конфигурации АСУВД проводится не в полном объеме.* Существуют слабые места в управлении конфигурацией технических средств АСУВД, что увеличивает риск раскрытия, несанкционированного доступа, модификации и потери информации. Кроме этого, в ряде задач для обслуживания АСУВД эксплуатирует неквалифицированный и слабо подготовленный персонал.

8. *Политики и процедуры реагирования на инциденты установлены не в полном объеме.* В ряде АСУВД политики и процедуры отчетности на инциденты ИБ не всегда указывают требуемые сроки отчетности или необходимость выявления инцидентов. Без доработки правил реагирования на инциденты всегда имеется повышенный риск невозможности реагировать на инциденты должным образом.

9. *Недостаток осведомленности персонала, обслуживающего критичные системы относительно механизмов обеспечения ИБ.* Политика безопасности утверждает, что весь персонал агентства гражданской авиации и подрядчики должны проходить ежегодные тренинги — повышение осведомленности в сфере информационной безопасности, а персонал связанный с обеспечением ИБ должен получать обучение согласно их ролям в системе обеспечения ИБ. Однако это не так.

10. *Отсутствие формального процесса анализа или документирования потенциального воздействия инцидентов на функционирование АСУВД.*

11. *Недостаточность тестирования возможностей реагирования на инциденты ИБ.*

12. *Планы непрерывности не завершены или не протестированы должным образом.* Не обеспечена готовность резервных планов для систем управления воздушным движением и диспетчерской службы. Планы обеспечения непрерывности были слабо или в не полной мере протестированы.

Вывод

Фундаментальная причина такого состояния дел в ИБ авиационной отрасли состоит в отсутствии реализации эффективной программы для управления ИБ, что выражается прежде всего в нечетком назначении ответственных за обеспечение ИБ. А отсутствие понимания четких целей, направления и показателей ИБ, вокруг которых можно организовать программу ИБ является следствием отсутствия стратегической политики ИБ.

Литература

1. Волосатова Т.М., Чичварин Н.В. Способы моделирования аппаратуры модульной авионики в условиях вредоносных воздействий // В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 58-63.
2. Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. 2016. № 6 (111). С. 85-96.
3. Глинская Е.В., Чичварин Н.В. Специфика конструирования бортовой аппаратуры модульной авионики с учетом требований информационной безопасности// В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 43-57.
4. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна // Вопросы кибербезопасности. 2018. № 4 (28). С. 9-20.
5. Чичварин Н.В. Базовые программные средства рабочих станций анализа ГИС-информации // Вопросы кибербезопасности. 2014. № 5 (8). С. 7-16.
6. Чичварин Н.В. Оптическая система связи и навигации для обеспечения безопасной посадки самолета // Информационно-измерительные и управляющие системы. 2018. Т. 16. № 10. С. 43-51.

7. Козарь А.А. Проблема информационной безопасности в сфере авионики // В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019. С.180-184.

Threats to the Information Security of a Civil Aircraft **Chichvarin N.V., Medvedev N.V.**

Abstract: The report considers the statement of the problem of ensuring information security (IS) of communication and navigation systems of a civil aircraft (GVS), with the aim of developing equipment that provides integrated flight safety. An analysis of comprehensive research conducted by leading developers of the Russian Federation and developed countries shows that the problem of flight safety is growing.

Keywords: on-board automated system, information vulnerability, on-board electronic equipment

Интеллектуальная защита сложных организационно-технических систем

И.И. Чукляев²⁸¹, Е.А. Чепурной²⁸², А.Л. Шевченко²⁸³

Аннотация. Обобщенно раскрыты разработанные методы и модели, созданные программные средства и предлагаемые технические решения для интеллектуальной защиты сложных организационно-технических систем в интересах решения актуальной научной проблемы в различных областях системы знаний: анализ информационно-управляющих систем и формирование информационных ресурсов, интеллектуальные системы комплексной защиты информации, построение сложных реляционных баз данных, разработка безопасного программного обеспечения, нечеткое моделирование и обучение нейро-нечетких моделей. Исследования выполнены при поддержке грантов Президента РФ и Российского фонда фундаментальных исследований.

Ключевые слова: информационная безопасность, риски нарушения защищенности, организационно-технические системы

Введение

Целью выполняемого научного исследования является повышение защищенности сложных организационно-технических систем (ОТС), для достижения которой предложена теория интеллектуальной защиты информации, созданы программные средства и технические решения для интеллектуальной защиты ОТС [1–3].

Актуальность и проблематика научного исследования подтверждена соответствием:

Доктрине информационной безопасности, утвержденной Указом Президента РФ от 05 декабря 2016 г. № 646;

приоритетным направлениям Стратегии научно-технологического развития РФ, утвержденной Указом Президента РФ от 01.12.2016 г. № 642, в части, касающейся создания систем искусственного интеллекта и обработки большого объема данных (п. 20, а), противодействия киберугрозам (п. 20, д);

дополненному проекту Федерального закона от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в РФ» приоритетными направлениями научно-технологического развития информационно-коммуникационных технологий в части, касающейся разработки функционально-ориентированных систем защиты информационных ресурсов и развития технологий статического, динамического и комбинированного анализа, обфускации (компиляторного преобразования) программного обеспечения (ПО) [1];

Плану фундаментальных исследований Российской академии наук на период 2011–2025 гг. в части, касающейся развития методов и технологий анализа и снижения уязвимостей, обфускации ПО (п. 1.5.5), организации данных неструктурированной информации и обеспечения их информационной безопасности в распределённой информационной среде (п. 4.1);

²⁸¹ Чукляев Илья Игоревич, доктор технических наук, доцент, Военная академия войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А.М.Василевского, Смоленск, smolrsu@mail.ru

²⁸² Чепурной Евгений Анатольевич, Военная академия войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А.М.Василевского, Смоленск, chepurnoy202@gmail.com

²⁸³ Шевченко Александр Леонидович, Военная академия войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А.М.Василевского, Смоленск, smolarm@pochta.ru

дополненному научно-техническому заделу при разработке базовых технологий производства приоритетных компонентов радиоэлектронной аппаратуры в рамках подпрограммы «Развитие производства вычислительной техники» Государственной программы РФ «Развитие электронной и радиоэлектронной промышленности на 2013–2025 гг.» [1];

ГОСТ Р 56939–2016 и ГОСТ Р 51897–2011, регламентирующими требования к разработке безопасного ПО и управлению рисками сложных ОТС.

При выполнении исследования использован системный подход, сочетание подходов к структурно-функциональному анализу систем и объектно-ориентированному формированию информационных ресурсов, онтологический подход, подход к оцениванию защищенности ИУС на основе паттернов дефектов ПО, подход к нечеткому моделированию и обучению нейро-нечетких моделей, дедуктивный метод создания аксиоматической теории функциональных баз данных, методы управления рисками и разработки безопасного ПО, математической статистики, имитационного и физического моделирования, сравнительного и экспертного анализа, экспериментальных исследований.

Основными результатами в развитии теории интеллектуальной защиты информации являются:

- а) Теоретические основы интеллектуальной защиты информации, включающие: результаты систематизации и классификацию методов и средств информационного противоборства; разработанную онтологическую модель защищенных функционально-ориентированных информационных ресурсов (ЗФОИР) ИУС; уточненные закономерности построения интеллектуальных систем комплексной защиты информации, сформулированные принципы и правила к интеллектуальным системам защиты ОТС, превентивной защите ПО, адаптивному и дифференцированному применению классов мероприятий по обеспечению (повышению) защищенности информационных потоков данных (ИПД), обоснованные требования к ним.
- б) Разработанный метод анализа ИУС и формирования ЗФОИР.
- в) Разработанный интеллектуальный метод комплексной защиты ИУС.
- г) Разработанный метод повышения защищенности ПО.

2. Основными результатами в создании интеллектуальных средств и технических решений для интеллектуальной защиты ОТС являются:

- д) Разработанное научно-методическое, информационное и алгоритмическое обеспечение, созданные программные средства и предложенные технические решения для интеллектуальной защиты ОТС [1, 4], включающей превентивную защиту ПО, адаптивную и дифференцированную защиту ИПД, которые учитывают требования концепции управления рисками, дополняют этапы жизненного цикла разработки безопасного ПО и включают в себя:

способы: использования вариантов противодействия сетевой и потоковой компьютерным разведкам и сетевым атакам и систему его реализующую [1, 4–5]; адаптивного мониторинга информационно-технических воздействий (ИТВ) [1, 4, 6], выбора средств и способов защиты ОТС от групповых разнородных ИТВ и систему его реализующую [1, 4, 7], моделирования мониторинга рисков для ИУС в условиях ИТВ [1, 4, 8]; динамического управления параметрами сети связи в признаковом пространстве [1, 4, 9]; обеспечения живучести распределенной абонентской сети связи [1, 4, 10];

модели и способы их построения: композиционную модель ИУС [1, 4, 11–12]; гибридную модель (ГМ) комплексного управления рисками нарушения защищенности ИУС, состоящую из нечетких деревьев (НД) и нечетких продукционных моделей (НПМ) нарушения защищенности ЗФОИР ИУС, игровых моделей (ИМ) формирования стратегий

и нейро-нечетких моделей (ННМ) формирования классов мероприятий по управлению рисками нарушения защищенности ЗФОИР ИУС [1, 4, 13–15];

алгоритмы: применения ГМ [1, 4]; построения НД и НПМ, ИМ и ННМ; обучения ННМ [1, 4, 16]; поиска ошибок при написании исходного кода ПО для типового правила, обоснования применимости правил при написании исходного кода ПО, генерации уникальных экземпляров бинарного кода ПО [1, 4, 17–19];

программы: минимизации риск-ситуаций нарушения защищенности ИУС [1, 4, 13]; моделирования мониторинга нарушения защищенности ИУС [1, 4, 14]; статического анализа и проверочные модули [1, 4, 17]; обфусцирующий компилятор и инструментатор исполняемого кода [1, 4, 18–19].

е) Выработанные рекомендации и предложения по внедрению, реализации и использованию результатов исследований:

при актуализации Прогноза научно-технологического развития РФ на период до 2030 г. и формировании Федерального закона от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в РФ»;

при формировании научно-технических направлений в прорывных исследованиях мирового уровня в области защиты информационных технологий и кибербезопасности АСУ;

в научно-техническом заделе при разработке базовых технологий производства приоритетных компонентов радиоэлектронной аппаратуры в рамках подпрограммы «Развитие производства вычислительной техники» Государственной программы РФ «Развитие электронной и радиоэлектронной промышленности на 2013–2025 гг.»;

на предприятиях промышленности РФ и в изделиях различного назначения.

Теоретическая значимость научной результатов подтверждается:

а) решением актуальной научной проблемы;

б) созданием нового научного направления «Интеллектуальная защита ОТС»;

в) развитием теории интеллектуальных систем комплексной защиты информации в следующих областях системы знаний:

в области анализа ИУС и формирования информационных ресурсов – разработанным методом анализа ИУС и формирования ЗФОИР на основе сочетания подходов к структурно-функциональному анализу систем и объектно-ориентированному формированию информационных ресурсов;

в области построения сложноструктурированных «больших» данных (хранилищ) – развитым подходом к построению и использованию сложно структурированных «больших» данных (хранилищ) на основе разработанной многоосновной алгебраической структуры;

в области интеллектуальных систем комплексной защиты информации:

результатами систематизации и классификацией методов и средств информационного противоборства в соответствии с обоснованным набором требований разделимости, согласованной иерархичности, репрезентативности, полноты и непротиворечивости;

развитым онтологическим подходом к представлению системы знаний в сфере комплексной защиты ИУС, дополненным и уточненным понятийно-терминологическим аппаратом на основе разработанной онтологической модели ЗФОИР ИУС;

уточненными закономерностями построения интеллектуальных систем комплексной защиты информации относительно системных закономерностей, закономерностей иерархической упорядоченности, закономерностей целеобразования, закономерностей управления рисками нарушения защищенности и закономерностей развития, сформулированными принципами и правилами, обоснованными требованиями к ним;

разработанным интеллектуальным методом комплексной защиты ИУС на основе комплексного управления рисками нарушения защищенности ЗФОИР ИУС предлагаемой гибридной моделью;

предлагаемым подходом к оценке защищенности ИУС на основе предлагаемых паттернов дефектов исходного и бинарного кодов ПО;

в области разработки безопасного ПО – разработанным методом повышения защищенности ПО на основе сочетания развитых подходов к статическому анализу исходного кода ПО и к обфускации исходного кода ПО;

в теории нечеткого моделирования и обучения нейро-нечетких моделей – разработанным подходом к нечеткому моделированию и обучению нейро-нечетких моделей на основе предлагаемых игровых моделей.

Практическая значимость научных результатов определяется научно-техническим уровнем и масштабом потенциального и осуществленного внедрения, реализации и использования результатов исследований.

Выводы.

Разработанные программные средства и технические решения для интеллектуальной защиты ОТС позволили:

дополнить существующие меры информационной защиты, прогнозировать и снизить риски нарушения защищенности изделий и ИУС различного назначения на этапах разработки, внедрения и эксплуатации;

повысить живучесть распределенной абонентской сети связи, интегрированной с Единой сетью электросвязи;

повысить защищенность узлов связи Единой сети электросвязи от компьютерной разведки и ИТВ;

повысить достоверность результатов мониторинга рисков для ИУС;

увеличить время наступления отказа Единой сети электросвязи в предоставляемых услугах при обслуживании абонентов;

сократить время анализа исходного кода ПО на наличие дефектов до значений, не превышающих время сборки ПО.

Исследования выполнены при поддержке грантов Президента РФ № МК-755.2012.10 (2012–2013 гг.) и МК-3604.2014.10 (2014–2015 гг.), Российского фонда фундаментальных исследований № 13-07-97518 (2010 г.) и № 10-07-97502 (2013–2015 гг.) [1–19].

Литература

1. Чукляев, И. И. Метод и модели комплексного управления рисками нарушения защищенности информационно-управляющих систем: монография. – Смоленск: ВА ВПВО ВС РФ, 2017. – ISBN 978-5-9906429-9-7. Рецензенты: чл.-кор. РАН, д-р физ.-мат. наук, профессор А. И. Аветисян (ИСП РАН); д-р техн. наук, профессор В. В. Борисов (НИУ МЭИ); д-р техн. наук, профессор С. Д. Кузнецов (ВМиК МГУ). – 144 с.

2. Чукляев, И. И. Вычислительные системы боевого управления войсковой ПВО: теоретическое обобщение, развитие, практические результаты: монография / И. И. Чукляев, А. В. Морозов, В. В. Борисов. – Смоленск: ВА ВПВО ВС РФ; изд-во «Смоленская городская типография», 2013. – ISBN 978-5-94223-588-8. Рецензенты: заслуженный военный специалист РФ, д-р воен. наук, профессор А. Д. Гаврилов (ВА ВПВО ВС РФ); заслуженный деятель науки РФ, д-р техн. наук, профессор В. М. Константиновский (ОАО «Концерн «Моринсис-Агат»); д-р воен. наук, канд. техн. наук, профессор Н. И. Турко (ВА ГШ ВС РФ). – 448 с.

3. Чукляев, И. И. Теоретические основы оптимального построения адаптивных систем комплексной защиты информационных ресурсов распределительных вычислительных систем: монография / И. И. Чукляев, А. В. Морозов, И. Б. Болотин. – Смоленск: ВА ВПВО ВС РФ, 2011. Рецензенты: д-р техн. наук, профессор П. М. Лопашин, д-р техн. наук, профессор В. И. Мищенко. – 227 с.

4. Чукляев, И. И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем // Вопросы кибербезопасности. 2016. – № 4(17). С. 61–71. – DOI 10.21681/2311-3456-2016-4-61-71.

5. Пат. № 2597457 Способ противодействия сетевой и потоковой компьютерным разведкам, сетевым атакам и система поддержки и принятия решений сетевого администратора компьютерной сети / И. И. Чукляев, Е. В. Гречишников, М. М. Добрышин, С. М. Климов, А. Н. Реформат. – М.: ФИПС (Роспатент), 2018. – Заявка № 2018105350. – Дата поступления 31.01.2018.

6. Пат. Адаптивная система мониторинга информационно-технических воздействий / И. И. Чукляев, М. М. Добрышин, П. В. Закалкин, Е. В. Гречишников, Д. Е. Шугуров, А. Л. Шевченко, А. В. Чижаньков. – М.: ФИПС (Роспатент), 2019. – Заявка № 2019123565. – Дата поступления 26.07.2019.

7. Пат. Система выбора средств и способов защиты организационно-технических систем от групповых разнородных информационно-технических воздействий / И. И. Чукляев, М. М. Добрышин, П. В. Закалкин, А. В. Чижаньков. – М.: ФИПС (Роспатент), 2019. – Заявка № 2019123568. – Дата поступления 26.07.2019.

8. Пат. № 2634169 Способ моделирования мониторинга рисков для информационно-управляющей системы в условиях информационно-технических воздействий / И. И. Чукляев, М. Ю. Храмов, К. Ю. Лавров, С. И. Туник, О. Н. Николаева. – М.: ФИПС (Роспатент), 2016. – Заявка № 2016147901. – Дата поступления 07.12.2016. – Дата регистрации 24.10.2017.

9. Пат. № 2597457 Способ динамического управления параметрами сети связи в признаковом пространстве / И. И. Чукляев, Е. В. Гречишников, М. М. Добрышин, С. П. Горелик. – М.: ФИПС (Роспатент), 2016. – Заявка № 2015111536. – Дата поступления 30.03.2015. – Дата регистрации 22.08.2016.

10. Пат. № 2600941 Способ обеспечения живучести распределенной абонентской сети связи / И. И. Чукляев, Д. О. Белоконев, С. П. Горелик, А. В. Скубьев, А. С. Белов. – М.: ФИПС (Роспатент), 2016. – Заявка № 2015130262. – Дата поступления 21.07.2015. – Дата регистрации 27.10.2016.

11. Чукляев, И. И. База данных защищенных функционально-ориентированных информационных ресурсов: база данных / И. И. Чукляев. – М.: ФИПС (Роспатент), 2016. – Заявка № 2016620690. – Дата поступления 13.05.2016. – Дата регистрации 23.09.2016. – Свидетельство о регистрации № 2016621313.

12. Чукляев, И. И. Композиционная модель и способ построения функционально-ориентированных информационных ресурсов информационно-управляющих систем / И. И. Чукляев // Труды ИСП РАН. – М.: ИСП РАН, 2016. – Т. 28. – Вып. 2. – С. 259–270. – DOI 10.15514/ISPRAS-2016-28(2)-17. – ISBN 2079-8156.

13. Чукляев, И. И. Программа минимизации риск-ситуаций защищенности функционально-ориентированных информационно-управляющих систем: программа ПЭВМ / И. И. Чукляев. – М.: ФИПС (Роспатент), 2016. – Заявка № 2016615293. – Дата поступления 13.05.2016. – Дата регистрации 07.07.2016. – Свидетельство о регистрации № 2016617543.

14. Чукляев, И. И. Программа моделирования мониторинга нарушения доступности, целостности и конфиденциальности для информационно-управляющей системы: программа ПЭВМ / И. И. Чукляев, М. Ю. Храмов, С. И. Туник, О. Н. Андреева. – М.: ФИПС (Роспатент), 2017. – Заявка № 2016663362. – Дата поступления 07.12.2016. – Дата регистрации 16.03.2017. – Свидетельство о регистрации № 2017613346.

15. Чукляев, И. И. Игровая модель обоснования средств комплексной защиты информационных ресурсов иерархической информационно-управляющей системы // И. И. Чукляев // Т-Comm: Телекоммуникации и транспорт. – М.: Медиа Паблишер, 2015. – Т. 9. – № 2–2015. – С. 64–68. – ISBN 2072-8735 (Print), 2072-8743 (Online).

16. Чукляев, И. И. Методика построения и нечеткая модель оценки защищенности и выбора классов мероприятий по минимизации рисков на основе нейронечеткого классификатора / И. И. Чукляев // Известия СмолГУ. – Смоленск: СмолГУ, 2015. – Вып. 2/1. – С. 312–319. – ISBN 2072-9464.

17. Чукляев, И. И. Инструмент статического анализа «RuleChecker» для языков С и С++: программа ПЭВМ / И. И. Чукляев, В. Н. Игнатьев, А. А. Белеванцев. – М.: ФИПС (Роспатент), 2016. – Заявка № 2015662101. – Дата поступления 10.12.2015. – Дата регистрации 04.02.2016. – Свидетельство о регистрации № 2016611555).

18. Чукляев, И. И. Обфусцирующий компилятор для затруднения эксплуатации уязвимостей: программа ПЭВМ / И. И. Чукляев, А. Р. Нурмухаметов, Ш. Ф. Курмангалеев, С. С. Гайсарян. – М.: ФИПС (Роспатент), 2016. – Заявка № 2016616567. – Дата поступления: 22.06.2016. – Дата регистрации 07.10.2016. – Свидетельство о регистрации № 2016661393.

19. Чукляев, И. И. Инструментатор исполняемого кода ELF ARM на базе пакета binutils: программа ПЭВМ / И. И. Чукляев, М. К. Ермаков, С. П. Вартанов, А. Ю. Герасимов. – М.: ФИПС (Роспатент), 2016. – Заявка № 2016616632. – Дата поступления: 22.06.2016. – Дата регистрации 11.08.2016. – Свидетельство о регистрации № 2016619020.

Informational security of technical systems

I.I. Chuklyayev²⁸⁴, E.A. Chepurnoy²⁸⁵, A.L. Shevchenko²⁸⁶

Abstract. *Developed methods and models, created software tools and proposed technical solutions for information security of technical systems are disclosed.*

Keywords: *information security, risks of violation of security, technical systems*

²⁸⁴ Chuklyayev Ilya Igorevich, Dr.Sc., Associate Professor, Military Academy of Air Defense of the Armed Forces of the Russian Federation, Smolensk, smolrsu@mail.ru

²⁸⁵ Chepurnoy Evgeny Anatolyevich, Military Academy of Air Defense of the Armed Forces of the Russian Federation, Smolensk, chepurnoy202@gmail.com

²⁸⁶ Shevchenko Alexander Leonidovich, Military Academy of Air Defense of the Armed Forces of the Russian Federation, Smolensk, smolarm@pochta.ru

Цепочки блоков в защите пространственных данных

Шайтура С.В.²⁸⁷, Минитаева А.М.²⁸⁸, Феоктистова В.М.²⁸⁹, Ордов К.В.²⁹⁰

В статье описаны принципы использования технологии блокчейн в различных пространственных задачах: в логистических системах, кадастровой деятельности, отслеживании перемещения людей, товаров вещей через Интернет на основе глобального позиционирования. В логистических задачах при производстве товара формируется токен, который сопровождает вещь до момента доставки. В кадастровой деятельности с каждым участком земли связывается токен, в котором учитываются характеристики участка и его владельцы. В общественном транспорте все передвижения могут контролироваться и оплачиваться при помощи блока цепочек. Технология блокчейн полностью исключает потерю вещей и людей.

Ключевые слова: блокчейн, пространственные технологии, криптографические методы

Введение

Технология цепочка блоков (блокчейн) основаны на трех принципах: распределенность, открытость, защищенность [1]. В статье проанализированы возможности использования этой технологии в различных пространственных задачах.

1. ГИС-сервисы на основе блокчейн в системе логистики

Существенным отличием методов управления в логистических системах является то, что в нем широко используется управление не только потоками и стационарными объектами, но и подвижными объектами [2, 3]. Учет отношений между пространственными данными очень важен для информационно логических систем, так как расход и пополнение ресурсов осуществляется в реальном пространстве и времени, что приводит к необходимости учитывать реальные пространственно – логические отношения, существующие в процессе перевозки и доставки [4].

Жизненный цикл [5] логистической поставки товара проходит этапы производство, комплектация, отгрузка, приемка, реализация. При смене этапов производятся транзакции в банковских операциях. Эти транзакции целесообразно проводить с помощью блокчейна. При производстве товара генерируется токен, который передается следующему владельцу товара, а в базу данных заносится произведенное действие. Архитектура системы включает клиентов, ГИС – сервис, распределенную базу данных, блокчейн.

2. Использование блокчейн в кадастровой деятельности

В случае составления кадастровых планов между участниками операций нет доверия, и существует необходимость в открытости. Самое слабое звено – это кадастровое бюро, где данные могут быть потеряны или могут быть совершены ложные сделки, что нельзя обнаружить сразу [6].

²⁸⁷ Шайтура Сергей Владимирович, доцент, кандидат технических наук, Российский университет транспорта (МИИТ), Москва, swshaytura@gmail.com

²⁸⁸ Минитаева Алина Мажитовна, доцент, кандидат технических наук, Московский государственный технический университет им. Н. Э. Баумана название организации, Москва, aminitaeva@mail.ru

²⁸⁹ Феоктистова Валентина Михайловна, доцент, кандидат технических наук, Российский государственный университет туризма и сервиса, Москва, vfeoktistova@gmail.com

²⁹⁰ Ордов Константин Васильевич, доктор экономических наук, Российский экономический университета имени Г.В. Плеханова Москва, post@ic-center.ru

Рассмотрим процедуру регистрации кадастровых записей на основе блокчейн. Связь между различными заинтересованными сторонами производится по заявке. Вся информация о собственности (текущий владелец, кадастровый план) оцифровывается и помещается в блокчейн. Имеется контракт, который гарантирует, что оцифрованное пространство регулируется определенными правилами. Приложение используется в виде интерфейса для облегчения всех транзакций. Договор купли – продажи перерабатывается в хеш-код и помещается в блокчейн. Банки, агенты по недвижимости, покупатели земли могут подтвердить достоверность этого соглашения о покупке и других документов посредством их уникальной цифровой подписи (хеш на блочной цепочке).

Алгоритм использования блокчейн следующий. Во-первых, через интерфейс открытого ключа сообщается всем заинтересованным лицам. Во-вторых, разрабатывается протокол, который связывает покупателя с продавцом, недвижимость, платеж, банк, смарт-контракт и реестр. В-третьих, используются специально улучшенные смартфоны, которые могут обрабатывать цифровые подписи, персональные компьютеры и телефон для взаимодействия с телефоном через некоторую форму аутентификации. Все это может работать в рамках блокчейн.

В Москве технологию блокчейн намерены широко применять в управлении городом, в частности, в сферах ЖКХ, здравоохранения, кадастрового учета, распределения субсидий и госзакупок [7] .

3. Блокчейн и геопространственные данные

Представьте себе путешественника в системе общественного транспорта, который использует смарт-мобильный, содержащий токены. Когда человек садится на автобус, крипто-пространственный слой отмечает точку посадки и точку высадки и автоматически взимает плату за проезд из пространственного кошелька путешественника и зачисляет его в пространственный кошелек транспортной компании. Нет необходимости в использовании карт или пополнении карт. Дебиты и кредиты подсчитываются мгновенно, и транзакция автоматически согласовывается с блок-цепочкой [8, 9, 10].

Движение товаров, перегрузку можно отслеживать, а расходы на доставку рассчитываются и дебитируются автоматически. Данные могут включать спутниковые данные, карты, данные земельных участков, данные 3D-визуализации и многое другое. Таким образом, пространственные данные со спутников, беспилотных летательных аппаратов и даже измерения на местности могут быть легко оценены и распределены. Защита данных может быть встроена через токены.

Выводы

Применение технологии блокчейн позволяет полностью контролировать пространственное перемещение произведенного товара, а в сочетании с технологиями пространственного позиционирования устраняет возможности краж. Блокчейн поможет снизить затраты на контроль за распределением продукции, повысит уровень доверия между участниками обменного процесса в процессе логистических перевозок.

Литература

1. Хрисанова Е.А. Разработка методики защиты распределенной геоинформационной базы данных// Славянский форум.- 2017.- № 3 (17).- С. 163 - 167.
2. Трубач Г.Г. Разработка среды мониторинга товарно-транспортных потоков на основе технологий блокчейн – В сборнике: Белорусский государственный университет. Научная конференция студентов и аспирантов. Сборник работ 74-й научной конференции студентов и аспирантов Белорусского государственного университета: в 3 частях. 2017. С. 96 – 99.
3. Антоненкова А.В., Шайтура С.В. Анализ информационных систем в логистике // Транспортное дело России. -2015.- № 5. - с. 105-106.

4. Shaitura S.V., Kozhaev Yu.P., Ordov K.V., Vintova T.A., Minitaeva A.M., Feoktistova V.M. Geoinformation services in a spatial economy // International Journal of Civil Engineering and Technology. 2018. T. 9. № 2. С. 829-841.
5. Дик В.В., Шайтура С.В. Жизненный цикл информационных систем // Вестник МГТУ МИРЭА. - 2014. - № 3 (4). - с. 116-129.
6. Павлов С.А. Совершенствование технологии формирования территориальных зон объектов техногенной безопасности при введении государственного земельного кадастра// Славянский форум.- 2017.- № 3 (17).- С. 144 - 149.
7. Хачатурова С.С. Роль компьютера в жизни человека // Международный журнал экспериментального образования. 2016. № 12-1. С. 49
8. Shaitura S.V., Kozhaev Yu.P., Ordov K.V., Antonenkova A.V., Zhenova N.A. Performance evaluation of the electronic commerce systems // [Espacios](#).- 2017.- Т. 38.- № 62.- С. 11.
9. Shaitura S.V., Minitaeva A.M, Ordov K.V., Shaparenko V.V. Virtual enterprises in a spatial economy // International Journal of Recent Technology and Engineering (IJRTE) -2019. Т. 7. № 6. С. 719 - 724.
10. Shaitura S.V., Ordov K.V., Lesnichaya I.G., Romanova Yu. D., Khachaturova S.S. Services and mechanisms of competitive intelligence on the internet // [Espacios](#).- 2018.- Т. 39.- № 45.- С. 24.

Blockchains in Spatial Data Protection

Shaytura S.V.²⁹¹, Minitaeva A.M.²⁹², Feoktistova V. M.²⁹³, Ordov K.V.²⁹⁴

The article describes the principles of using blockchain technology in various spatial tasks: in logistics systems, cadastral activities, tracking the movement of people, goods of goods over the Internet based on global positioning. In logistics tasks, a token is formed during the production of goods, which accompanies the thing until delivery. In cadastral activities, a token is associated with each plot of land, which takes into account the characteristics of the plot and its owners. In public transport, all movements can be controlled and paid using a block of chains. Blockchain technology completely eliminates the loss of things and people.

Keywords: *blockchain, spatial technologies, cryptographic methods*

²⁹¹ Shaytura Strgey Vlodimirovich, Ph.D., Associate Professor, Russian University of Transport (MIIT), Moscow, swshaytura@gmail.com

²⁹² Minitaeva Alina Mazhitovna, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, aminitaeva@mail.ru

²⁹³ Feoktistova Valentina Michaylovna, Ph.D., Associate Professor, Russian State University of Tourism and Service, Moscow, vfeoktistova@gmail.com

²⁹⁴ Ordov Konstantin Vasilievich, Dr.Sc., Professor, Plekhanov Russian University of Economics, Moscow, post@ic-center.ru

Подход к предотвращению инсайдерских утечек информации

Шатунов А.В.²⁹⁵, Ченцов В.А.²⁹⁶

В настоящей статье рассматривается возможность использования данных, находящихся в открытом доступе, такие как параметры системы мониторинга и анализа инцидентов информационной безопасности для борьбы с инсайдерскими утечками информации, и такие как категоризация инцидента на умышленный и не умышленный. Описывается проблематика современных решений борьбы с инсайдерами и методы анализа данных при помощи коммерческой разведки с использованием открытых данных, так же актуализация угроз инсайдерской утечки конфиденциальной информации.

Ключевые слова: анализ открытых данных, OSINT, конфиденциальная информация, информационная безопасность.

Введение

В настоящее время инсайдерская утечка информации является актуальной проблемой. Для полноценной защиты информации недостаточно простого внедрения средств защиты информации, так как любая настройка системы не совершенна, вследствие чего в системе появляется множество ложных срабатываний, при этом в огромном количестве событий, порожденных данной системой, порой крайне трудно выявить действительно важное событие. Кроме того, современные системы не всегда могут классифицировать инцидент по признаку: умышленно/не умышленно.

В настоящее время постоянно появляются новости о краже и утечке конфиденциальной информации различных компаний. По данным исследования компании «Стахановец» более 92,6 % компаний сталкивались с утечкой информации. Подобных утечек становится все больше с каждым годом, о чем свидетельствуют исследования, проведенные компанией InfoWatch [1], результаты которых представлены ниже (рис. 1).



Рис. 16. Число зарегистрированных утечек информации за период с 2006 по 2019 гг.

При этом злонамеренные действия инсайдеров являются одними из наиболее частых видов утечек конфиденциальной информации [2].

²⁹⁵ Шатунов Александр Владимирович, старший преподаватель кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, г. Москва, suovik@mail.ru.

²⁹⁶ Ченцов Владимир Андреевич, студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, г. Москва, chentsovvladimir@gmail.com.

Существует множество решений системы защиты информации (далее по тексту СЗИ), позволяющих обеспечить безопасность организации как от внешних угроз, так и от внутренних. Однако введение в эксплуатацию СЗИ является недостаточной мерой для обеспечения информационной безопасности, что обусловлено постоянным развитием и изменениями организации. Обеспечение безопасности системы предполагает создание препятствий для любого несанкционированного вмешательства в процессе ее функционирования, так же полный мониторинг этих событий. Следовательно, системы СЗИ должны быть настроены корректно и учитывать особенности компании [3].

Социальные сети являются неотъемлемой частью жизни в современном социуме и, как показывает статистика, ими пользуются большое количество людей, а значит это важная структура данных для анализа. По оценкам аналитического агентства Hoodsights, в 2019 году аудитория Глобальной информационной сети Internet насчитывает 4,39 миллиарда человек, что на 366 миллионов (9%) больше, чем в январе 2018 года. В социальных сетях в настоящее время зарегистрировано 3,48 миллиардов пользователей. По сравнению с данными на начало 2018 года данный показатель вырос на 288 миллионов (9%). Таким образом, около 80% пользователей Глобальной информационной сети Internet пользуются социальными сетями [4, 5].

В российском законодательстве имеется тонкая грань между мониторингом контента сотрудников организаций и нарушением их тайны переписки, телефонных переговоров, тайны личной жизни. Конституция РФ, УК РФ, Федеральный закон от 27 июля 2006 г. 152-ФЗ «О персональных данных», Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральный закон от 27 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» накладывают серьезные ограничения на мониторинг контента, нарушение которых может повлечь юридическую ответственность. В этой связи необходимо тщательно прорабатывать процесс мониторинга на соответствие законодательству Российской Федерации [6].

Современные DLP-системы, как самый распространенный способ борьбы с инсайдерскими утечками информации, умеют создавать профиль сотрудника, находят его социальные страницы, анализируют общение в интернете на предмет передачи коммерческой информации, но не сопоставляют одно с другим [7, 8].

СЗИ, установленные в компании, умеют работать только с трафиком, относящимся к компании и машинами, на которые распространяется доменная политика. Однако в данный перечень не входят смартфоны сотрудников, которые умеют анализировать далеко не все СЗИ несмотря на то, что через них также может быть реализована умышленная или не умышленная отправка персональных данных. Таким образом, необходимо анализировать не только конечные точки, представляющие собой персональные компьютеры (далее по тексту ПК), но и все информационное поле, которое относится к организации.

Изложенное обуславливает необходимость применения иных методов обеспечения защиты от инсайдерских утечек информации. Одним из новых подходов к решению указанной задачи является применение OSINT.

OSINT (Open Source INTelligence) – это набор инструментов коммерческой разведки, позволяющий искать, собирать и анализировать информацию из открытых источников [9, 10].

Ниже (рис. 2) представлен пример карты ресурсов для коммерческой разведки, данный пример не отображает всех возможностей OSINT framework, но уже позволяет многое узнать о человеке и компании.

Анализ открытых данных при помощи набора инструментов коммерческой разведки OSINT, способен помочь решить эти проблемы, объединив анализ событий внутри компании и ее информационное поле в открытых источниках в одно целое, тем самым улучшить безопасность компании и найти взаимосвязанные события, которые ранее не

удавалось связать. Система коммерческой разведки OSINT, как средство анализа данных, находящихся в открытом доступе и способна помочь администраторам безопасности в выявлении инсайдеров и предотвращении утечек коммерческой информации в связке с внутренним анализом и DLP-системой.

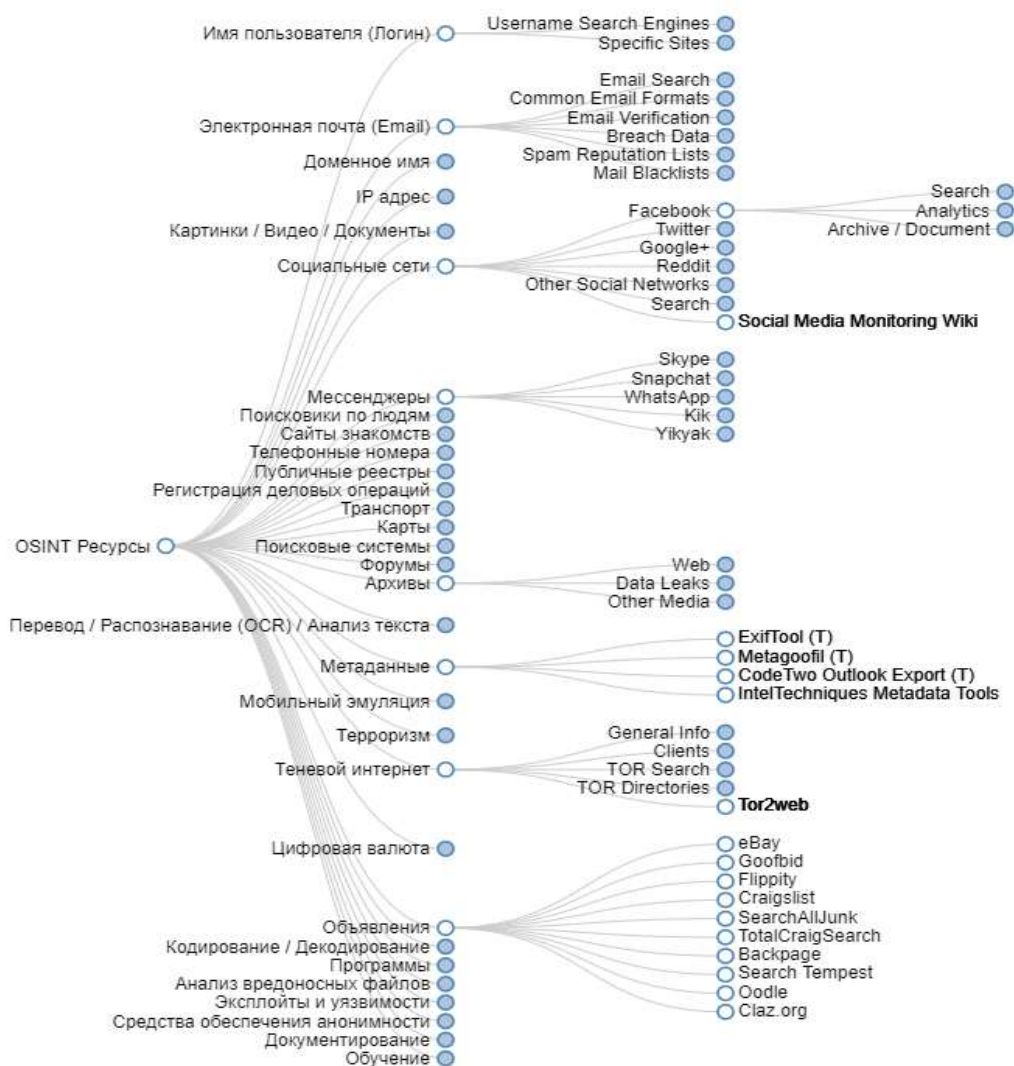


Рис. 17. Карта ресурсов для коммерческой разведки

Подобные наборы решений, как OSINT framework нацелены на сбор данных о конкурентах, однако эти же самые механизмы можно применять и для обеспечения информационной безопасности. Чем выше осведомлённость организации о данных, относящихся к ней, которые находятся в открытом доступе, тем проще защититься. Кроме этого, подобные решения позволяют собирать информацию не только на организацию в целом, но и на ее сотрудников. В частности, таким образом, подобные решения могут помочь организациям:

- выявлять аномальные поведения сотрудников,
- создавать психологический портрет сотрудников,
- классифицировать инциденты на умышленные / не умышленные,
- осуществлять проверку контрагентов и сотрудников, как новых, так и уже работающих,

- создавать доказательную базу для качественного расследования инцидентов информационной безопасности,
- оперативно реагировать на инциденты информационной безопасности, составить портрет собственной компании по открытым данным.

При этом OSITN позволяет действовать в рамках законодательства.

Период работы сотрудника в компании можно разделить на 3 основных этапа: устройство на работу, период работы, увольнение. Полный цикл занимает у сотрудника в среднем от 3 до 5 лет и за последние годы сокращается, об этом свидетельствуют множество открытых исследований. Однако есть еще один этап, который можно назвать «после увольнения». К сожалению, сотрудники уходят из компаний по разным обстоятельствам и не всегда по обоюдному согласию. Указанный фактор свидетельствует о том, что действия человека после увольнения также необходимо анализировать, особенно, если речь идет о сотрудниках, которые имели дело с большим количеством конфиденциальных данных, не зависимо от того, было подписано Соглашение о неразглашении или нет.

При устройстве на работу нового сотрудника компания оперирует только той информацией, которую передает сам сотрудник. Такой подход не дает полной картины о человеке, который устраивается на работу, и покрывает лишь профессиональные навыки, опыт и образование. Дальнейшее общение с сотрудником на этапе собеседования позволяет определить дополнительные характеристики, однако человек может быть подготовлен к конкретным вопросам, и реального портрета соискателя определить, скорее все не получится несмотря на то, что специалисты подбора кадров применяют различные технологии для выявления ключевых характеристик [11].

Собеседование и устройство на работу, это осознанное решение, к которому человек так или иначе готовится, составляя резюме с конкретными фактами о себе. Кроме того, чтобы показать свои сильные стороны кандидат продумывает ответы на вопросы, которые, скорее всего, будут заданы на собеседовании. Как уже было сказано ранее, такая подготовка не всегда отражает реальные факты о человеке. Однако большую часть времени, человек не задумывается об этом и ведет себя привычно и более раскрепощено. Изложенное касается поведения в обществе, а также ведения свой личной страницы в Глобальной информационной сети Internet, общения на форумах, и многих других фактором.

Вместе с тем, на данном этапе, имея согласие на обработку персональных данных, можно многое узнать о человеке: наличие вредных привычек, кредитная надежность, социальный нигилизм, активность в социальных сетях, увлечения и хобби, аудитория влияния, семейное положение, марка телефона, упоминания в СМИ, наличие налоговых задолженностей, судимость. Однако ручная обработка и анализ этих данных занимает большое количество времени. Автоматизация данного процесса позволит существенно сократить время анализа и выявить закономерности и связи, которые трудно выявить человеку, а также предоставит систематизированный отчет. Подобный систематизированный подход позволяет минимизировать риски, сопутствующие найму нового сотрудника и оценить сотрудника в целом [12].

Каждый день сотрудники выполняют множество действий: посещают огромное количество веб-сайтов, производят миллионы подключений, отправляют письма, общаются в мессенджерах, скачивают сотни файлов и многие другие. Каждое из подобных действий несет в себе определенные риски для организации, от заражения ПК сотрудника до утечки тендерной информации во время перерыва. Большинство из этих рисков можно закрыть современными средствами защиты, однако лишь ограниченное количество средств защиты информации способны определить мотив данного действия.

Решение о причине инцидента, к которым относятся умышленные действия, заблуждение, халатность или ошибка, каждая организация принимает сама. Однако знание причин инцидентов имеет высокое значение. Проведение анализа поведения сотрудника для определения психологического портрета может помочь ответить на этот вопрос не

только при расследовании инцидента, но и на этапе, когда этот инцидент еще не состоялся. Если компания узнает, что ее сотрудник часто обсуждает организацию в сети Internet или среди его ближнего круга множество сотрудников конкурирующих компаний, к сотруднику стоит проявить особую бдительность. Миллионы транзакций, проходящих через СЗИ, генерируют множество событий в том числе и ошибочных, когда компания знает, что события конкретного пользователя необходимо более тщательно проанализировать, риск потерять данный инцидент в общем количестве событий сводится к минимуму.

Таблица 3

Критерии оценки сотрудника

Показатель	Описание	Критерии	Оценка	Коэффициент
Тестовая рассылка	Проведение тестовой фишинговой рассылки по почте	Действия, произведённые сотрудником	0-10	0.6
Общение контрагентами	Общается ли сотрудник с представителями контрагентов в рамках работы	Да/Нет Частота общения	0-5	0.5
Общение конкурентами	Общается ли сотрудник с представителями конкурирующих организаций в рамках работы	Да/Нет Частота общения	0-5	0.9
Обновление резюме	Обновление резюме на сайтах для поиска работы	Да/Нет Временные рамки (на неделю, этот месяц, этот год)	0-3	0.4
Чрезмерное использование социальных сетей во время работы	Анализ посещения сайтов с конкретизацией сайтов	По времени	0-5	0.2
Аномальная активность сетевого соединения	Выявление нехарактерных действий/подключений для сотрудника	По протоколам По количеству	0-10	0.7
Работа коммерческой тайной	Анализ доступных сотруднику данных, относящихся к коммерческой тайне	Степень данных	0-5	0.9
Права доступа	Определение прав доступа в ИС	Ролевая модель	0-5	0.7
Стаж работы	Анализ стажа работы	По времени	0-5	0.3
Упоминание компании в соц. сетях	Выявление упоминаний компании	Да/Нет Частота	0-4	0.7
Работа удаленно	Имеет ли работник возможность работать удаленно	Да/Нет	0-1	0.2
Время работы	Отклонение от норм	По времени	0-3	0.2
Сумма сделок	Средняя сумма сделок, на которые влияет сотрудник	Денежная оценка	0-10	0.7
И т.п.				

Для систематического анализа необходимо составить определенный профиль сотрудника, в котором будут зафиксированы различные показатели и события / инциденты, связанные с ним, краткий перечень которых представлен выше (табл. 1).

В данной таблице приведены показатели, оценки, коэффициенты, которые каждая компания определяет сама, так как у каждой компании своя специфика, набор решений, архитектура и разное отношение к определенным рискам. Кроме того, как видно из вышеуказанной таблицы, количество таких критериев бесчисленное множество, и каждый

из них относятся к разным категориям данных, от сетевой активности до должностных инструкций.

Информационная безопасность организации, в целом, состоит из двух важных частей: технической и организационно-правовой. Если для анализа технической части существует множество механизмов анализа, то для организационно-правовой, решений позволяющих автоматизировано анализировать данные почти нет. Перевод всей информации в цифровой вид и механизмы анализа такой информации позволяют убрать существенный барьер между двумя составляющими информационной безопасности и рассматривать их как одно целое.

Увольнение – важный этап, в связи с тем, что не зависимо от причины ухода (по собственному желанию / вследствие инцидента) необходимо удостовериться, что сотрудник не нанес ущерб компании и его можно отпустить. Изложенное касается, как имущества (инвентаризация оборудования, выданного сотруднику), так и действий, не проанализированных во время работы сотрудника в компании и инцидентов, если такие были. Кроме того, если сотрудника увольняют вследствие инцидента, связанного с нарушением информационной безопасности, компании необходимо иметь базу доказательств, подтверждающих, что действия конкретного сотрудника повлекли за собой определенные последствия. Следовательно, необходимо систематизировать данные о сотруднике и обеспечить их хранение до момента, пока они станут не действительны. В связи с тем, что некоторые события могут выявиться уже после увольнения, этап после увольнения выделен отдельно от остальных.

Как уже отмечено ранее, иногда инциденты выявляются уже после увольнения сотрудника из компании, и если хранение информации о сотруднике не обеспечивается должным образом, то после его увольнения доказать его причастность будет крайне сложно. Кроме того, бывший сотрудник может нанести ущерб репутации компании или раскрыть коммерческую тайну на новой работе. В целях предотвращения указанного необходимо четко прописывать обязательства бывшего сотрудника перед компанией после увольнения и продолжить анализ данных сотрудника в рамках законодательства РФ.

При предотвращении инсайдерских утечек информации и обеспечении информационной безопасности в целом, следует также анализировать данные, находящиеся в открытом доступе как на компанию, так и на сотрудников компании. Данный анализ позволит более точно выявить инсайдеров, упростит работу администраторам безопасности, обеспечит более быстрое реагирование на инциденты и при возможности сформирует доказательную базу, и самое главное повысит уровень безопасности в компании. Необходимо доработать законодательство, регулирующее обработку данных, находящихся в открытом доступе, так как текущая ситуация ограничивает, как механизмы контроля, так и права граждан на эти данные.

Литература

1. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года. Ежегодный отчет // Аналитический центр «InfoWatch» – 2019. С. 9. Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1 (Дата обращения – 10.11.2019 г.).

2. Шатунов А.В. Актуальность исследований в области предотвращения утечки конфиденциальной информации в связи со злонамеренными действиями инсайдеров. Сборник трудов VI Всероссийской научно-технической конференции «Безопасные информационные технологии» – М.: МГТУ им. Н.Э. Баумана, НУК «Информатика и системы управления», 2015. С. 146-150.

3. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности – 2013, выпуск № 1(1). С. 17-27.

4. Басараб М.А., Иванов И.П., Колесников А.В., Матвеев В.А. Обнаружение противоправной деятельности в киберпространстве на основе анализа социальных сетей: алгоритмы, методы и средства (обзор)//Вопросы кибербезопасности. 2016. № 4 (17). С. 11-19.
5. Дорофеев А.В. Прикладные вопросы анализа социальных сетей. В сборнике: Безопасные информационные технологии (БИТ-2016). Сборник трудов Седьмой Всероссийской научно-технической конференции. Под редакцией В.А. Матвеева. 2016. С. 153-155.
6. Эткина А., Астахов А. Правовые и неправовые аспекты мониторинга контента: американский опыт // Директор по безопасности – 2019, выпуск № 8. С. 10-13.
7. Барабанов А.В., Гришин М.И., Марков А.С., Цирлов В.Л. Формирование требований по безопасности информации к DLP-системам // Вопросы радиоэлектроники. 2013. Т. 3. № 2. С. 67-76.
8. Petrenko S.A. Innovative methods for detecting anomalies. In: The 2018 Symposium on Cybersecurity of the Digital Economy (CDE'18) Вторая международная научно-техническая конференция. 2018. С. 90-99.
9. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети интернет//Мониторинг правоприменения. 2016. № 1 (18). С. 41-53.
10. Dorofeev A.V., Markov A.S., Tsirlov V.L. Social Media in Identifying Threats to Ensure Safe Life in a Modern City, Communications in Computer and Information Science, 2016, vol. 674, pp. 441-449. DOI: 10.1007/978-3-319-49700-6_44.
11. Бондарев В.В. Психологические аспекты информационной безопасности. Сборник трудов IX Всероссийской научно-технической конференции «Безопасные информационные технологии» (БИТ-2018) – М.: МГТУ им. Н.Э. Баумана, НУК «Информатика и системы управления», 2018. С. 28-31.
12. Оладько В. С. Программный комплекс для определения закона распределения атак злоумышленников // Вопросы кибербезопасности. 2015. № 1 (9). С. 55-59.

Научный руководитель: Медведев Николай Викторович, кандидат технических наук, доцент, доцент кафедры «Информационная безопасность», medvedevnick54@yandex.ru.

An approach to preventing insider leaks **Shatunov A.V.²⁹⁷, Chentsov V.A.²⁹⁸**

This article discusses the possibility of using publicly available data, such as the parameters of the information security incident monitoring and analysis system to combat insider leaks, and such as categorizing the incident into intentional and non-intentional. Describes the problems of modern solutions to combat insiders and methods of data analysis with the help of commercial intelligence using open data, as well as the actualization of threats of insider leakage of confidential information.

Keywords: *analysis of open data, OSINT, confidential information, information security.*

²⁹⁷ Alexander Shatunov, senior lecturer of the Department "Information security", MSTU. N.E. Bauman, Moscow, suovik@mail.ru.

²⁹⁸ Vladimir Chentsov, student of the Department "Information security", MSTU. N.E. Bauman, Moscow, chentsovvladimir@gmail.com.

Исследование алгоритма Isolation Forest при бинарной классификации сетевых аномалий

Шелухин О.И.²⁹⁹, Полковников М.В.³⁰⁰

Аннотация

Проведен сравнительный анализ качественных характеристик алгоритмов iForest и RF в задачах бинарной классификации аномалий сетевого трафика. Для оценки эффективности анализируемых моделей используются метрики precision, recall, F-score, ROC-кривые, AUC-ROC. В качестве набора данных использовалась модификация набора NSL-KDD. Для проведения сравнительного анализа алгоритмов iForest и RF введена в рассмотрение евклидова метрика минимизирующая ошибки классификации 1-го и 2-го рода. Показано наличие оптимума по выбранному критерию у алгоритма iForest и найдена величина порогового уровня минимизирующая вероятности 1-го и 2-го рода. В качестве критерия сравнения алгоритмов iForest и RF использована скорость обучения и тестирования. Показано, что по скорости обучения и тестирования алгоритм iForest превосходит RF, однако незначительно уступает ему по качеству бинарной классификации.

Ключевые слова: машинное обучение, случайный лес, аномалия, darpa, nsl-kdd, атрибуты, критерии

Введение

Аномалии сетевого трафика — это шаблоны данных, имеющих характеристики отличные от нормального трафика. Обнаружение аномалий имеет важное значение и часто является критически важным. Так, например, необычный шаблон сетевого трафика может означать несанкционированный доступ к ресурсам сети.

Большинство существующих подходов к обнаружению аномалий трафика основаны на моделях и предполагают построения профиля нормального функционирования (ПНФ), а затем идентифицируют в качестве аномалий те, которые ему не соответствуют. Одним из наиболее перспективных методов обнаружения аномалий являются методы, основанные на машинном обучении [8]. Широкое распространение в задачах классификации получили следующие алгоритмы классификации: метод k-ближайших соседей (k-Nearest Neighbors, k-NN) [2]; множественная логистическая регрессия (Logistic Regression) [3]; мультиномиальный Наивный Баис (Multinomial Naive Bayes, NB) [5]; метод опорных векторов (Support Vector Machines, SVM) [6]; дерево решений (Decision Tree Classifier, DTC) [7]; случайный лес (Random Forest) [11].

В отличие от указанных работ в [10] предложены алгоритмы основанные на выделении аномалии, а не на ПНФ. Примером таких алгоритмов является алгоритм машинного обучения Изолирующий Лес (iForest) [1].

Алгоритм классификации iForest

Алгоритм iForest впервые описанный в [1], является модификацией алгоритма Random Forest (RF), для решения задач обнаружения аномалий и выбросов. Алгоритм iForest, подобно Random Forest, строит ансамбль деревьев решений, названных Деревьями изоляции (iTree). Его главное отличие состоит в том, что iForest не учитывает метку класса, считая все экземпляры нормальными. Суть алгоритма обнаружения сводится к тому, что по

²⁹⁹ Шелухин Олег Иванович, д.т.н., профессор, МТУСИ, Москва, sheluhin@mail.ru

³⁰⁰ Полковников Михаил Вадимович, магистрант, МТУСИ, Москва, mnxamoto@mail.ru

сравнению с нормальными, аномальные экземпляры в подавляющем большинстве быстро изолируются, т.е. имеют короткие длины пути в iTree (имеют более близкое расположение к корню дерева). В связи с этим исследуемому экземпляру присваивается оценка аномалии в зависимости от длины пути прохождения по iTree. По сравнению с другими алгоритмами в iForest большая часть дерева изолирует нормальные точки, которые не требуются для обнаружения аномалий так что эту часть дерева нет необходимости строить. В результате сокращается размер деревьев и не используется часть набора данных.

Результаты бинарной классификации алгоритма iForest

Для исследования в качестве набора данных использовался набор данных NSL-KDD [4].

На рисунке 1 приведены гистограммы оценок аномалии и нормального трафика, полученные путём подсчёта количества оценок для каждого интервала. Гистограммы иллюстрируют возможность применения алгоритма iForest для обнаружения аномалий трафика методом бинарной классификации.

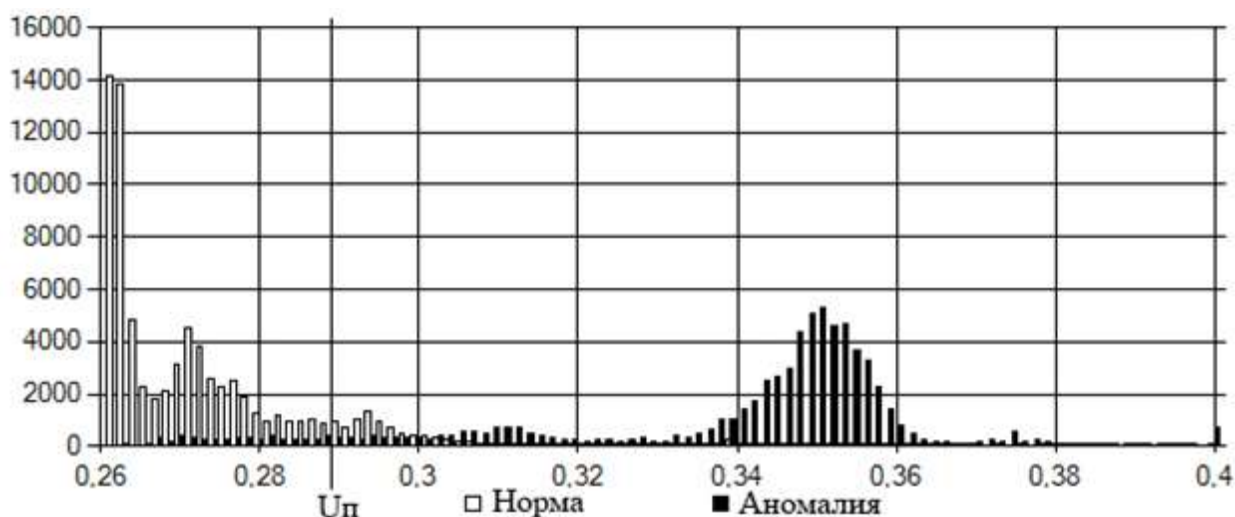
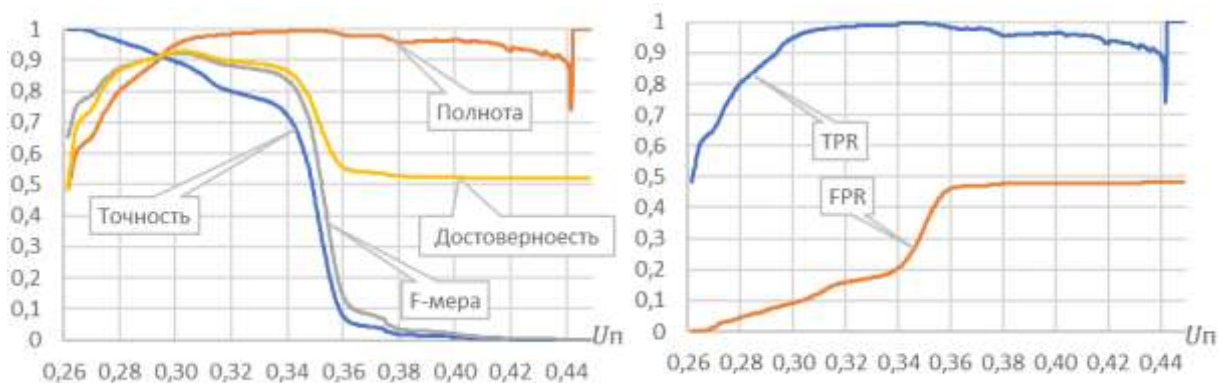


Рис.1. Гистограмма оценки аномалии

Пороговое значение $\llbracket U \rrbracket_{\text{п}}$ на рисунке 1 определяется вероятностями ошибок первого и второго рода. На рисунке 2 представлены зависимости основных метрик, характеризующих качество бинарной классификации аномалий от величины порогового уровня алгоритма iForest.



а)

б)

Рис.2. Влияние порога на качество обнаружения аномалий

Как видно из представленных на рисунке 2 зависимостей при изменении $U_{\text{п}}$ изменяется и соотношение ошибок первого и второго рода, определяемых параметрами:

$\text{FPR} = \text{FP} / (\text{FP} + \text{TN})$ - False Positive Rate – вероятность ошибки 1-го рода.

$\text{TPR} = (\text{TP} + \text{FN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN})$ - True Positive Rate – вероятность истинно положительных решений.

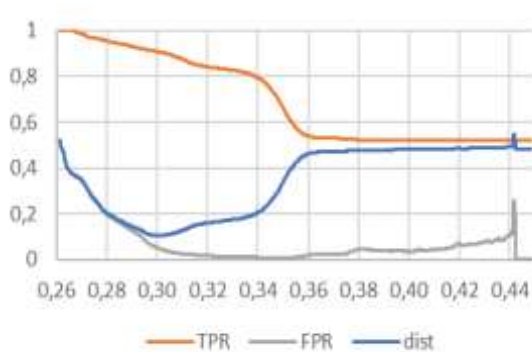
Для минимизации ошибок первого и второго рода для j -го атрибута введем в рассмотрение метрику в виде евклидова расстояния

$$\text{dist}(m_{(i,j)}^*) = \sqrt{((1 - \text{TPR}_{(i,j)}^*)^2 + (0 - \text{FPR}_{(i,j)}^*)^2)}, \quad (1)$$

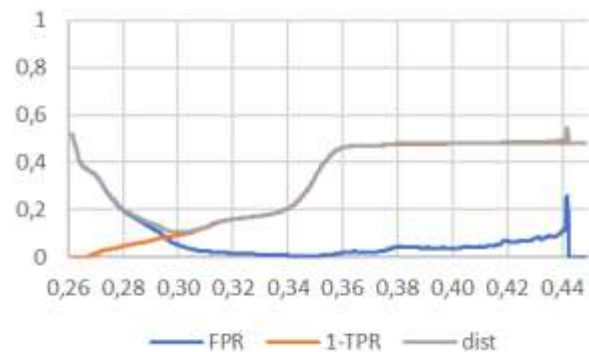
$i \in \{\text{anomaly}, \text{normal}\}; \text{anomaly} \in \{\text{dos}, \text{u2r}, \text{r2l}, \text{probe}\}, j \in J.$

Будем определять величину $\llbracket U \rrbracket_{\text{п}} (\text{TPR}_{(i,j)}^*; \text{TPR}_{(i,j)}^*)$ из условия $\min \sum_j \sum_i \text{dist}(m_{(i,j)}^*)$.

Представленные на рисунке 3 зависимости метрики $\text{dist}(\cdot)$ от величины порогового уровня, показывают наличие оптимума по выбранному критерию. Из представленных зависимостей видно, что минимальное значение $1 - \text{TPR} = \text{FPR} = 0,1$ достигаются при значении порога $U_{\text{п}} = 0,3$.



а)



б)

Рис.3. Влияние порога на а) TPR, FPR и dist; б) 1-TPR, FPR и dist

Проведенные эксперименты по оценке влияния количества деревьев алгоритма iTree в ансамбле на эффективность классификации (рисунок 4) показали, что при найденном значении $\text{dist} = 0.1$ количество iTree можно ограничить 40.

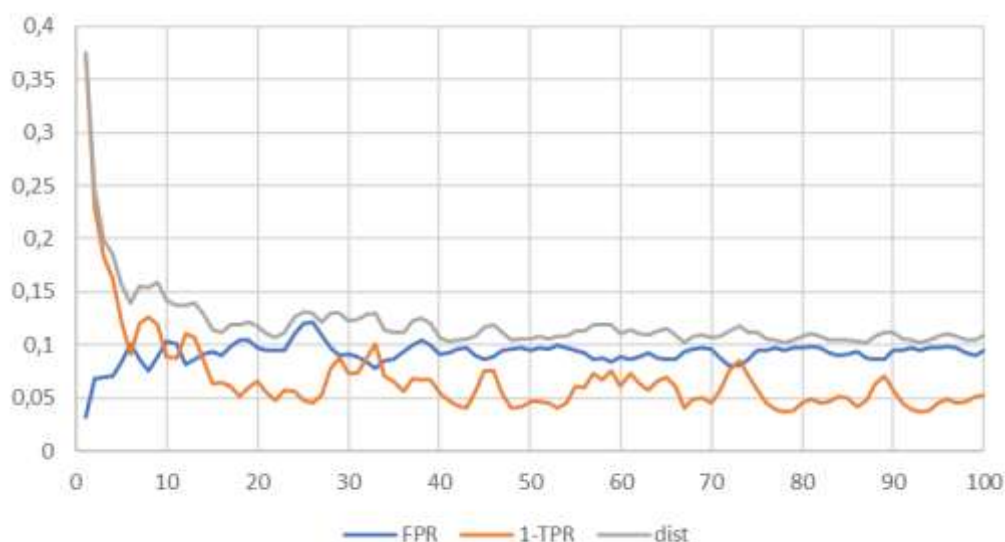


Рис.4. Влияние количества деревьев на 1-TPR, FPR и dist

Результаты бинарной классификации Random Forest

Для сравнительного анализа алгоритмов iForest и RF было исследовано влияние ключевых параметров алгоритма RF [11] на качество классификации при использовании метрики (1). Найдено, что в отличие от iForest у алгоритма RF зависимости качества классификации от порогового урона не имеют явно выраженного оптимума, а искомая метрика принимает минимальное значение $\text{dist} = 0,04$.

Поскольку метрика dist у обоих алгоритмов принимает минимальное значение при одинаковом количестве деревьев, для сравнения был проведен анализ времени обучения и тестирования. Зависимости, представленные на рисунке 5 показывают, что при одинаковом количестве деревьев быстродействие алгоритма iForest значительно превосходит алгоритм RF.

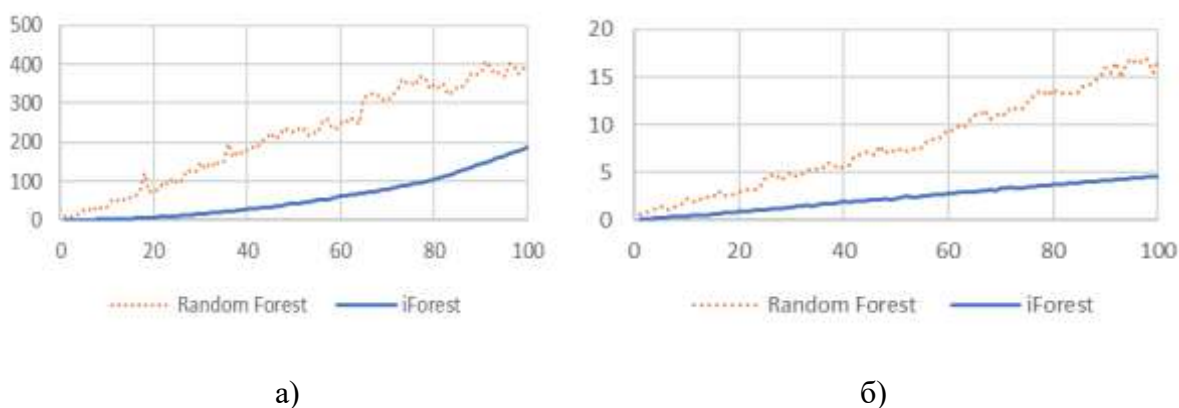


Рис.5. Влияние количества деревьев на время: а) обучения; б) тестирования

Так при фиксированном количестве деревьев равном 40 по длительности времени обучения RF уступает алгоритму iForest в 8 раз, а по времени тестирования в 3 раза.

Выводы

Введена в рассмотрение евклидова метрика минимизирующая ошибки классификации FPR (1-го) и 1-TPR (2-го рода).

Показано наличие у алгоритма iForest оптимума по выбранному критерию качества и найдена величина порогового уровня минимизирующая вероятности 1-го и 2-го рода. Найдено, что в отличие от iForest алгоритм RF не имеет явно выраженного оптимума. В качестве ключевых параметров рассматривались пороговый уровень, количество деревьев, максимальная глубина, количество атрибутов, количество деревьев, количество наблюдений на лист и размер тренировочного поднабора.

Поскольку введенная в рассмотрение евклидова метрика у обоих алгоритмов принимает минимальное значение при одинаковом количестве деревьев, в качестве критерия сравнения была использована длительность времени обучения и тестирования. По итогам сравнения выявлено, что по скорости обучения и тестирования алгоритм iForest значительно превосходит RF, однако незначительно уступает ему по качеству бинарной классификации.

Литература

1. Liu F. T., Ting K. M., Zhou Z-H. Isolation forest. Proceedings of the Eighth IEEE International Conference on Data Mining. Los Alamitos CA USA : IEEE., 2008, pp. 413 – 422
2. Ибраева З.Г. Особенности разработки knn-алгоритмов классификации данных на графических процессорах// Студенческая наука для развития информационного общества сборник материалов VI Всероссийской научно-технической конференции. 2017. С. 217-219.
3. Шарашова Е.Е., Холматова К.К., Горбатова М.А., Гржибовский А.М. Применение множественного логистического регрессионного анализа в здравоохранении с использованием пакета статистических программ SPSS//Наука и здравоохранение. 2017. № 4. С. 5-26.
4. Protic D.D. Review of kdd cup '99, nsl-kdd and kyoto 2006+ datasets// Vojnotehnicki glasnik. 2018. T. 66. № 3. С. 580-596.
5. Lagutina K., Larionov V., Petryakov V., Lagutina N., Paramonov I., Shchitov I. Sentiment classification into three classes applying multinomial bayes algorithm, n-grams, and thesaurus//Conference of Open Innovation Association, FRUCT. 2019. № 24. С. 214-219.
6. Шелухин О.И., Ерохин С.Д., Ванюшина А.В. Под редакцией Шелухина О.И. Классификация IP –трафика методами машинного обучения. М., Горячая-линия – Телеком, 2018, 284 с.
7. Parvin H., Mirnabibaboli M., Alinejad-Rokny H. Proposing a classifier ensemble framework based on classifier selection and decision tree// Engineering Applications of Artificial Intelligence. 2015. T. 37. С. 34-42.
8. Шелухин О.И., Барков В.В., Полковников М.В. Классификация зашифрованного трафика мобильных приложений методом машинного обучения//Вопросы кибербезопасности. 2018. № 4 (28). С. 21-28.
9. Шелухин О.И., Барков В.В., Полковников М.В. Сравнительный анализ алгоритмов оценки количества и структуры атрибутов в задачах классификации мобильных приложений// Научные технологии в космических исследованиях Земли. 2019. Т. 11. № 2. С. 90-100.
10. Sun, Li & Versteeg, Steven & Boztas, Serdar & Rao, Asha. Detecting Anomalous User Behavior Using an Extended Isolation Forest Algorithm: An Enterprise Case Study// arXiv e-prints. 2016.
11. Шелухин О.И., Полковников М.В. Повышение эффективности классификации сетевого трафика мобильных устройств с использованием алгоритма Random Forest// Технологии информационного общества Материалы XIII Международной отраслевой научно-технической конференции. 2019. С. 415-418.

Investigation of the Isolation Forest binary classification algorithm for detecting network traffic deviations

Sheluhin O.I., Polkovnikov M.V.

Abstract

The article provides a comparative analysis of the qualitative characteristics of the iForest and RF algorithms in the problems of binary classification of traffic anomalies. To assess the effectiveness of the constructed models, the common metrics precision, recall, F-score, ROC-curves, AUC-ROC are used. As a data set, a modification of the NSL-KDD set, often used for testing and evaluating the quality of intrusion detection systems, was used. To conduct a comparative analysis of the classification algorithms iForest and RF, a Euclidean metric minimizing classification errors of the 1st and 2nd kind was introduced. The presence of an optimum according to the selected criterion for the iForest algorithm is shown and a threshold level value is found that minimizes the probabilities of the 1st and 2nd kind. Since the Euclidean metric introduced by both algorithms takes the minimum value with the same number of trees, the duration of the training and testing time was used as a comparison criterion. According to the results of the comparison, it was revealed that the iForest algorithm is superior to RF in terms of training and testing speed, but slightly inferior to it in the quality of the binary classification of anomalies.

Keywords: machine learning, random forest, anomaly, darpa, nsl-kdd, attributes, criteria

References:

1. Liu F. T., Ting K. M., Zhou Z-H. Isolation forest. Proceedings of the Eighth IEEE International Conference on Data Mining. Los Alamitos CA USA : IEEE., 2008, pp. 413 – 422
2. Ibrayeva Z.G. Osobennosti razrabotki knn-algoritmov klassifikatsii dannykh na graficheskikh protsessorakh// Studencheskaya nauka dlya razvitiya informatsionnogo obshchestva sbornik materialov VI Vserossiyskoy nauchno-tekhnicheskoy konferentsii. [Features of the development of knn-algorithms for data classification on graphics processors // Student science for the development of the information society, collection of materials of the VI All-Russian Scientific and Technical Conference.] 2017. pp. 217-219.
3. Sharashova Ye.Ye., Kholmatova K.K., Gorbatova M.A., Grzhibovskiy A.M. Primeneniye mnozhestvennogo logisticheskogo regressionnogo analiza v zdravookhraneni s ispol'zovaniyem paketa statisticheskikh programm SPSS//Nauka i zdravookhraneniye. [The use of multiple logistic regression analysis in health care using the statistical software package SPSS // Science and Health Care.] 2017. № 4. pp. 5-26.
4. Protic D.D. Review of kdd cup '99, nsl-kdd and kyoto 2006+ datasets// Vojnotehnicki glasnik. 2018. T. 66. № 3. C. 580-596.
5. Lagutina K., Larionov V., Petryakov V., Lagutina N., Paramonov I., Shchitov I. Sentiment classification into three classes applying multinomial bayes algorithm, n-grams, and thesaurus//Conference of Open Innovation Association, FRUCT. 2019. № 24. pp. 214-219.
6. Sheluhin O.I., Yerokhin S.D., Vanyushina A.V. Klassifikatsiya IP-trafika metodami mashinnogo obucheniya. Goryachaya liniya – telekom [Classification of IP-traffic methods of machine learning. Hotline - Telecom], 276 p., 2018
7. Parvin H., Mirnabibaboli M., Alinejad-Rokny H. Proposing a classifier ensemble framework based on classifier selection and decision tree// Engineering Applications of Artificial Intelligence. 2015. Vol. 37. pp. 34-42.
8. Sheluhin O.I., Barkov V.V., Polkovnikov M.V. Klassifikatsiya zashifrovannogo trafika mobil'nykh prilozheniy metodom mashinnogo obucheniya//Voprosy kiberbezopasnosti. [Classification of encrypted mobile application traffic using machine learning // Cybersecurity issues.] 2018. № 4 (28). pp. 21-28.
9. Sheluhin O.I., Barkov V.V., Polkovnikov M.V. Sravnitel'nyy analiz algoritmov otsenki kolichestva i struktury atributov v zadachakh klassifikatsii mobil'nykh prilozheniy// Naukoyemkiye tekhnologii v kosmicheskikh issledovaniyakh Zemli. [Comparative analysis of algorithms for estimating

the number and structure of attributes in the tasks of mobile application classification // Science-intensive technologies in Earth space research.] 2019. T. 11. № 2. pp. 90-100.

10. Sun, Li & Versteeg, Steven & Boztas, Serdar & Rao, Asha. Detecting Anomalous User Behavior Using an Extended Isolation Forest Algorithm: An Enterprise Case Study//arXiv e-prints. 2016.

11. Sheluhin O.I., Polkovnikov M.V. Povysheniye effektivnosti klassifikatsii setevogo trafika mobil'nykh ustroystv s ispol'zovaniyem algoritma Random Forest// Tekhnologii informatsionnogo obshchestva Materialy XIII Mezhdunarodnoy otraslevoy nauchno-tekhnicheskoy konferentsii. [Improving the classification efficiency of network traffic of mobile devices using the Random Forest algorithm // Technologies of the Information Society Materials of the XIII International Industrial Scientific and Technical Conference.] 2019. pp. 415-418.

Обнаружение дрейфа концепта с использованием статистики Фишера-Пейджа-Хинкли при потоковой классификации трафика мобильных приложений

Шелухин О.И.³⁰¹, Секретарев С.А.³⁰²

Аннотация. Важным аспектом классификации приложений в условиях априорной неопределенности является работа алгоритмов в потоковом режиме, при непрерывном поступлении данных измерений. Отличительной особенностью классификации данных в потоковом режиме является смещение (дрейф) концепта. Смещение концепта происходит, когда исследуемое явление, о котором были собраны данные, изменяется с течением времени. В условиях нестационарных потоков данных классификация мобильных приложений должна осуществляться в паре с детектором смены концепта (ДСК). В работе предложен двухступенчатый алгоритм обнаружения смены концепта в наблюдаемом потоке данных, базирующийся на статистических характеристиках атрибутов, анализируемых с помощью двух скользящих окон, контролирующих изменение текущих статистических характеристик атрибутов мобильных приложений. На первом этапе применяется решающая статистика в соответствии с критерием Фишера. На втором этапе применяется тест Пейджа – Хинкли. В результате проведенных экспериментов с помощью искусственного набора данных были получены зависимости, позволяющие оценить работоспособность предложенного двухэтапного алгоритма обнаружения дрейфа концепта. Показано, что ДСК позволяет снизить вероятность ошибки классификации при каждой смене концепта примерно на 5%.

Ключевые слова: машинное обучение, *k nearest neighbors*, изменение концепта, скользящие окна, критерий Фишера, тест Пейджа-Хинкли.

Введение

Современные алгоритмы классификации трафика мобильных приложений требуется адаптировать для работы в потоковом режиме из-за ресурсных ограничений по используемой памяти и быстродействию. Важными особенностями задач классификации потоков данных являются их большая длина и смещение (дрейф) концепта. Смещение концепта является общим свойством потоков данных, которое присутствует в случае изменения исследуемого трафика, например, при появлении новых приложений, при изменении интенсивности существующих атрибутов или при появлении в сети новых мобильных устройств.

Изменение свойств потока может приводить к утрате обученной моделью своей актуальности и падению качества выдаваемых прогнозов. Известно много методов для борьбы с дрейфом концепта [1]. Как правило для обнаружения дрейфа анализируются показатели качества классификации, которые невозможно получить, не имея информации об истинных метках обрабатываемых объектов [1,2, ,3]. В работе анализируется возможность обнаружения дрейфа концепта без использования данной информации с помощью специального детектора смены концепта (ДСК).

ДСК на основе скользящих окон и статистики Фишера-Пейджа-Хинкли

Пусть имеется множество $Y = \{y_1; y_2; \dots; y_N\}$ обрабатываемых объектов. Каждый $y_t = \{y_{t,1}; y_{t,2}; \dots; y_{t,K}\}$ является множеством признаков мобильных приложений, полученного в момент времени t , где K – количество признаков. Пусть имеются два

³⁰¹ Шелухин Олег Иванович, доктор технических наук, профессор, МТУСИ, Москва, sheluhin@mail.ru

³⁰² Секретарев Сергей Александрович, магистрант, МТУСИ, Москва, svoboda.vezde@gmail.com

смежных окна $W_1 = \{y_{t-N_1-N_2+1}; y_{t-N_1-N_2+2}; \dots; y_{t-N_2}\}$ и $W_2 = \{y_{t-N_2+1}; y_{t-N_2+2}; \dots; y_t\}$, где N_1 и N_2 – размеры первого и второго окон соответственно ($N_2 \ll N_1$). Первое окно характеризует статистику атрибутов приложения в «прошлом», в то время как второе – характеризует статистику приложения «в настоящем».

Статистический анализ атрибутов анализируемых приложений показал, что наиболее важные из них, связанные с изменением объема трафика, имеют экспоненциальный вид [4]. В этих условиях для обнаружения аномальных изменений анализируемых атрибутов может быть использован алгоритм обнаружения смещения концепта наблюдаемого потока данных на базе использования критерия Фишера для выбросов средних значений

$$R(t) = \frac{M_2(t)}{M_1(t)}, \quad (1)$$

где M_1 и M_2 – выборочные средние значения признаков наблюдаемых мобильных приложений, входящих в первое и второе окно соответственно:

$$M_1(t) = \frac{1}{N_1 K} \sum_{i=t-N_1-N_2+1}^{t-N_2} \sum_{j=1}^K y_{i,j} \quad \text{и} \quad (2)$$

$$M_2(t) = \frac{1}{N_2 K} \sum_{i=t-N_2+1}^t \sum_{j=1}^K y_{i,j}. \quad (3)$$

Если $R(t) > \lambda_1$, то делается вывод о том, что в потоке могли произойти изменения.

Используя соотношение (1), введем в рассмотрение среднее значение для решающей статистики на интервале наблюдения $[0; T]$

$$\overline{R(T)} = \frac{1}{T+1} \sum_{t=0}^T R(t). \quad (4)$$

Тогда накопленная разница между текущим значением решающей статистики $R(t)$ и ее средним значением $\overline{R(T)}$ может быть записана как

$$m(T) = \sum_{t=0}^T (R(t) - \overline{R(T)} - \delta), \quad (5)$$

где δ соответствует величине допустимого изменения. Пусть также имеется функция $M(T) = \min(m(t), t = 0, \dots, T)$, равная минимальному значению накопленной разности $m(t)$ на промежутке $[0; T]$.

Введем в рассмотрение решающую статистику Пейджа-Хинкли [5]

$$PH(T) = m(T) - M(T) > \lambda_2. \quad (6)$$

Если $PH(T) > \lambda_2$, то делается вывод о том, что произошел дрейф концепции. Увеличение порогового уровня λ_2 приводит к уменьшению количества ложных срабатываний, однако может приводить либо к пропускам дрейфа, либо к задержке в обнаружении. Управляя этим параметром, можно найти компромисс между вероятностями ошибок обнаружения 1-го и 2-го рода.

Будем считать, что совокупность алгоритмов (1), (2), (3) и (6) и формируют ДСК Фишера-Пейджа-Хинкли.

Оценка эффективности ДСК

Для оценки эффективности рассмотренного ДСК был проведен эксперимент, заключающийся в классификации специально подготовленного набора данных разработанным для данных целей классификатором, реализующим алгоритм K Nearest Neighbors [6, 7].

В качестве множества экспериментальных данных был использован набор данных «CIRCLES» [2, 8,

9]. Каждый элемент использованного набора данных характеризуется двумя признаками – координатами точки в двумерном пространстве. Класс элемента характеризует, находится ли точка внутри круга или снаружи. Смена концепта происходит из-за изменения радиуса круга. В используемом в эксперименте наборе данных концепт меняется два раза – сначала происходит увеличение радиуса круга, а затем – уменьшение. В результате данного изменения некоторые точки меняют свой класс. Набор содержит 60000 элементов. Радиус круга до увеличения и после уменьшения равен 10. Радиус после увеличения равен 20.

Эксперимент осуществлялся в следующей последовательности. Пусть значение $y_{t,1}$ элемента y_t характеризует класс, к которому принадлежит элемент. При получении очередного элемента последовательности y_t последовательность значений признаков $\{y_{t,2}; y_{t,3}; \dots; y_{t,K}\}$ используются классификатором для предсказания значения $y_{t,1}$. Пусть предсказанное классификатором значение обозначается как $\hat{y}_{t,1}$. Если $y_{t,1} \neq \hat{y}_{t,1}$, то происходит увеличение счетчика ошибок E на 1. На следующем этапе взятые по модулю значения признаков $\{|y_{t,2}|; |y_{t,3}|; \dots; |y_{t,K}|\}$ используются детектором для обнаружения дрейфа концепта.

Если детектор фиксирует наличие дрейфа, то устанавливается флаг l , обозначающий активное состояние фазы обучения. После того как флаг l установлен, происходит накопление элементов y_t в массиве Y_L . При достижении массивом размера L его содержимое используется для обучения новой модели. Флаг l при этом сбрасывается, а массив Y_L очищается. Схожий принцип применяется в алгоритме Adaptive Random Forest (ARF) [10].

Для использованных детекторов были заданы следующие параметры: $N = 5000$; $N_2 = 1000$; $\lambda_1 = 1,25$; $\lambda_2 = 100$; $\delta = 0,1$.

На графике (рис. 18) представлены зависимости вероятности ошибок классификации от объема поступающих данных. Две вертикальные линии (вблизи значений 20000 и 40000 по оси абсцисс) обозначают моменты смены концепта. Можно заметить, что на начальном участке вероятность ошибки находится на уровне единицы, что обусловлено необходимостью получить 2000 элементов перед началом обучения классификатора. Верхняя кривая характеризует эффективность классификации при отсутствии детектора дрейфа.

Из представленных зависимостей можно видеть, что использование детектора смены концепта позволяют снизить примерно на 5% вероятность ошибки классификации при каждой смене концепта.

Выводы

В работе предложен двухступенчатый алгоритм обнаружения смены концепта в наблюдаемом потоке данных, базирующийся на статистических характеристиках атрибутов трафика мобильных приложений и названный в работе ДСК Фишера-Пейджа-Хинкли. Текущий анализ анализируемых приложений осуществляется с помощью двух скользящих окон, контролирующих изменение текущих статистических характеристик атрибутов мобильных приложений.

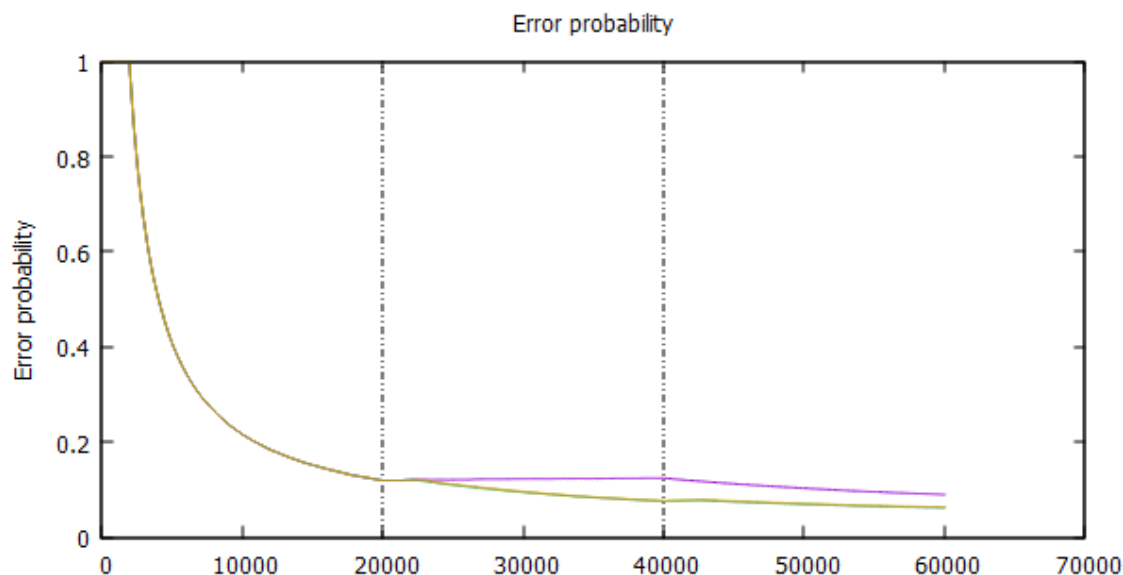


Рис. 18. Зависимость изменения вероятности ошибок классификации от объема поступающих данных при двух смещениях концепта.

На первом этапе применяется решающая статистика в соответствии с критерием Фишера. На втором этапе для проверки гипотез используется тест Пейджа – Хинкли. В результате проведенных экспериментов по классификации искусственного набора данных с использованием разработанного классификатора, реализующего алгоритм K Nearest Neighbors, получены данные, позволяющие оценить работоспособность предложенного двухэтапного алгоритма обнаружения дрейфа концепта.

В процессе эксперимента получены зависимости, позволяющие оценить уровень вероятности ошибок, допускаемых классификатором при использовании разработанного ДСК. Показано, что классификатор, не использующий ДСК, допускает примерно на 5% больше ошибок, чем классификаторы, использующие его.

Литература

1. Gama J. et al. A survey on concept drift adaptation //ACM computing surveys (CSUR). – 2014. – Т. 46. – №. 4. – С. 44.
2. Baena-Garcia M. et al. Early drift detection method //Fourth international workshop on knowledge discovery from data streams. – 2006. – Т. 6. – С. 77-86.
3. Gama J., Sebastião R., Rodrigues P. P. On evaluating stream learning algorithms //Machine learning. – 2013. – Т. 90. – №. 3. – С. 317-346.
4. Шелухин О. И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. – М.: Горячая линия –Телеком, 2019. – 448 с. ISBN 978-5-9912-0756-0.
5. Mouss H. et al. Test of page-hinckley, an approach for fault detection in an agro-alimentary production system //2004 5th Asian Control Conference (IEEE Cat. No. 04EX904). – IEEE, 2004. – Т. 2. – С. 815-818.
6. Шелухин О. И., Ерохин С. Д., Ванюшина А. В. Классификация IP-трафика методами машинного обучения //Горячая линия–телеком. – 2018.
7. Cunningham P., Delany S. J. k-Nearest neighbour classifiers //Multiple Classifier Systems. – 2007. – Т. 34. – №. 8. – С. 1-17.
8. Minku L. L., White A. P., Yao X. The impact of diversity on online ensemble learning in the presence of concept drift //IEEE Transactions on knowledge and Data Engineering. – 2009. – Т. 22. – №. 5. – С. 730-742.
9. Gama J. et al. Learning with drift detection //Brazilian symposium on artificial intelligence. – Springer, Berlin, Heidelberg, 2004. – С. 286-295.

10. Gomes H. M. et al. Adaptive random forests for evolving data stream classification //Machine Learning. – 2017. – T. 106. – №. 9-10. – C. 1469-1495.

Concept drift detection in a network mobile traffic setting using a Fisher-Page-Hinckley test

Sheluhin O.I.³⁰³, Sekretarev S.A.³⁰⁴

Abstract. *In a streaming data classification, there is a problem called a concept drift. The concept drift occurs when a data used to learn a model is changed. When in a streaming data setting a mobile traffic classifier should be used with a concept drift detector. This article proposes a 2-step concept drift detection algorithm. The proposed algorithm is based on two sliding windows that monitor mobile traffic attributes. Algorithm's first step uses the Fisher criterion. Algorithm's second step uses the Page-Hinckley test. Performed experiments show that proposed algorithm can be used to detect concept drift. Obtained results show that proposed algorithm decreases classification error probability by 5% in comparison to classifier without a concept drift detector.*

Keywords: *machine learning, k nearest neighbors, concept drift, sliding windows, the Page Hinckley test*

³⁰³ Oleg Sheluhin, Dr.Sc, Professor, MTUCI, Moscow, sheluhin@mail.ru

³⁰⁴ Sergey Sekretarev, MTUCI, Moscow, svoboda.vezde@gmail.com

Разработка модели испытательного стенда для установки и настройки системы аудита безопасности Linux сервера.

Юшкевич А.С.³⁰⁵

***Аннотация.** В данной статье представлен процесс разработки модели испытательного стенда и ее проверки на решении реальных задач для тестирования системы аудита. Подробно описаны структура, принцип работы функциональных элементов, результаты тестирования системы и анализ рассматриваемого стенда. Разработанная модель позволяет полностью подстроиться под структуру реальной сети, на ранних этапах выявить недостатки и ошибки в настройках и работе системы и без остановки бизнес-процессов предприятия или компании внедрить, уже протестированную и отлаженную систему аудита.*

***Ключевые слова:** правила аудита, бизнес-процессы, тестирование, автоматизация.*

Введение

Аудит является важным аспектом системного администрирования, так как с его помощью можно получать подробную информацию о всех системных событиях, дальнейший анализ которых позволяет выявлять подозрительную активность и находить атаки[1]. Грамотная эксплуатация системы аудита существенно повышает уровень безопасности всей системы. Для обеспечения удобства использования и корректного подбора конфигураций настроек аудита под конкретные задачи безопасности, необходимо тестировать систему на специальных испытательных стендах [2]. Пример процесса разработки одного из возможных вариантов архитектуры сети для тестирования системы аудита безопасности далее описан в данной статье.

Общая структура испытательного стенда

Принцип работы испытательного стенда заключается в взаимодействии сервера с удаленным пользователем, путем отправки запросов. Как видно из рисунка 1, взаимодействие между ними осуществляется по каналу связи SSH.

Сервер и клиент имеют ряд подключенных к ним облачных сервисов, а именно: удаленное хранилище данных (Sonatype Nexus), система мониторинга log файлов (Splunk), система мониторинга показателей нагрузки системы (Chronograf), система автоматического запуска компиляции программ (Jenkins CI).

Подсистема аудита предназначена для отслеживания критичных, с точки зрения безопасности, событий [3], и устанавливается на стороне сервера.

³⁰⁵ Юшкевич Алексей Сергеевич, студент МГТУ им.Н.Э.Баумана, yshkevichas@gmail.com

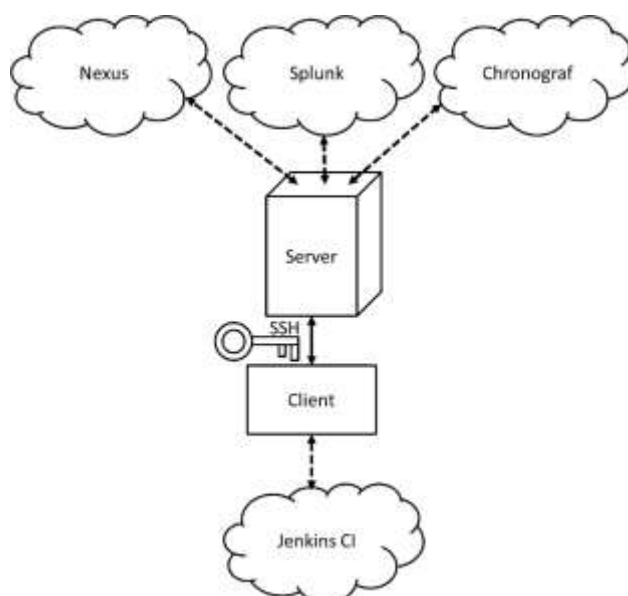


Рис.1. Структура испытательного стенда

Принцип работы функциональных элементов стенда

На стороне клиента разрабатываются bash скрипты, где содержится набор команд. Jenkins CI автоматически посылает запросы этих скриптов на удаленный сервер.

Для контроля папок сервера, которыми пользуется клиент, были прописаны соответствующие правила для подсистемы Audit Daemon. Любое событие фиксируется журнальном файле: /var/log/audit/audit.log.

Для резервного копирования журнального файла, модель предусматривает автоматическую загрузку его разных версий в удаленное хранилище Nexus. Данное решение позволяет предотвратить заполнение дискового пространства сервера, увеличивающимся log файлом[4].

Важной задачей первичной обработки системных событий является представление содержимого log файлов в читабельном виде[5]. В данном случае используется система Splunk, настроенная на прослушивание директории /var/log/audit.

Для решения многих задач при настройке аудита полезным является знать показатели нагрузки на сервер[6]. При осуществлении взаимодействия сервера с клиентом, для обеспечения работы функциональных элементов стенда сервер расходует производственные ресурсы. Сервис Chronograf реагирует на запуск того или иного процесса и отражает конкретные показатели нагрузки, что позволяет выявлять критические значения нагрузки для сервера.

Конфигурационные настройки функциональных элементов стенда

На примере полностью настроенного и работающего испытательного стенда для тестирования аудита безопасности системы, рассмотрим конфигурацию каждого функционального элемента в отдельности.

Клиент Ubuntu обладает следующими техническими характеристиками:

- Разрядность ОС – 64 бит;
- Оперативная память – 3072 МБ;
- Дисковое пространство – 20 ГБ;
- Количество ядер – 1.

Сервер Centos 7 обладает следующими техническими характеристиками:

- Разрядность ОС – 64 бит;
- Оперативная память – 3072 МБ;

- Дисковое пространство – 10 ГБ;
- Количество ядер – 2.

Jenkins CI. Подключиться к сервису можно по ссылке в браузере: «ip_local:port». На рисунке ниже приведен фрагмент интерфейса настроек задачи для сборки. Данный код выполняет функцию проверки статуса работы установленных на сервере сервисов.

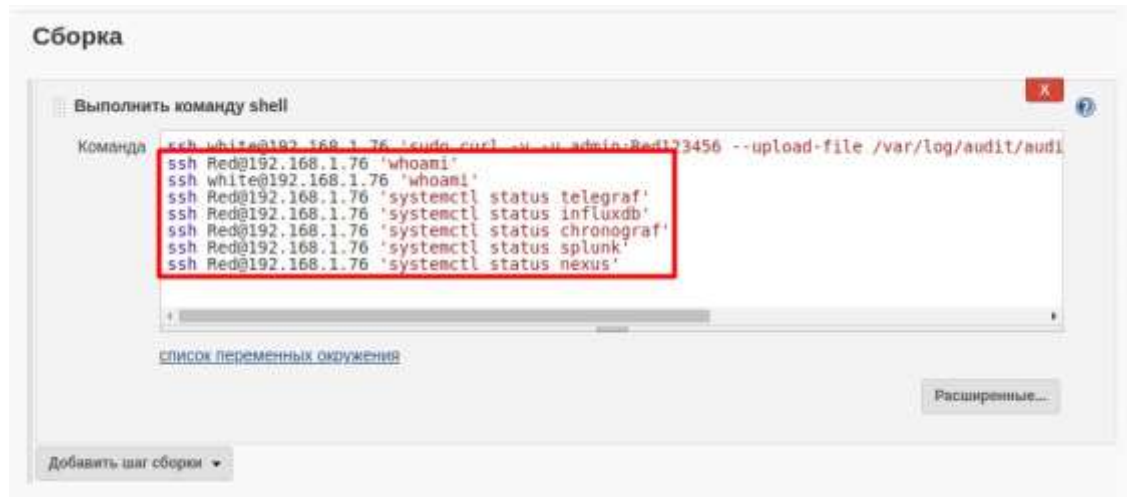


Рис.2. Проверка статуса работы сервисов

Audit Daemon. Данный пакет является стандартным и дополнительных команд для скачивания и распаковки дистрибутивов не требует[7]. По умолчанию сервис не имеет правил. Главный конфигурационный файл находится по следующему пути: «/etc/audit/audit.conf». Правила нужно прописывать напрямую в файл: «/etc/audit/rules.d/audit.rules».

Nexus, Chronograf, Splunk. Оставшиеся сервисы специальной настройки не требуют. Подключение к ним аналогичны, как и к сервису Jenkins, за исключением разницы в портах.

Написание bash скриптов

Рассмотрим в качестве примера один из разработанных bash скриптов.

```
scp -T white@192.168.1.76:/home/white/Ubuntu-client/Other/Video/569.mp4
/home/white/Документы/files/OTHERS/Video
...
scp -T /home/white/Документы/files/OTHERS/Video/1/a/817 white@192.168.1.76:/home/white/Ubuntu-
client/Other/Video/1
...
rm /home/white/Документы/files/OTHERS/Video/1/a/817
rm /home/white/Документы/files/OTHERS/Video/2/b/569
...
ssh white@192.168.1.76 'sudo curl -v -u --upload-file /var/log/audit/audit.log
http://192.168.1.76:8081/repository/AUDIT_LOG/"$i"'
```

Принцип алгоритма заключается в том, что клиент и сервер обмениваются между собой файлами и удаляют их. После чего со стороны сервера загружаются текущие журнальные файлы в Nexus. Алгоритм повторяется 10 раз. При компиляции второго скрипта клиент копирует себе из папок сервера файлы и удаляет все загруженное, что повторяется 150 раз. Данный скрипт обеспечивает пиковую нагрузку на сервер, когда оставшиеся ресурсы начинают резко расходоваться на выполнение множества простых команд[8].

Написание правил аудита

При открытии содержимого в, уже известном, файле «audit.rules» можно найти список постоянных правил системы аудита сервера. А именно:

```
-w /home/Ubuntu-client/Video -p wa -k hosts_file_change
```

Как уже говорилось выше - наблюдение за файловой системой может быть установлено на файлы и каталоги. Синтаксис правил, которые показаны выше, реализует именно этот функционал:

- -w - путь к файлу или каталогу;
- -p - опции, при выполнении которых будет генерироваться запись;
- -k - помогает определить, какие правила генерировали конкретную запись в журнале.

При грамотном и правильном использовании возможностей стандартного сервиса по аудиту системы локально можно контролировать и более серьёзные процессы[9]. Таким образом, система аудита сгенерирует новую запись в журнале, если произойдёт доступ к любому файлу одной из определенных папок сервера[10].

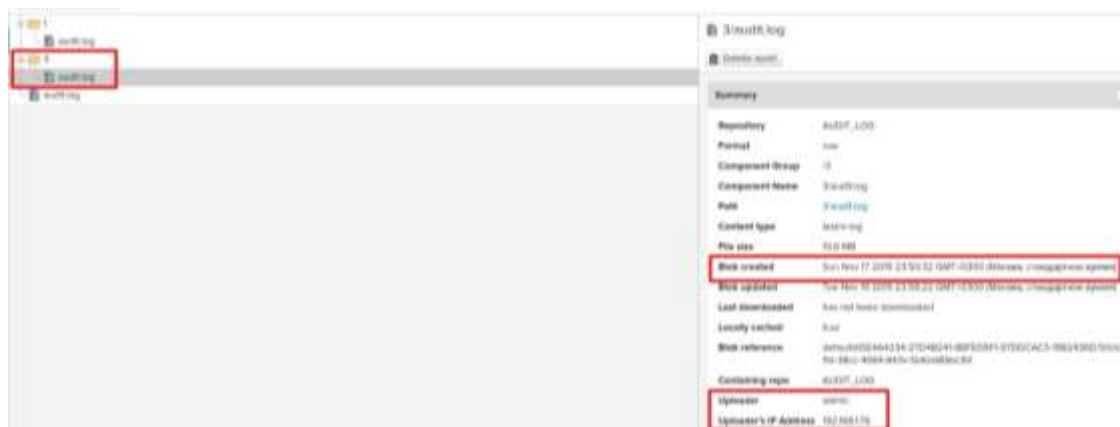
Демонстрация работы испытательного стенда

Сервисы настроены так, что при включении машин они будут запускаться автоматически. Через браузер открываем все сервисы по определенным ссылкам. В Jenkins CI нажатием на клавишу старта сборки скрипта. Ниже показана метрика, которую измеряет Chronograf:



Рис.3. Результат работы сервиса измерения системной нагрузки

На левом графике отображается в процентном соотношении загруженность оперативной памяти сервера. Первый скачок, после которого наблюдается растущая



динамика загрузки, произошел в период времени запуска bash скрипта. На правом графике так же можно наблюдать скачек после старта первого процесса загрузки, что отображает скорость работы дискового пространства. С увеличением загрузки оперативной памяти различными процессами, видна общая динамика снижения скорости.

Рис.4. Результат работы сервиса измерения системной нагрузки

На рисунке 4 представлен интерфейс хранилища Nexus, где после двух выполненных циклов, была произведена выгрузка журнальных файлов системы аудита, о которых доступна минимальная информация: дата записи, размер файла, формат, IP адрес отправителя и т.д.

Анализ результатов работы

К основным плюсам испытательного стенда тестирования системы аудита, можно отнести:

1. Полная автоматизация алгоритма работы стенда на всех этапах его жизненного цикла;
2. Масштабируемость;
3. Простота реализации;
4. Ресурсоемкость;
5. Взаимозаменяемость функциональных элементов;
6. Отсутствие четких требований к конфигурациям настройки стенда;
7. Гибкость системы;
8. Широкий спектр сфер применения.

Под масштабируемостью понимается возможность увеличения количества серверов и подключенных к нему клиентов или добавление новых структурных элементов (база данных, маршрутизатор, принтер).

Представленная модель испытательного стенда не требует больших ресурсов от локального компьютера, при условии воссоздания модели сети с небольшим количеством серверов и клиентов.

При необходимости каждый функциональный элемент можно заменить на любой другой, с соответствующим функционалом. Так же нет четкой привязки к операционным системам клиентов и серверов.

Отсутствие четких требований к конфигурациям настройки стенда является следствием взаимозаменяемости элементов. Это обусловлено тем, что каждый отдельный сервис имеет свои отличительные преимущества по сравнению с другими, поэтому под каждый функциональный элемент стенда настройки будут индивидуальными.

Гибкость обусловлена большим набором настроек всех функциональных элементов по отдельности. Под этим подразумевается легкость в перенастройке одного и того же стенда под абсолютно разные задачи.

Главным достоинством является широкий спектр сфер применения модели испытательного стенда. Сервер может быть почтовым, веб или файловым, меняются лишь запросы от клиента и конфигурации правил аудита.

Выводы

В данной статье подробно были описаны структура испытательного стенда, принцип работы его функциональных элементов по отдельности и всей системы в целом, а так же создана система аудита сервера для решения поставленных задач. После чего наглядно продемонстрирован метод запуска системы и процесс ее работы с реальными итоговыми показателями.

Исходя из проведенного анализа разработанного испытательного стенда можно с уверенностью отметить полную пригодность данной модели для тестирования установки,

настройки и отладки системы аудита под требуемые задачи. Это позволит избежать допущения ошибок при ее настройке, например, на реальной сети компании или предприятия. Так же модель позволит заранее выявить недостатки и особенности разрабатываемой системы аудита и без вмешательств в рабочие процессы сотрудников произвести полную установку, уже корректно работающей, системы аудита.

Литература

1. Лаврищева Е.М., Мутилин В.С., Рыжов А.В. Моделирование прикладных и информационных систем из готовых сервисных ресурсов интернет // [Труды института системного программирования РАН. 2019. 16 с.](#)
2. Абгарян К.К., Гаврилов Е.С. Информационная поддержка интеграционной платформы многомасштабного моделирования // Системы и средства информатики. 2019. С. 57.
3. Буренин А.Н., Легков К.Е. Основные проблемы безопасности подсистем обеспечения единым временем элементов систем управления сложными организационно-техническими объектами // Т-сomm: телекоммуникации и транспорт. 2019. С. 48.
4. Макаревич О.Б., Пескова О.Ю., Бабенко Л.К. Аналитический обзор актуальной проблематики в области информационной безопасности по результатам проведения XIII международной научно-практической конференции "Информационная безопасность-2014" // Вопросы защиты информации. 2015. С. 81.
5. Марков С. А., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации: учеб. издание. -М.: Радио и связь, 2012. 192 с.
6. Кияев В.И., Сайтов А.В. Защита информации в информационных системах, локальных и глобальных компьютерных сетях // Комплексная информационная безопасность в управлении современным предприятием. 2016. С. 132.
7. Лаврищева Е.М., Рыжов А.Г. Подход к моделированию систем и сайтов из готовых ресурсов // Научный сервис в сети интернет. 2018. С. 336.
8. Соколова Н.А., Ходакова В.Е., Бабина О.А., Антипенко И.В. Оценивание развития одного класса сложных систем // Информационная безопасность регионов России (ИБРР-2015). 2015. С. 232.
9. Лисс А.А., Соловьев Д.Н., Пестунова П.М. Создание экспериментальной сетевой среды для изучения компьютерной и сетевой безопасности // [Информационное противодействие угрозам терроризма](#). 2015. С. 249.
10. Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. № 1 (14). С. 24-30.

Научный руководитель: Марков Алексей Сергеевич, профессор, доктор технических наук, руководитель ГК НПО «Эшелон», a.markov@bmstu.ru.

Development of a test bench model for installing and configuring a Linux server security audit system Yushkevich A.S.

Annotation. This article presents the process of developing a test bench model and its examination on solving real tasks of testing an audit system. There is a detailed description of the structure, the principle of operation of functional elements, the results of system testing and analysis of the stand. The developed model allows adapt to the structure of a real network, to identify flaws and errors in the settings and operation of the system at the early stages and without stopping the business processes of an enterprise or company to introduce an already tested and debugged audit system.

Keywords: audit rules, business processes, testing, automation.

ОГЛАВЛЕНИЕ

1. Акулов Е.А. Программно-аппаратная система аутентификации в пользовательских приложениях.....	2
2. Антонов С.Г., Гвоздева Г.А., Климов С.М. Методика повышения устойчивости функционирования информационно-управляющих систем при информационно-технических воздействиях.....	6
3. Басараб М.А., Бельфер Р.А., Кравцов А.В. Учебный имитатор объединенной отечественной сети ПД специального назначения (структура, функции).....	12
4. Басараб М.А., Троицкий И.И., Якубов Р.Ж. Использование линейной фильтрации дискретного сигнала в аддитивном шуме по двум каналам передачи информации для улучшения его корреляционного приема	19
5. Бегаев А.Н., Юркин А.А., Шугуров Д.Е., Бегаев С.Н. Предложения по учету основных свойств систем аутентификации при поименованном взаимодействии субъектов (объектов) в компьютерных системах и сетях	27
6. Белова Е.А., Кузнецов А.М., Нестерова М.А., Погорелко Е.А. Влияние экранирования на энергию сигнала, излучаемого интерфейсом LVDS.....	33
7. Бондарев В.В. Возможный подход к оценке средств защиты информации.....	38
8. Бондарев В.В. Учебно–материальная база подготовки специалиста в области информационной безопасности	42
9. Быков А.Ю., Акулова Н.О. Игровая постановка задачи выбора дополнительного фактора аутентификации для рабочих мест на примере клавиатурного почерка	46
10. Быков А.Ю., Крыгин И.А. Постановка задачи выбора средств защиты на основе модели дискретно-непрерывной игры с противоположными интересами при ограничениях на ресурсы и подходы к ее решению	51
11. Ванин А.В. Методы аутентификации с использованием носимых устройств.....	56
12. Варфоломеев А. А. Усиление стойкости протокола обмена ключами с аутентификацией Белловина и Меррита за счет использования асимметричного выполнения криптосистем	60
13. Величко И.К. Исследование криптовалюты Monero с точки зрения информационной безопасности.....	65
14. Вишневский А.С., Ключарев П.Г. Звуковой пользовательский интерфейс обманной системы	70
15. Воронина Е.Н. Сравнительный анализ подходов к поиску уязвимостей программного обеспечения методом фаззинг-тестирования	75
16. Ворончихин И. С. Динамическое изменение структурно-функциональных характеристик информационной системы в целях снижения эффективности сетевой разведки	81
17. Галимов Ш.У. Криптографические операции на устройствах малой производительности.....	88
18. Глинская Е.В. Безопасное обновление операционных систем для мобильных устройств	96
19. Гончаров Н.И. Подход к обоснованию мер по защите информации в информационно-телекоммуникационных сетях	102
20. Леонтьев В.К., Гордеев Э.Н. О числе допустимых решений систем булевых уравнений.....	107

21. Леонтьев В.К., Гордеев Э.Н. О приближенных «решениях» несовместных систем булевых уравнений.....	111
22. Горшков Ю.Г. Средства фonoскопической экспертизы нового поколения	117
23. Дамдинова Т.Ц., Базарон С.С., Абатнин А.А. Обработка изображений в информационной безопасности.....	121
24. Добкач Л.Я. Обзор методов распознавания компьютерных атак.....	124
25. Ефремов Е.А., Ершова Ю.А., Чуфистов А.А. Анализ проектов электронной идентификации граждан в Латинской Америке	130
26. Жиров П.В. Анализ методов сбора событий информационной безопасности при использовании систем мониторинга событий информационной безопасности с применением технологий SIEM.....	135
27. Жоголев Г.Д. Реализация криптографических алгоритмов на ПЛИС	140
28. Жуков Д.А. О порядке одной перестановки на элементах квадратной матрицы	143
29. Зеленецкий А.С. Изучение булевых функций, имеющих аффинные аннигиляторы	146
30. Зуев Ю.А. О вероятности одновременного осуществления нескольких событий при отсутствии условия независимости.....	150
31. Иванов И.И. Протокол динамического управления маскированными каналами связи.....	153
32. Капалова Н.А., Хаумен А. Симметричный блочный алгоритм шифрования данных «BC-2»	161
33. Карцхия А. А., Макаренко Д. Г. Правовые аспекты статуса и рисков искусственного интеллекта.....	167
34. Климцов В.Е., Чиликов А.А. Локализация сбоев при дифференциальном криптоанализе по ошибкам вычислений поточных шифров, основанных на нелинейных регистрах сдвига	172
35. Ключарёв П.Г. Графы Пайзера в задачах криптографии и обработки информации	176
36. Козарь А.А. Проблема информационной безопасности в сфере авионики.....	180
37. Козачок А.В., Копылов С.А., Нгуен М.Т. Аналитическая модель оценки предельно достижимой емкости встраивания робастного водяного знака.....	185
38. Козачок А.В., Спирин А.А. Подходы к классификации псевдослучайных последовательностей	191
39. Козлов Д.В. Метод представления информации об инцидентах информационной безопасности.....	196
40. Кокорин А.О. Исследование возможностей системы Agda в создании верифицированного генератора псевдослучайных чисел	200
41. Кондаков С.Е., Рудь И.С. К вопросу об определении «вредоносного программного обеспечения»	204
42. Кондаков С.Е., Рудь И.С. Классификация компьютерных атак с использованием вредоносного программного обеспечения.....	208
43. Коновалов А.А. Методика обеспечения сжатия и безопасности передачи данных в области телемедицины.....	212

44. Корнеев Н.В., Меркулов В.Д. Интеллектуальная аналитика в обеспечении защищенности от комплексных угроз	215
45. Костогрызов А.И. Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта	220
46. Кузнецова В.Ю. Аспекты оценки эффективности подготовки специалистов в области информационной безопасности	230
47. Кулагин Г.И. Исследование современных технологий добычи электронных денег в сетях блокчейн.....	233
48. Лебедев А. Н. Доказательство сводимости задачи DLOG к задаче DH.....	238
49. Лебедев А.Н., Марченков С.Д. Анализ стратегий ложных информационных систем.....	242
50. Лебедев А.Н., Николаенкова Е.К. Исследование стеганографического метода хранения информации в текстурах 3D-объектов.....	246
51. Литвиненко Д.И. Разработка способа практической реализации технологии применения электронной подписи в рамках предприятия	251
52. Ловцов Д.А., Гаврилов Д.А., Макаренко Г.И. Защищенная переработка визуальной информации в автоматизированной оптико-электронной системе наземно-космического мониторинга	254
53. Малахов М.В., Алексеев К.А. Автоматизированное средство статической инструментации исполняемого кода встроенного программного обеспечения	261
54. Маркин Д.О., Вихарев А.Н., Звягинцев С.А., Павлов Д.И. Алгоритм защиты терминальных программ от анализа на основе виртуальных машин с секретной архитектурой.....	267
55. Маркин Д.О., Зверев А.А., Саклаков А.И., Рыков Д.А. Технологии распознавания моделей точек входа веб-приложений	275
56. Маркин Д.О., Умбетов Т.К., Архипов М.А., Миначев В.М. Современные технологии построения доверенных сред исполнения приложений на уровне базовой системы ввода-вывода	281
57. Маркова И.А. Эмулирование сети как метод исследования уязвимостей на примере протокола междоменной маршрутизации BGP.....	287
58. Марченко А.В. Метод защиты персональных данных в «ЕНР – электронная медицинская книжка»	293
59. Мессерле А.А. Применение средств поиска ключевых слов в слитной речи в DLP-системах	297
60. Минаков В.Ф., Шепелёва О.Ю., Лобанов О.С. Ресурсно-временная модель повышения защищенности конфиденциальных данных	301
61. Нечаев О.В. Исследование основных криптовалют на рынке и их сравнение с точки зрения информационной безопасности	305
62. Пономаренко Г.С. Ключарёв П.Г. Классификация программ на языке Javascript по признаку обфусцированности при помощи искусственной нейронной сети с механизмом внимания	312
63. Райкова Н.О. Риск-ориентированный подход в разработке безопасного программного обеспечения	317

64. Ревенков П.В., Бердюгин А.А. Вероятностный анализ риска воздействия кибератак на системы электронного банкинга.....	323
65. Ромашкина Н.П. Новые технологии: вызовы международной безопасности и стабильности.....	329
66. Сафин И.Р., Колосов Д.В. Анализ защищенности высокочастотных бесконтактных смарт-карт Mifare	335
67. Строгалева С. Ю., Ефремов Е. А. Определение стойкости шифрования методом гаммирования	338
68. Титов А.Ю. Обзор подходов к применению технологий искусственного интеллекта в информационной безопасности	343
69. Фомченко А.В. Разработка алгоритма стегоанализа с использованием машинного обучения.....	352
70. Чиликов А.А., Жуков А.Е., Верховский А.И. Исследование обратимых клеточных автоматов с конечной решеткой	354
71. Чиликов А.А., Яковлев А.Н. Информационная безопасность и цифровая криминалистика: проблемы, решения и новые вызовы.....	361
72. Чичварин Н.В., Медведев Н.В. Угрозы информационной безопасности гражданского воздушного судна.....	367
73. Чукляев И.И., Чепурной Е.А., Шевченко А.Л. Интеллектуальная защита сложных организационно-технических систем.....	371
74. Шайтура С.В., Минитаева А.М., Феоктистова В.М., Ордов К.В. Цепочки блоков в защите пространственных данных	377
75. Шатунов А.В., Ченцов В.А. Подход к предотвращению инсайдерских утечек информации	380
76. Шелухин О.И., Полковников М.В. Исследование алгоритма Isolation Forest при бинарной классификации сетевых аномалий	387
77. Шелухин О.И., Секретарев С.А. Обнаружение дрейфа концепта с использованием статистики Фишера-Пейджа-Хинкли при потоковой классификации трафика мобильных приложений	394
78. Юшкевич А.С. Разработка модели испытательного стенда для установки и настройки системы аудита безопасности Linux сервера.....	399

ISBN 978-5-9906630-6-0



Издательство МГТУ им. Н.Э.Баумана
Россия, Москва, 105005, ул.2-я Бауманская, д.5, стр.1.
Тел. (499)263-6391, Факс: (499) 267-4844
Подписано в печать 29.12.2019, Заказ 029876
Формат 60х90.8. Гарнитура Times New Roman
Усл. печ. 27.12. Тираж 100 экз.