

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»

СЕДЬМАЯ
ВСЕРОССИЙСКАЯ
НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

(Москва, 16-17 ноября 2017 года)

СБОРНИК ТРУДОВ КОНФЕРЕНЦИИ

Под общей редакцией В.А.Матвеева

МГТУ им.Н.Э.Баумана
НУК «Информатика и системы управления»
МОСКВА-2016

УДК 003.26.7:004.09
ББК 32.973.202
Б31

Б31

Безопасные информационные технологии. Сборник трудов Седьмой всероссийской научно-технической конференции / под. ред. В.А. Матвеева – М.: МГТУ им. Н.Э.Баумана, 2016. 345 с. – илл.

ISBN 978-5-9906630-2-2

Сборник содержит тезисы докладов, представленных на Седьмой всероссийской научно-технической конференции "Безопасные информационные технологии" (БИТ-2016), проходившей 16-17 ноября 2016 в Москве в МГТУ им. Н.Э. Баумана.

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

Редколлегия:

Матвеев В.А., Заслуженный деятель науки РФ, д-р техн. наук, профессор, руководитель НУК ИУ МГТУ им.Н.Э.Баумана – зав. кафедрой ИУ-8 МГТУ им.Н.Э.Баумана

Марков А.С., д-р техн. наук, профессор кафедры ИУ-8 МГТУ им.Н.Э.Баумана
Медведев Н.В., канд. техн. наук., доцент кафедры ИУ-8 МГТУ им.Н.Э.Баумана
Ковынев Н.В., ассистент кафедры ИУ-8 МГТУ им.Н.Э.Баумана

УДК 003.26.7:004.09
ББК 32.973.202

ISBN 978-5-9906630-2-2

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

Определение актуальных угроз в критических системах информационной инфраструктуры и противодействие им

Алешин В.В.¹

В данной статье проведен обзор состояния вопроса обеспечения безопасности критических систем информационной инфраструктуры, приведены методологии по построению модели нарушителя и модели угроз в таких системах, а также обоснована актуальность использования устройств класса Unified Threat Management для противодействия угрозам информационной безопасности критически важных объектов.

Ключевые слова: АСУ ТП, критически важные объекты, модель угроз, модель нарушителя

Введение

Ключевая система информационной инфраструктуры (КСИИ) – это информационно система, которая осуществляет управление критически важным объектом (КВО), в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация. К таким системам относятся автоматизированные системы управления технологическими процессами (АСУ ТП) объектов автономной промышленности, топливно-энергетического комплекса, а также систем госструктур и другие. Понятие КСИИ обобщает в себе множество различных классов систем: предупреждения чрезвычайных ситуаций; навигационные; управления водоснабжением; управления транспортом другие.

В процессе определения угроз безопасности информации (УБИ) в КСИИ необходимо уделять внимание угрозам, не только связанным с нарушением конфиденциальности, целостности и доступности информации, но и направленными воздействиями на КВО, поэтому при формировании перечня актуальных УБИ в КСИИ, необходимо учесть все возможные сценарии реализации угроз. [1]

Процесс формирования перечня актуальных угроз включает в себя следующие этапы:

- разработка модели нарушителя;
- разработка модели УБИ.

Разработка модели нарушителя

Модель нарушителя ИБ содержит:

- уровень физического доступа (PhL) к информации;
- уровень логического доступа (LogL) к информации;
- уровень компетенции (C) нарушителя;
- уровень оснащенности (A) нарушителя;
- мотивацию (M) нарушителя.

Общая запись модели нарушителя производится в виде строки:

$$PhL:[x]/LogL:[x]/C:[x]/A:[x]/M:[x]$$

где вместо [x] записывается значение соответствующего параметра

Общий уровень компетенции (C) нарушителя ИБ вычисляется по формуле:

$$C = \begin{cases} \text{высокий (H) при } (C_{IQ} + C_{SYS}) > 5 \\ \text{средний (M) при } 2 < (C_{IQ} + C_{SYS}) \leq 5 \\ \text{низкий (L) при } (C_{IQ} + C_{SYS}) \leq 2 \end{cases} \quad (1)$$

где C_{IQ} – общие технические знания нарушителя (от 0 до 5), C_{SYS} – осведомленность нарушителя (от 0 до 5).

¹ Алешин Вячеслав Вячеславович, МГТУ им. Н.Э. Баумана, Москва, v.nishela@gmail.com

Оценка предварительного базового потенциала нарушителя производится на основе значений уровней компетенции и оснащённости (см. Таблица 1).

Таблица 1 – Значения уровней компетенции и оснащённости нарушителя

Уровень	Показатель	Значение
Компетенции (C)	Низкий	0
	Средний	2
	Высокий	5
Оснащённости (A)	Отсутствует	0
	Стандартное оборудование	1
	Специализированное оборудование	3
	Заказное оборудование	5

Полученные значения суммируются, и определяется предварительный базовый потенциал нарушителя:

$$Pt_{BASE} = \begin{cases} \text{высокий (H)} & \text{при } (C + A) \geq 8 \\ \text{средний (M)} & \text{при } 5 \leq (C + A) < 8 \\ \text{низкий (L)} & \text{при } 3 \leq (C + A) < 5 \\ \text{отсутствует (N)} & \text{при } (C + A) < 3 \end{cases} \quad (2)$$

При вычислении базового потенциала, необходимо учитывать уровни логического доступа к КСИИ (см. Таблица 2).

В случае высокой мотивации потенциал переходит на следующий уровень, в случае ее отсутствия – на предыдущий.

Таблица 2 – Определение базового потенциала нарушителя ИБ с учетом прав логического доступа к объектам системы

Уровень логического доступа нарушителя к объектам системы	Предварительный базовый потенциал нарушителя безопасности информации в системе			
	отсутствует	низкий	средний	высокий
L ₀	отсутствует	низкий	средний	высокий
L ₁	отсутствует	низкий	средний	высокий
L ₂	низкий	средний	Высокий	высокий
L ₃	низкий	средний	Высокий	высокий

Разработка модели УБИ

Под УБИ понимается совокупность условий и факторов, создающих потенциальную опасность нарушения конфиденциальности, доступности и целостности информации. Для выявления актуальных УБИ используется метод построения деревьев атак, на основе данных о функционировании КСИИ, уязвимостях программного обеспечения, а также о возможных векторах реализации УБИ. [2]

Вероятность реализации УБИ определяется исходя из базового потенциала нарушителя, уровня физического доступа к КСИИ, необходимостью реализации угрозы рассматриваемым путем, а также уровня опасности уязвимостей, способствующих реализации УБИ. Уровень опасности уязвимостей оценивается исходя из методики CVSS. Пример оценки вероятности реализации УБИ в КСИИ отображен в таблицах (см. табл 3, табл. 4).

Противодействие угрозам в КСИИ

Проблемы в области информационной безопасности (ИБ) КСИИ вызваны как объективными, так и субъективными причинами. К объективным можно отнести проблемы, связанные с возможным влиянием средств защиты информации на задержки и время реакции компонентов КСИИ. К субъективным – отсутствие централизованного управления средствами защиты КСИИ, что существенно усложняет процесс администрирования.

Таблица 3 – Предварительная оценка вероятности реализации УБИ

Базовый потенциал нарушителя (Pt_{BASE})	Уровень физического доступа нарушителя (LogL)	Необходимость физического доступа к компонентам АС	
		Да	Нет
Высокий	Out	Низкая	Высокий
Высокий	In	Высокая	Высокий
Средний	Out	отсутствует	Средний
Средний	In	Средняя	Средний
Низкий	Out	отсутствует	Низкий
Низкий	In	Низкая	Низкий
Отсутствует	Out	отсутствует	Отсутствует
Отсутствует	In	отсутствует	отсутствует

Таблица 4 – Оценка вероятности реализации УБИ с учетом уровня опасности уязвимостей

Вероятность реализации УБИ	Уровень опасности уязвимостей				
	отсутствует	низкий	средний	высокий	критический
Отсутствует	отсутствует	отсутствует	отсутствует	отсутствует	отсутствует
Низкая	отсутствует	отсутствует	Низкая	средняя	средняя
Средняя	низкая	низкая	Средняя	высокая	высокая
Высокая	средняя	средняя	Высокая	высокая	высокая

В состав системы обеспечения ИБ КСИИ должны входить следующие основные подсистемы:

- Управления доступом;
- Регистрации и учета;
- Антивирусной защиты;
- Обнаружения вторжений;
- Межсетевого экранирования.

При установке средств защиты под каждую из подсистем, возникают трудности при внедрении и обслуживании. Вытекающие из этого факторы стали аккумулялирующими для использования средств защиты класса Unified Threat Management. [3]

UTM или Unified Threat Management – это многофункциональный программно-аппаратный комплекс, в котором совмещены функции таких устройств, как: межсетевой экран, система обнаружения вторжений, антивирусный шлюз и т. д. [4]

Типичная архитектура UTM-системы изображена на схеме (рис. 1).

Чаще всего UTM-системы выступают в роли шлюза безопасности. В таком случае сетевой трафик из внутренней локальной сети проверяется каждой подсистемой, а центральная консоль управления позволяет администрировать устройство, как полноценное сетевое оборудование. [5]

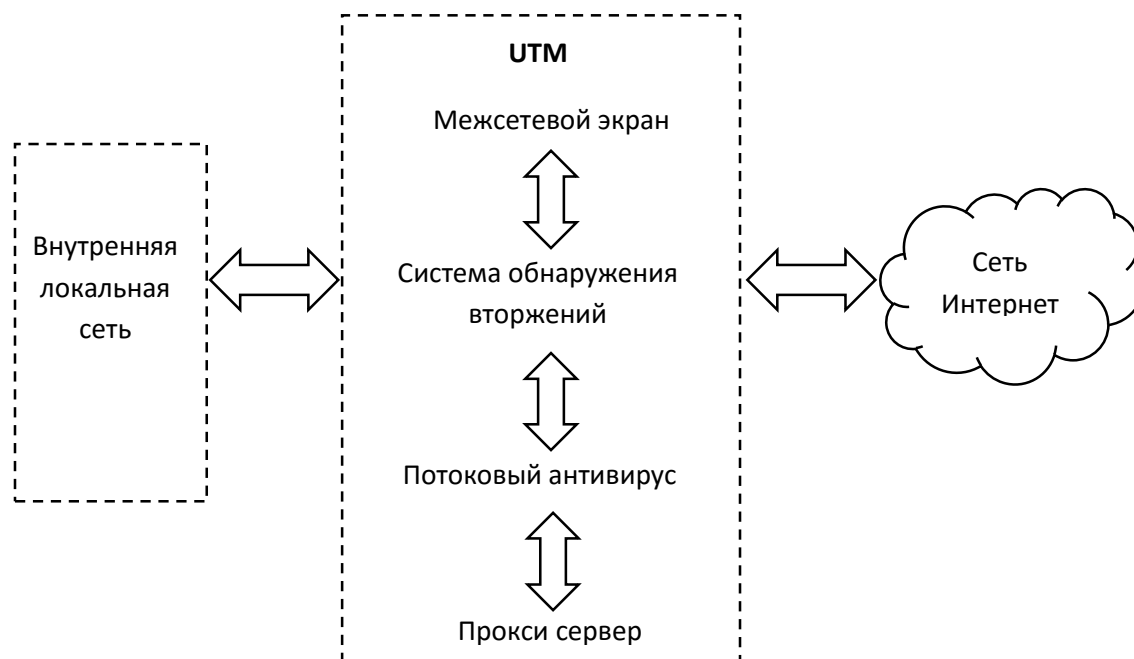


Рисунок 1 – Структура UTM-системы

Вывод

Большинство проблем в области ИБ КС ИИ связаны с отсутствием современного подхода к противодействию УБИ КВО. В данной статье приведен формальный способ определения потенциального нарушителя и актуальных УБИ, а также, приведен новый класс устройств, позволяющих решить ряд проблем, связанных с противодействием УБИ в КС ИИ. В дальнейшей работе будет разработана система класса UTM, направленная на противодействие актуальным угрозам в КС ИИ.

Литература

1. Кирсанов С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли // Управление, вычислительная техника и информатика, 2013. С. 112.
2. Добротун Е.Б. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя // Программные продукты и системы, 2016. №3 (29). С. 42.
3. Комаров А.В. Специализированные устройства против UTM – битва проиграна? // Защита информации. Инсайд, 2011. №4 (40). С. 64.
4. E. Tittel Unified Threat Management For Dummies: John Wiley & Sons, Inc., 2012.
5. Шивдяков Л.А. Проблемы обеспечения информационной безопасности в ключевых системах информационной инфраструктуры органов государственного управления. Модель угроз безопасности информации в КС ИИ // Безопасность информационных технологий, 2009. №1. С. 82

Научный руководитель: Троицкий Игорь Иванович, к. т. н., зам. зав. кафедры ИУ8 по научной работе МГТУ им. Н.Э. Баумана, email: iitroickiy@mail.ru

Determination of Actual Threats in Crucial Objects and Opposition to It

Aleshin V.V.²

In this article, a state review of the security issues of critical information infrastructure systems was conducted, the methodology for the construction of the violator model and threat model in such systems was given, as well a relevant of using devices of Unified Threat Management class to deal with actual threats in crucial objects was proved.

Keywords: APCS, critical objects, threat model, violator model

УДК 681.326

Противодействие несанкционированному доступу в операционной системе Android

Авдеев В.С.³

ОС Android за небольшой промежуток времени стала одной из самых популярных систем для всевозможных мобильных устройств. Ее используют как крупные производители с мировым именем, так и небольшие компании. Данная статья посвящена анализу существующих решений в области защиты мобильных устройств, анализу алгоритмов управления доступом. Описаны программные и аппаратные требования для функционирования мобильной программы в операционной системе Android, определена математическая постановка задачи.

Ключевые слова: защита, Android, алгоритм

Введение. На современном этапе развития все более активно в повседневную деятельность внедряются различные мобильные устройства. Уже несколько лет рынок мобильных устройств занимает лидирующие позиции по количеству пользователей, превосходя рынок персональных компьютеров. Учитывая возможности современных мобильных устройств перед разработчиками встают новые вопросы и проблемы в области обеспечения информационной безопасности. Для достижения этих целей мобильные устройства необходимо защищать от самых разных угроз. Данная статья содержит анализ существующих решений в области управления метками безопасности мобильных приложений в операционной системе Android, анализ программных и аппаратных требований для функционирования мобильной программы в операционной системе Android. Конструкторская часть содержит в себе выбор аппаратной платформы и программного обеспечения, для которого будет предназначаться разрабатываемая система, описана математическая постановка дипломного проекта, описана разработка алгоритма управления мобильного приложения в операционной системе Android.

Обзор существующих решений. Популярность использования мобильных устройств требует больших ресурсов для управления настройками и обеспечения информационной безопасности. Разработанные для управления инфраструктурой мобильных устройств Mobile Device Management системы задают настройки соответствия политикам безопасности и настройки доступа в корпоративную сеть для всех одобренных мобильных устройств. При этом с их помощью осуществляется регистрация и мониторинг устройств, а, в случае потери или кражи смартфона или планшета, с помощью MDM с него можно

² Aleshin Vyacheslav, Bauman MSTU, Moscow, v.nishela@gmail.com

³ Авдеев Валентин Сергеевич, МГТУ им.Н.Э.Баумана, Москва, milhen08@gmail.com

удалить конфиденциальные либо все данные. Сейчас все больше компаний стараются обеспечивать подобную защиту мобильных устройств своих работников. Поэтому активно используется подход user agreement: если пользователь хочет использовать корпоративные ресурсы, ему необходимо соответствовать определенным требованиям. Рассмотрим на примере уже существующие MDM-решения от иностранного и российского разработчиков:

1. McAfee Enterprise Mobility Management

Компания McAfee, входящая в состав Intel Security, является крупнейшей в мире компанией, специализирующейся на разработке технологий безопасности. Функциональные возможности:

- Центральная веб-консоль для различных операционных систем;
- Учет устройств и управление ими;
- Конфигурация устройств;
- Политика шифрования (телефон, карта памяти);
- Блокировка безопасности (фотокамера, карта памяти, Bluetooth, Wi-Fi);
- Принудительное использование паролей;
- Удаленная блокировка и стирание данных;
- Самообслуживание конечных пользователей.

2. Safe Phone

Safe Phone является решением Mobile Device Management (MDM) и предназначено для защиты от несанкционированного доступа (НСД) к информации, хранящейся и обрабатываемой на корпоративных смартфонах и планшетах, а также для централизованного управления данными устройствами. Функциональные возможности:

- Функции защиты осуществляются с помощью установленного на мобильное устройство приложения SafePhoneClient, которое пользователь не может ни остановить, ни удалить.

- Дистанционный контроль попыток инсталляций/деинсталляций программного обеспечения на мобильном устройстве.

- Ведение банка доверенных приложений и невозможности установки приложений из других источников.

- Дистанционное блокирование мобильного устройства.

- Дистанционное удаление данных, с перезаписью областей памяти, содержащих удаляемую информацию.

- Возможность дистанционного запрета на использование опасных интерфейсов связи, например, Bluetooth, Wi-Fi, цифровая фотокамера, микрофон.

- «Тревожная кнопка» для скрытного информирования с мобильного устройства об угрозе физического нападения или о работе под принуждением.

- Взаимодействие между мобильным устройством и сервером SafePhone осуществляется посредством защищённого VPN, работающего поверх беспроводных интерфейсов Wi-Fi или GPRS (в интеграции с решениями сторонних производителей).

Основные угрозы и уязвимости информационной безопасности мобильных устройств под управлением ОС Android:

Использование недоверенных мобильных устройств. Сегодня в мобильных устройствах не реализованы технологии «корня доверия» (root of trust), например, модули Trusted Platform Module, (TPM), которые все чаще встраиваются в ноутбуках и рабочих станциях. К тому же нередко встречаются такие действия, как «rooting» мобильных устройств, свидетельствующие о том, что встроенные ограничения по безопасности, используемые операционной системой можно обойти.

Использование недоверенных сетей. Поскольку мобильные устройства используют для доступа в интернет внешние каналы связи, пользователь обычно не может

контролировать безопасность используемых устройств сетей. В их число могут входить широкополосные сети, в том числе кабельные и беспроводные, например, Wi-Fi или сотовые сети. Эти системы связи не защищены от перехвата данных, что создает риск кражи конфиденциальной информации с целью перехвата и модифицирования сообщений.

Риски, возникающие при использовании недоверенных сетей, можно уменьшить, применяя технологии шифрования (например, VPN), а также с помощью механизмов взаимной аутентификации для проверки подлинности обеих сторон.

Использование недоверенных приложений. Мобильные устройства позволяют легко находить, приобретать, устанавливать и использовать приложения сторонних разработчиков из магазинов мобильных приложений. Это создает очевидные риски, особенно для платформ и магазинов приложений, не накладывающих на приложения ограничений, обусловленных требованиями безопасности, или иных условий.

Риск, связанный с этими приложениями, можно уменьшить несколькими способами. Можно запретить установку посторонних приложений, создать «белый список» для допуска к установке только доверенных приложений, проверять, что приложение имеет только необходимый доступ к ресурсам мобильного устройства, или реализовать безопасную программную среду, которая изолирует конфиденциальные данные от прочих данных и приложений на мобильном устройстве.

Взаимодействие с другими системами. Мобильные устройства могут взаимодействовать с другими системами в рамках обмена данными и хранения данных. Взаимодействие с локальной системой чаще всего подразумевает соединение мобильного устройства со стационарным компьютером или ноутбуком по беспроводному каналу или через кабель для зарядки и/или синхронизации. В момент синхронизации устройств злоумышленник может перехватить конфиденциальную информацию.

Троянские программы. В зависимости от семейства, эти вредоносные программы обладают широким функционалом. Чтобы реализовать возможность установки приложений, не вызывая подозрений со стороны пользователя, троянцам необходимы права root, которые в ОС Android можно получить, установив стороннюю прошивку на мобильное устройство.

Программные и аппаратные требования

Основную информацию о программе в системе предоставляет файл манифеста *AndroidManifest.xml*. Каждое приложение должно иметь свой файл *AndroidManifest.xml*. Назначение файла:

- объявляет имя Java-пакета приложения, который служит уникальным идентификатором;
- описывает компоненты приложения — деятельности, службы, приемники широковещательных намерений и контент-провайдеры, что позволяет вызывать классы, которые реализуют каждый из компонентов, и объявляет их намерения;
- содержит список необходимых разрешений для обращения к защищенным частям API и взаимодействия с другими приложениями;
- объявляет разрешения, которые сторонние приложения обязаны иметь для взаимодействия с компонентами данного приложения;
- объявляет минимальный уровень API Android, необходимый для работы приложения;
- перечисляет связанные библиотеки.

Версия операционной системы

Устройства могут поддерживать разные версии ОС Android. Каждая последующая версия системы часто дополняется новыми функциями API, которые недоступны в предыдущих версиях системы. Для определения набора доступных функций API каждой

версии ОС соответствует уровень API. Например, Android 1.0 – это 1-й уровень API, а Android 5.0 – это 20-й уровень. Каждая последующая версия ОС Android обеспечивает совместимость для приложений, которые были составлены с помощью функций API предыдущих версий, то есть мобильное приложение всегда будет совместимо с будущими версиями ОС Android.

Вывод

В результате были проанализированы существующие угрозы и уязвимости в ОС Android, проведен обзор версий операционной системы и рассмотрены аппаратные и программные требования для функционирования мобильной программы в ОС Android.

На основании анализа выявлено, что основными угрозами противодействия несанкционированного доступа являются использование недоверенных приложений, что может привести к несанкционированному доступу в устройство, троянские программы, эта угроза является следствием недоверенных программ.

Литература

1. Михайлов С.Ф., Петров В.А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие М.: МИФИ, 1995. 192 с.
2. Мельникова О.В., Смартфоны на Android Москва, 2013. - 304 с.
3. Список уязвимостей ОС Android. Система известных уязвимостей: [Электронный ресурс] / MITRE corp.
4. Роджерс Рик, Ломбардо Джон, Медникс Зигурд, Мейк Блейк Android. Разработка приложений-Москва, 2010. - 400 с.
5. Левин А.А. Android на планшетах и смартфонах 2013. - 224 с.

Научный руководитель: *Медведев Николай Викторович, доцент кафедры ИУ-8 МГТУ им. Н.Э.Баумана, к.т.н., доцент, medvedevnick54@yandex.ru*

Unauthorized Access Opposition in Android OS

Avdeev V.

Android OS for a small period became one of the most popular systems for various mobile devices. It is used both large producers with a world name, and the small companies. This article is devoted to the analysis of the existing decisions in the field of protection of mobile devices, to the analysis of control algorithms by access. Program and hardware requirements for functioning of the mobile program in the Android operating system are described, mathematical problem definition is defined.

Keywords: Protection, Android, algorithm.

УДК 519.1

Признак наличия петель в заданном множестве вершин ориентированного графа

Авезова Я.Э.⁴, Фомичёв В.М.⁵

Исследован признак наличия петель в заданном множестве вершин в циклической полугруппе ориентированных графов, получены оценки и формула для вычисления показателя данного признака, выраженные через длины контуров орграфа, образующего данную полугруппу. Результаты позволяют уточнить оценки экспонентов некоторых примитивных систем орграфов

⁴ Авезова Я.Э., ЗАО «НПО «Эшелон», г.Москва, avezovayana@gmail.com

⁵ Фомичёв В.М., д-р ф.-м. н., проф., Финансовый университет при Правительстве Российской Федерации, г. Москва, fomichev.2016@yandex.ru

и существенно расширяют область систем орграфов, для которых удастся получить оценки экспонентов.

Ключевые слова: признак, показатель признака, примитивность системы орграфов, экспонент системы орграфов.

Введение

Исследование характеристик примитивности орграфов и систем орграфов является важным направлением анализа криптографических систем, реализуемого в рамках матрично-графового подхода к определению существенных переменных криптографических функций. Прикладное значение исследований направлено на получение оценок стойкости блочных шифров и генераторов гаммы относительно атак типа последовательного опробования частей ключа. Другим важным направлением приложений является исследование функций, распространяющих искажения и используемых в системах аутентификации.

Одной из решаемых задач является определение экспонента системы орграфов $\hat{\Gamma} = \{\Gamma_1, \dots, \Gamma_m\}$, обозначаемого $\text{exp } \hat{\Gamma}$ (для экспонента системы матриц соответствующее определение дано в [1, 2]). Один из возможных способов получения оценки $\text{exp } \hat{\Gamma}$ основан на построении примитивного орграфа Γ' , являющегося словом в алфавите $\hat{\Gamma}$ (то есть элемента полугруппы $\langle \hat{\Gamma} \rangle$), и оценке $\text{exp } \Gamma'$ в соответствии с универсальным критерием примитивности [3,4]: орграф Γ' примитивный $\Leftrightarrow$ сильно связный и содержит множество простых контуров взаимно простых длин.

Условие примитивности орграфа Γ' выполнено, в частности, при наличии петель в определенном подмножестве вершин орграфа Γ_j^t при некотором $j \in \{1, \dots, m\}$ и некотором натуральном t . Пример такой системы $\hat{\Gamma}$ из двух графов рассмотрен в [5]. Настоящая работа посвящена получению оценок показателя признака, связанного с наличием петель в заданном подмножестве вершин.

1. Понятие признака. Признак наличия петель в заданном подмножестве вершин орграфа. Подмножество H полугруппы G , состоящее из всех элементов G , обладающих определенным свойством, называется признаком H (H -признаком) в полугруппе G [1, с.178]. Если $H \leq G$ — подполугруппа, то H называется полугрупповым признаком в G . Признак H называется наследственным, если из включения $g \in H$ следует, что $\langle g \rangle \subseteq H$.

Пусть G — полугруппа орграфов с множеством вершин $V = \{1, \dots, n\}$, $\emptyset \neq P \subseteq V$. В полугруппе G наследственным полугрупповым признаком (обозначим его P_{loop}) является, в частности, множество всех орграфов, имеющих петли в каждой вершине множества P .

Пусть $\Gamma \in G$, обозначим $\langle \Gamma \rangle$ циклическую полугруппу, порожденную орграфом Γ . Показателем P_{loop} -признака в полугруппе $\langle \Gamma \rangle$ называется наименьшее натуральное t , при котором $\Gamma^t \in P_{loop}$ (обозначается l_P).

Утверждение 1. Признак P_{loop} в полугруппе $\langle \Gamma \rangle$ не пуст $\Leftrightarrow$ каждая вершина из P является циклической.

2. Оценки показателя признака наличия петель в заданном подмножестве вершин орграфов. Рассмотрим орграф Γ , все вершины которого из подмножества P являются циклическими. Обозначим в Γ : $\hat{C} = \{C_1, \dots, C_k\}$ — множество k простых контуров; $l(C)$ — длина контура C , $V(C)$ — множество вершин контура C ; $L(i)$ — множество длин контуров, проходящих через вершину i ; $L^{[m]}(i)$ — множество не превосходящих

натурального числа m длин контуров, проходящих через вершину i ; $\Lambda(i)$ — множество длин простых контуров, проходящих через вершину i ; $C_{\min,i}$ — кратчайший простой контур, проходящий через вершину i , $i \in V$.

Утверждение 2. Показатель признака P_{loop} определяется равенством:

$$l_P = \min_{i \in P} \bigcap L(i). \quad (1)$$

Доказательство. Заметим, что $\lambda \in \bigcap_{i \in P} L(i) \Leftrightarrow$ через любую вершину множества P проходит контур длины λ , в этом случае орграф Γ^λ имеет петли в вершинах множества P . Следовательно, по определению показателя признака $l_P = \min_{i \in P} \bigcap L(i)$. ■

Поскольку через каждую вершину $i \in P$ проходит бесконечно много контуров, применение (1) для вычисления точного значения показателя признака P_{loop} затруднительно. Чтобы для определения l_P число вычислительных операций было конечным, получим ряд оценок величины l_P .

Для последовательности $w_1, \dots, w_m$, $m > 1$, непустых путей определен путь w с помощью операции конкатенации, обозначаемой символом $\bullet$, если конечная вершина предыдущего пути совпадает с начальной вершиной следующего пути, то есть $w = w_1 \bullet \dots \bullet w_m$. Также обозначим: $w(i, j)$ — путь из вершины i в вершину j ; $\text{len}(w)$ — длина пути w . Если $w = w_1 \bullet \dots \bullet w_m$, то $\text{len}(w) = \text{len}(w_1) + \dots + \text{len}(w_m)$.

Контуры C и C' назовем смежными в орграфе Γ (обозначается $C \sim C'$), если в Γ есть вершина, через которую проходят оба контура. Систему контуров $\hat{C} = \{C_1, \dots, C_k\}$ назовем связной в орграфе Γ , если связной является часть графа Γ , совпадающая с $C_1 \cup \dots \cup C_k$.

Лемма 1. Пусть орграф Γ содержит связную систему контуров $\hat{C} = \{C_1, \dots, C_k\}$, $k \geq 1$. Тогда в Γ имеется контур длины $l(\hat{C}) = l(C_1) + \dots + l(C_k)$, обходящий однократно каждый контур системы $\hat{C}$.

Доказательство (индукция по числу контуров связной системы). При $k=1$ утверждение тривиально. Пусть орграф Γ имеет связную систему из $k=2$ контуров C_1 и C_2 длины l_1 и l_2 , где $C_1 \sim C_2$ и i — общая вершина контуров C_1 и C_2 . Тогда искомым контур C есть $C_1(i) \bullet C_2(i)$ и $\text{len} C = l_1 + l_2$.

Докажем лемму при любом $k \geq 2$ для орграфа Γ , имеющего связную систему $\hat{C}$ из k контуров. Предположим, что теорема выполнена в Γ для любой связной системы из меньшего количества контуров. Рассмотрим произвольный контур системы $\hat{C}$, обозначим его C_1 . Поскольку C_1 принадлежит связной системе контуров, C_1 смежный хотя бы с одним из остальных контуров орграфа Γ . Обозначим C_2 любой из смежных с C_1 контуров. Тогда либо C_1 , либо C_2 смежен хотя бы с одним из остальных контуров орграфа Γ (обозначим любой из таких контуров C_3). Продолжая рассуждения аналогичным образом, построим множество $\{C_1, \dots, C_{k-1}\}$ контуров, образующих часть орграфа Γ . Система контуров $\{C_1, \dots, C_{k-1}\}$ связная по построению. Тогда по предположению индукции в Γ существует контур C' длины $l_1 + \dots + l_{k-1}$, однократно обходящий каждый из контуров $C_1, \dots, C_{k-1}$. Не вошедший в множество $\{C_1, \dots, C_{k-1}\}$ контур системы $\hat{C}$ (обозначим его C_k) по условию смежен хотя бы с одним из контуров $C_1, \dots, C_{k-1}$, значит $C_k \sim C'$. Тогда по предположению индукции в Γ существует контур C длины $l + l_{k+1}$, обходящий однократно контуры C' и C_k . ■

Введем ряд определений, позволяющих сформулировать оценку показателя l_P , являющуюся прямым следствием леммы 1. Запишем, что система контуров

$\hat{C}=\{C_1,\dots,C_k\}$ содержит множество P , если $P\subseteq V(C_1)\cup\dots\cup V(C_k)$. Связную систему контуров, содержащую множество P , назовем P -сокращенной, если после удаления любого контура оставшаяся подсистема либо не является связной, либо не содержит множество P . P -сокращенную систему $\hat{C}=\{C_1,\dots,C_k\}$ назовем минимальной в Γ , если сумма длин её контуров принимает наименьшее значение. Заметим, что P -сокращенных и минимальных систем в орграфе Γ может быть несколько. Далее полагаем $P=\{1,\dots,p\}$.

Теорема 1. Если в орграфе Γ связная система контуров $\hat{C}=\{C_1,\dots,C_k\}$ содержит множество P , то верны оценки:

$$\max\{l(C_{\min,i}): i\in P\}\leq l_P(\hat{C}). \quad (2)$$

Доказательство. По лемме 1, через любую вершину из P проходит контур длины $l_1+\dots+l_k$. Следовательно, $\bigcap_{i\in P} L(i)\neq\emptyset$ и $\min_{i\in P} \bigcap_{i\in P} L(i)\leq l_1+\dots+l_k$. По утверждению 2 $l_P=\min_{i\in P} \bigcap_{i\in P} L(i)$, тогда $\max\{l_{C_{\min}(i)}: i\in P\}\leq l_P$, так как $l_{C_{\min}(i)}\leq \min_{i\in P} \bigcap_{i\in P} L(i)=l_P$ для любой вершины $i\in P$. ■

Верхняя оценка (2) принимает наименьшее значение, если система $\hat{C}$ P -сокращенная и минимальная.

Теорема 2. Для любого разбиения множества $P=P_1\cup\dots\cup P_r$ выполнено:

$$l_P\leq \text{НОК}(l_{P_1},\dots,l_{P_r}). \quad (3)$$

Доказательство. Следует из определения показателя признака P_{loop} и свойств наименьшего общего кратного. ■

Следствие 1 (для минимального разбиения множества P). Верна оценка:

$$l_P\leq \min\{\text{НОК}\{(\lambda_1,\dots,\lambda_p)\in\Lambda(1)\times\dots\times\Lambda(p)\}\}. \quad (4)$$

Доказательство. Если $\lambda\in\Lambda(i)$, то $\lambda N\subseteq L(i)$, $i=1,\dots,p$. Тогда $\theta N\subseteq L(1)\cap\dots\cap L(p)$ при $\theta=\text{НОК}(\lambda_1,\dots,\lambda_p)$ и при любом наборе $(\lambda_1,\dots,\lambda_p)\in\Lambda(1)\times\dots\times\Lambda(p)$. По утверждению 2, $l_P=\min\{L(1)\cap\dots\cap L(p)\}$, где $\min\{L(1)\cap\dots\cap L(p)\}\leq\theta$. Следовательно, нужная оценка верна. ■

Оценка (4) позволяет уточнить (1) с помощью замены бесконечных множеств конечными.

Следствие 2. При $m=\min\{\text{НОК}\{(\lambda_1,\dots,\lambda_p)\in\Lambda(1)\times\dots\times\Lambda(p)\}\}$ выполнено:

$$l_P=\min_{i\in P} \bigcap_{i\in P} L^{[m]}(i). \quad (5)$$

Уточним оценку (5) с использованием верхней оценки (2).

Следствие 3. Если в Γ связная система контуров $\hat{C}=\{C_1,\dots,C_k\}$ содержит множество P , то формула (5) верна при $m=\min\{l(\hat{C}), \min\{\text{НОК}\{(\lambda_1,\dots,\lambda_p)\in\Lambda(1)\times\dots\times\Lambda(p)\}\}\}$.

Следствие 4. Пусть орграф Γ содержит компоненты сильной связности $\Gamma_1,\dots,\Gamma_r$ с множествами вершин $V_1,\dots,V_r$ соответственно и $P_i=P\cap V_i$, $i=1,\dots,r$, тогда верна оценка (3).

Пример. Определение показателя признака P_{loop} .

Пусть граф Γ (рис. 1) состоит из компонент сильной связности Γ_1 и Γ_2 . Компонента сильной связности Γ_1 есть связная система простых контуров $C_1=(1,2,3)$, $C_2=(3,4)$ и $C_3=(4,5,6,7,8)$ длины 3, 2 и 5 соответственно. Компонента сильной связности Γ_2 есть связная система простых контуров $C_4=(9,10)$, $C_5=(10,11)$ и $C_6=(10,11,12)$ длины 2, 2 и 3 соответственно.

Для орграфа Γ при некоторых P посчитаны оценки показателя l_P с помощью оценок (2) и (4) (таблицы 1, 2), а также точное значение показателя l_P (таблица 3) с помощью (5) или следствия 3.

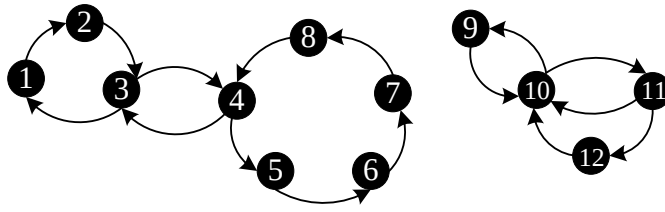


Рис. 1. Орграф Γ

Таблица 1

Верхняя оценка (2) показателя l_P для различных множеств P

P	Минимальная связная система, содержащая P	Оценка (2)
$\{1,5\}$	$\{C_1, C_2, C_3\}$	$l_P \leq 3+2+5=10$
$\{1,4\}$	$\{C_1, C_2\}$	$l_P \leq 3+2=5$
$\{9,11\}$	$\{C_4, C_5\}$	$l_P \leq 2+2=4$

Таблица 2

Верхняя оценка (4) показателя l_P для различных множеств P

P	$\Lambda(i), i \in P$	Оценка (4)
$\{1,5\}$	$\Lambda(1)=\{3\}, \Lambda(5)=\{5\}$	$l_P \leq \text{НОК}(3,5)=15$
$\{1,4\}$	$\Lambda(1)=\{3\}, \Lambda(4)=\{2,5\}$	$l_P \leq \min\{\text{НОК}(3,2), \text{НОК}(3,5)\}=6$
$\{9,11\}$	$\Lambda(9)=\{2\}, \Lambda(11)=\{2,3\}$	$l_P \leq \min\{\text{НОК}(2,2), \text{НОК}(2,3)\}=2$
$\{1,4,9,11\}$	$\Lambda(1)=\{3\}, \Lambda(4)=\{2,5\}, \Lambda(9)=\{2\}, \Lambda(11)=\{2,3\}$	$l_P \leq \min\{\text{НОК}(3,2,2,2), \text{НОК}(3,5,2,2), \text{НОК}(3,2,2,3), \text{НОК}(3,5,2,3)\}=6$

Таблица 3

Показатель l_P для различных множеств P , посчитанный с помощью (5)

P	m	$L^{[m]}(i), i \in P$	l_P (5)
$\{1,5\}$	10	$L^{[10]}(1)=\{3,5,6,7,8,9,10\}, L^{[10]}(5)=\{5,7,9,10\}$	$l_P = \min L^{[10]}(1) \cap L^{[10]}(5) = 5$
$\{1,4\}$	5	$L^{[5]}(1)=\{3,5\}, L^{[5]}(4)=\{2,4,5\}$	$l_P = \min L^{[5]}(1) \cap L^{[5]}(4) = 5$
$\{9,11\}$	2	$L^{[2]}(9)=L^{[2]}(11)=2$	$l_P = 2$
$\{1,4,9,11\}$	6	$L^{[6]}(1)=\{3,5,6\}, L^{[6]}(4)=\{2,4,5,6\}, L^{[6]}(9)=\{2,4,5,6\}, L^{[6]}(11)=\{2,3,4,5,6\}$	$l_P = \min\{5,6\}=5$

Из таблиц 1-3 следует, что для $P=\{1,5\}$ и $P=\{1,4\}$ оценка (2) точнее оценки (4), а для $P=\{9,11\}$ соотношение обратное. Для $P=\{1,4,9,11\}$ с помощью следствия 3 получаем оценку $l_P \leq \text{НОК}(2,5)=10$; величина оценки (4) более точная (см. таблицу 2), но превышает точное значение, посчитанное в таблице 3.

Выводы

Результаты показывают, что в некоторых случаях оценки (2) и (4) достижимы. Для многих орграфов с большим числом вершин сложность вычисления оценок показателя l_p по предварительным оценкам меньше, чем сложность определения точного значения. Однако для вычисления по формуле (5) точного значения l_p следует вычислить параметр m , являющийся верхней оценкой l_p , и затем построить пересечение множеств $L^{[m]}(1), \dots, L^{[m]}(p)$.

Перспективное направление дальнейших исследований P_{loop} -признака связано с алгоритмическими вопросами вычисления показателя признака в полугруппе $\langle \Gamma \rangle$.

Доказанные оценки показателя P_{loop} -признака могут быть использованы для оценки экспонентов некоторых примитивных систем орграфов. Полученные результаты существенно расширяют область систем орграфов, для которых удастся получить оценки экспонентов.

Литература

1. Фомичев В.М. Методы дискретной математики в криптологии. — М.: Диалог-МИФИ, 2010. — 424 с.
2. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты. — М.: Издательство Юрайт, 2016. — 209 с.
3. Сачков В.Н. Комбинаторика неотрицательных матриц / В.Н. Сачков, В.Е. Тараканов. — М.: ТВП, 2000. — 448 с.
4. К.Г. Когос, В.М. Фомичев. Положительные свойства неотрицательных матриц // Прикладная дискретная математика, №4(18), 2012. — С. 116-121.
5. Я.Э. Аvezова, В.М. Фомичев. Условия примитивности системы двух графов // Прикладная дискретная математика. Приложение, № 8, 2015. — С.113–114.

The Character of Loops at the Given Vertex Set of Directed Graph

Avezova Y.⁶, Fomichev V.⁷

This paper presents the results of loop existing research at the given vertex subset in cyclic semigroup of digraphs named as loop-character. Formula and some bounds for the loop-character index are obtained by circuits lengths of digraph — the generator of the cyclic semigroup. The results can be used for some exponents evaluation of digraph system.

Keywords: loop-character, index of loop-character, primitiveness of digraph system, exponent of digraph system.

⁶ Avezova Y. NPO Echelon, Moscow, avezovayana@gmail.com

⁷ Fomichev V. Dr. Sc. (Phys.-Math.), Professor, Financial University under the Government of the Russian Federation, Moscow, efomichev.2016@yandex.ru

Разработка алгоритма стеганографической передачи информации Бакеренков П.С.⁸

В работе был смоделирован процесс скрытой передачи данных злоумышленнику, разработан принцип скрытой передачи информации, основанный на использовании журнала Интернет-ресурсов. Алгоритм работы программы, в соответствии с которым происходит передача кодированной информации, представляет собой новый подход к скрытой передаче информации. Был успешно проведен ряд экспериментов по скрытой передаче информации и разработаны методические рекомендации по снижению рисков реализации скрытой передачи информации.

Ключевые слова: скрытый канал, статистический скрытый канал

1. Введение

Современные информационные системы невозможно представить без разного рода сетей, от простейших локальных до автоматизированных распределенных глобальных. Важнейшим элементом работы сети является передача информации между адресатами. Попытки скрыть факт передачи информации изучает наука стеганография, которая находит свои корни задолго до появления информационных систем. Чтобы выделить методы стеганографии, используемые в современных информационных системах, опирающихся на электронном представлении данных, появился термин компьютерная стеганография. Впервые понятие скрытого канала было использовано в работе Батлера Лэмпсона в 1973 году. Скрытый канал — это коммуникационный канал, пересылающий информацию методом, который изначально был для этого не предназначен.

В среде операционных систем невозможно отделить один процесс от эффектов, которые провоцирует другой процесс. Процесс-отправитель создает скрытый канал, который резервирует некоторое состояние (дисковое пространство, доступность ресурса и др.), зарегистрированное злоумышленником.

2. Моделирование скрытого канала, основанного на статистическом методе

Статистический скрытый канал использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями. Скрытость таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем инспектор, не имеющий знаний о структуре сообщений.

Интерпретированная модель функционирования скрытого канала представлена на рис. 1.

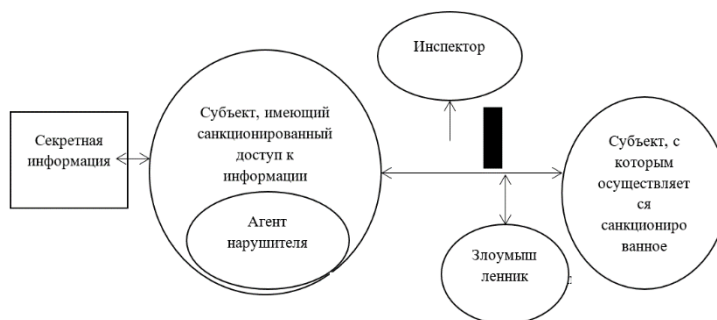


Рисунок 1 - Интерпретированная модель функционирования скрытого канала

⁸ Бакеренков Павел Сергеевич, МГТУ им. Н.Э. Баумана, Москва, b.p.s.iu8@gmail.com

Для разработки программы, реализующей передачу информации с использованием статистического скрытого канала, смоделируем процесс передачи информации с использованием статистического скрытого канала. Пусть агент злоумышленника и злоумышленник знают некоторый секретный ключ. Сформулируем некоторые вводные параметры передачи информации с использованием скрытого статистического канала:

1. n -длинна передаваемого сообщения;
2. $\{ts_1, \dots, ts_n\}$ - время передачи сообщения;
3. δ -интервал передачи информации;
4. $C > 0$ – константа.

Пусть S_i - позиции, t_j – переходы процесса. Для модели статистического скрытого канала имеем:

- S_1 — агент злоумышленника получил информацию ограниченного доступа;
- t_1 — агент злоумышленника формирует специальную последовательность исходящих пакетов из информации ограниченного доступа;
- S_2 — сформированы пакеты $V_1, \dots, V_n$, адресованные санкционированному пользователю вне сети;
- t_2 — злоумышленник путем перехвата пакетов отслеживает какие пакеты проходят через него в каждый момент времени $[ts_i, ts_i + \delta)$, $i=1, n$;
- S_3 — злоумышленник ожидает получения пакетов с информацией ограниченного доступа и отслеживает входящий трафик;
- t_3 — с целью отслеживания пакетов злоумышленник вычисляет следующие величины:

$$\vartheta(V_{j_1}) = \sum_{i=1}^n I\{V_{j_1} \in [ts_i, ts_i + \delta)\},$$

$$\vartheta(V_{j_2}) = \sum_{i=1}^n I\{V_{j_2} \in [ts_i, ts_i + \delta)\},$$

где $j_1, j_2 \in \{1, N\}$.

S_4 — злоумышленник имеет некоторое правило, согласно которому он обрабатывает полученные вычисления от агента;

t_4 — злоумышленник обрабатывает вычисления по следующим правилам:

если $\vartheta(V_{j_1}) < C \leq \vartheta(V_{j_2})$, то агент злоумышленника передает 1,

если $\vartheta(V_{j_2}) < C \leq \vartheta(V_{j_1})$, то агент злоумышленника передает 0,

в ином случае передача данных по скрытому статистическому каналу отсутствует.

S_5 — зашифрованная критически важная информация проходит проверку у инспектора и попадает к злоумышленнику.

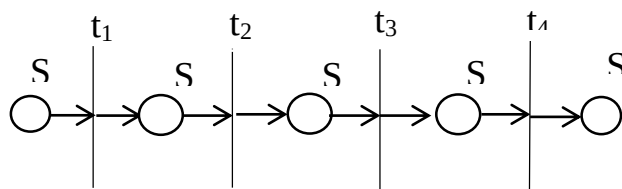


Рисунок 2 -Метод использования статистических скрытых каналов

Для того, чтобы сервер мог отделить наличие передачи данных от нормальной работы сети, необходимо оценить длину эксперимента n .

Если $\vartheta < C$, то происходит нормальная работа сети, скрытой передачи данных нет.

Если $\vartheta \geq C$, идет передача данных по скрытому каналу.

Оценим пропускную способность такого статистического скрытого канала. Пусть в каждый момент времени злоумышленник наблюдает за пакетами, адресованными получателям $V_{i1}, \dots, V_{in}$, $i_1, \dots, i_k \in \{1, N\}$.

Злоумышленником вычисляются следующие величины:

$$\vartheta(V_{ij}) = \sum_{i=1}^n I\{V_{ij} \in [ts_i, ts_i + \delta)\},$$

где $j = \overline{1, k}$.

Разобьем все множество $\{\vartheta(V_{ij})\}$ на два непересекающихся подмножества:

$$C_1 = \{\vartheta(V_{ij}) : \{\vartheta(V_{ij})\} < C, j = \overline{1, k},$$

$$C_2 = \{\vartheta(V_{ij}) : \{\vartheta(V_{ij})\} \geq C, j = \overline{1, k}.$$

Таким образом существует всего C_k^p вариантов разбиения на множества мощности p и $k-p$, существует $\sum_{i=1}^k C_k^p = 2^k$ вариантов разбиения на 2 непересекающихся множества, что соответствует множества E_2^k .

Определим $T = t_n - t_1$ - общее время, необходимое для передачи 1 Кбит информации. В связи с тем, что для поиска одного пакета, адресованного определенному узлу рассматривается интервал $[t_1, t_i + \delta)$, $i \in \{1, \dots, n\}$

$$T \geq \delta n.$$

Тогда для модели передачи 1 Кбит и k Кбит имеем следующую пропускную способность:

$$\varphi = \frac{1}{T} \leq \frac{1}{\delta n},$$

$$\varphi = \frac{k}{T} \leq \frac{k}{\delta n}.$$

Таким образом можно сделать вывод о том, что использование статистического скрытого канала дает малую вероятность возникновения ошибок при приеме информации ограниченного доступа злоумышленником и достаточную пропускную способность для передачи значительных объемов информации. Разработаем статистический скрытый канал, на базе которого будет работать программное обеспечение, реализующее скрытую передачу данных.

3. Разработка и имитационное моделирование скрытого статистического канала

Учитывая экономическую ситуацию в России проблема утечки конфиденциальной (служебной) информации только возрастает. Все это требует пристального внимания администраторов безопасности, а также научного подхода к проблеме.

С целью разработки мероприятий и организационных методов, направленных на повышение защищенности автоматизированной информационной системы, разработаем алгоритм передачи информации с использованием скрытых статистических каналов.

В основе методики лежит разработка собственного уникального алгоритма модификации трафика, который позволяет организовать выделение канала передачи информации через инспектора автоматизированной информационной системы.

К программной реализации алгоритма предъявляются следующие требования:

1. Отказоустойчивость;

2. Надежность передачи данных и хранение секретных ключей;
3. Пропускная способность реализованного канала;
4. Совместимость с различным сетевым оборудованием.

Разработанный алгоритм реализации скрытой передачи данных включает в себя решение следующих задач:

1. Кодировка информации для скрытой передачи в последовательность бит, при условии двухсторонней осведомленности агента злоумышленника и злоумышленника о правилах перевода ключевой информации;
2. Поиск соответствия значений бита передаваемой информации и результата выполнения функции от параметров;
3. Отправка запроса;
4. Дешифрация злоумышленником скрытой информации в конечный вид.

Принцип разработанного нами скрытого канала заключается в посещении программой Интернет-ресурса при совпадении результата работы функции с битом введенной агентом информации. При исполнении данного критерия программа посещает определенную страницу, запись о посещении вносится в журнал регистрации событий Интернет-ресурса. В заранее оговоренный промежуток времени злоумышленник инспектирует журнал событий данного Интернет-ресурса, проводя поиск записей конкретного пользователя. На последнем этапе скрытой передачи злоумышленник собирает информацию из журнала событий и дешифрует ее в конечный вид по заранее оговоренным правилам.

Рассмотрим процесс работы программы более подробно. В разработанной программе предусмотрена возможность ввода информации для скрытой передачи.

Пусть агент злоумышленника имеет санкционированный доступ к ресурсу А и обладает информацией ограниченного доступа. Злоумышленник в свою очередь должен обладать информацией о правилах дешифрации полученных битов информации в конечный вид представления информации. Кроме того, злоумышленник и агент заранее оговаривают конкретный Интернет-ресурс, журнал которого злоумышленник инспектирует в некоторый промежуток времени.

После ввода информации программа кодирует введенные символы в набор битов по следующим правилам:

1. Для букв алфавита задается обозначения ($a = 0, b = 1, v = 2, \dots, y = 32$);
2. Заданные обозначения букв переводятся в двоичный код с добавлением при необходимости нулей до пяти символов.

Так, например, введенные символы "абв" после кодировки примут вид "00000000100010", в котором и будет в дальнейшем обрабатываться информация.

Сформулируем правила, в соответствии с которыми программа определяет необходимость посещения Интернет-ресурса в определенный промежуток времени.

```

//ключевые фразы
$key = array(array(0=> 'вконтакте новости', 1=> 'вконтакте', 2=> 'вк'),
array(0=> 'вконтакте группы', 1=> 'вконтакте мои группы', 2=> 'сообщества Иванова Ивана'),
array(0=> 'вконтакте друзья', 1=> 'вконтакте мои друзья', 2=> 'вконтакте друзья Иванова Ивана'));
//страницы
$url = array(0=> 'vk.com/feed', 1=> 'vk.com/groups', 2=> 'vk.com/friends');
$len = strlen($text);

//загрузка адреса, её размера, связанных с ней ключей, подсчёт суммы всех значений букв
$object = new schanel;
$object->url = $url[0];
$object->size = 15;
$object->keys = $key[0];
$object->calckeysdata();

```

Рисунок 3 - Обработка информации в соответствии с параметрами

Перечислим параметры, участвующие в формировании ключа:

1.Поисковый ключ.

С целью эмуляции поведения пользователя в системе программа подбирает запрос по определенной тематике сайта, по которому:

- 0=> 'вконтакте новости';
- 1=> 'вконтакте';
- 2=> 'вк'.

Программа исследует N страниц сайта и M – число запросов на каждой странице сайта для разработанного нами алгоритма (число запросов может быть задано в произвольном порядке при необходимости). Таким образом, происходит кодирование по следующему правилу 0=а,1=б,2=в и т.д.

Конечным значением поискового ключа будет сумма кодированных букв.

2.Учет времени

Процесс учета времени как параметра для кодирования информации заключается в выборе десятков секунд по причине не мгновенности работы сети Интернет. Так же программа не отправляет запросы при значении единиц секунд более 7, т.к. при возможной задержке веб-ресурс получит другие значения

Размер веб-страницы

Размер веб-страницы также учитывается в конечном кодировании информации.

Таким образом, итоговой формулой формирования ключа для каждого сравнения с битом информации ограниченного доступа является следующая функция

$$f(i) = k_i \times t_i \times N_i,$$

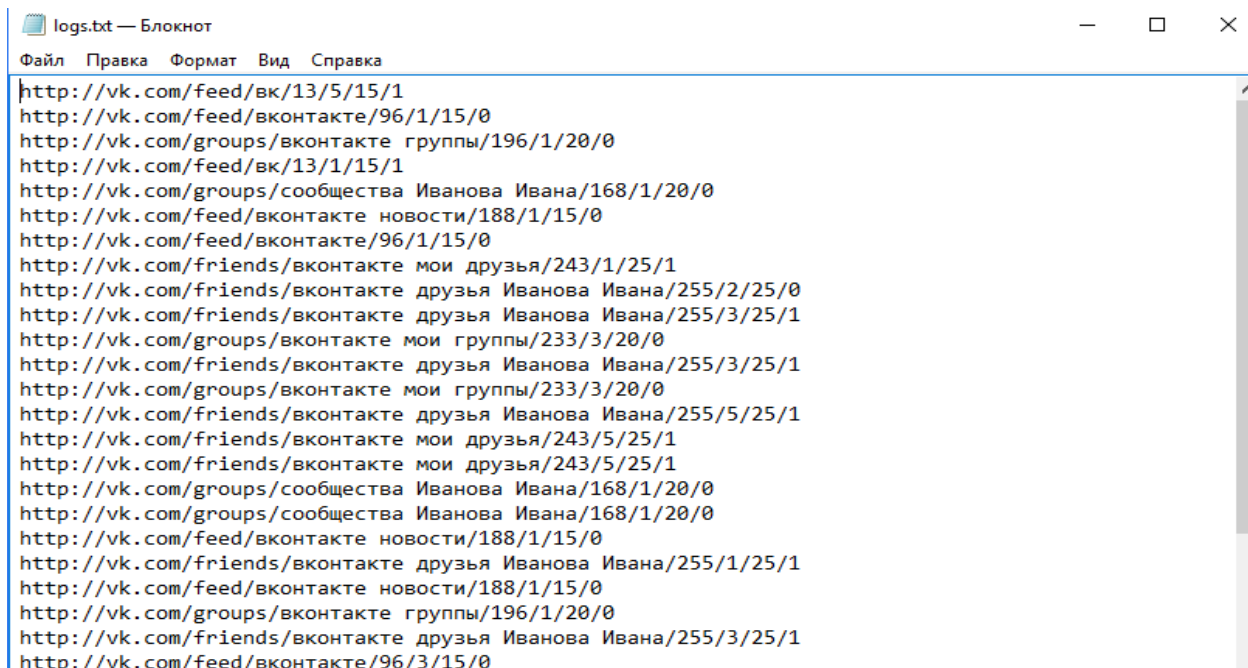
где k – поисковый ключ;

t – время, измеренное в десятках секунд;

N – размер веб-страницы, кб.

После чего производится деление на 2 и по полученному остатку принимается решение о факте посещения страниц сайта при наличии соответствия значения функции $f(i)$ и бита информации ограниченного доступа.

(8)



```
logs.txt — Блокнот
Файл  Правка  Формат  Вид  Справка
http://vk.com/feed/вк/13/5/15/1
http://vk.com/feed/вkontakte/96/1/15/0
http://vk.com/groups/вkontakte группы/196/1/20/0
http://vk.com/feed/вк/13/1/15/1
http://vk.com/groups/сообщества Иванова Ивана/168/1/20/0
http://vk.com/feed/вkontakte новости/188/1/15/0
http://vk.com/feed/вkontakte/96/1/15/0
http://vk.com/friends/вkontakte мои друзья/243/1/25/1
http://vk.com/friends/вkontakte друзья Иванова Ивана/255/2/25/0
http://vk.com/friends/вkontakte друзья Иванова Ивана/255/3/25/1
http://vk.com/groups/вkontakte мои группы/233/3/20/0
http://vk.com/friends/вkontakte друзья Иванова Ивана/255/3/25/1
http://vk.com/groups/вkontakte мои группы/233/3/20/0
http://vk.com/friends/вkontakte друзья Иванова Ивана/255/5/25/1
http://vk.com/friends/вkontakte мои друзья/243/5/25/1
http://vk.com/friends/вkontakte мои друзья/243/5/25/1
http://vk.com/groups/сообщества Иванова Ивана/168/1/20/0
http://vk.com/groups/сообщества Иванова Ивана/168/1/20/0
http://vk.com/feed/вkontakte новости/188/1/15/0
http://vk.com/friends/вkontakte друзья Иванова Ивана/255/1/25/1
http://vk.com/feed/вkontakte новости/188/1/15/0
http://vk.com/groups/вkontakte группы/196/1/20/0
http://vk.com/friends/вkontakte друзья Иванова Ивана/255/3/25/1
http://vk.com/feed/вkontakte/96/3/15/0
```

Рисунок 4—Результат логирования

На последнем этапе реализации разработанной нами скрытой передачи данных программа собирает информацию из журнала событий Интернет-ресурса и дешифрует ее в конечный вид по заранее оговоренным правилам.

По результатам работы программы злоумышленник получает расшифрованную информацию ограниченного доступа.

Таким образом, мы разработали новейшей подход к скрытой передачи информации с использованием статистического канала Интернет-ресурсов. На базе полученной информации по принципам работы скрытого статистического канала и разработанного программного обеспечения, сформулируем организационные методы, позволяющие снизить риск реализации атак с использованием скрытых статистических каналов и повысить эффективность системы безопасности:

1. проверка устанавливаемого программного обеспечения на наличие не декларируемых возможностей обмена данными с Интернет-ресурсами;
2. наличие грамотно настроенной системы защиты, блокирующей активность пользователей, обладающих информацией ограниченного доступа, в сети Интернет;
3. постоянный контроль активностей в сети интернет пользователей, обладающих информацией ограниченного доступа;
4. разработка регламентов обеспечения информационной безопасности с обязательным доведением до всех сотрудников организации.

4. Выводы

В данной статье был смоделирован процесс скрытой передачи данных злоумышленнику, разработан уникальный принцип скрытой передачи информации, основанный на использовании журнала Интернет-ресурсов. Алгоритм работы программы, в соответствии с которым происходит передача кодированной информации, представляет собой новейший подход к скрытой передачи информации и может дополняться разносторонними факторами, учитываемыми при создании скрытого статистического канала. Необходимо отметить, что нами был успешно проведен ряд экспериментов по скрытой передаче информации и разработаны методические рекомендации по снижению рисков реализации скрытой передачи информации в системе.

Список использованных источников

1. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения
2. ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов
3. James J.V Building Higher Resolution Synthetic Clocks for Signaling in Covert Timing Channels [Текст] / J.V. James, D.B. Darby, D.D. Schnachenberg // Proceedings of the Eight IEEE Computer Security Foundations Workshop (CSFW'95). – IEEE 1995. – P. 85-95.
4. Rouland K. – Covert Channels in the TCP/IP Suite 1996. –С. 3-14.
5. Жуков А.Е. Криптоанализ по побочным каналам (SideChannelAttacks) [Текст] / М. Триумф, – 2002. – С. 102-211.

Научный руководитель: Родионов Дмитрий Евгеньевич, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н.Э. Баумана. derodionov@yandex.ru

Development of Algorithm Steganography Information Transfer Bakerenkov P.S.⁹

Abstract. In this paper, the process of secret data handing towards the attacker has been modeled, the principle (it bases on using the log of Internet resources) of secret information transmission has been developed. A new approach for hidden information transmission is the program algorithm according to which the encoded information can be handed. The series of experiments on the secret information transmission has been carried out in the successful way and guidelines on reducing the risk of realization of secret information transmission have been developed.

Keywords: the hidden channel, the statistic hidden channel.

УДК 004.056

Концепция создания информационных систем автоматизации деятельности по анализу уязвимостей программного обеспечения при проведении сертификационных испытаний

Барабанов А.В.¹⁰

Представлено исследование существующих подходов к выполнению анализа уязвимостей программного обеспечения при проведении сертификационных испытаний по требованиям безопасности информации. С учетом особенностей отечественной и зарубежных систем сертификации средств защиты информации разработаны предложения по формированию информационных систем автоматизации процесса поиска известных (подтвержденных) уязвимостей программного обеспечения и автоматизации деятельности экспертов испытательной лаборатории при разработке тестов проникновения.

Ключевые слова: сертификация программного обеспечения, защита информации, анализ уязвимостей.

Введение

Проведение анализа уязвимостей программного обеспечения (ПО) в настоящее время

⁹ Pavel Bakerenkov, Bauman Moscow State Technical University, Moscow, b.p.s.iu8@gmail.com

¹⁰ Барабанов Александр Владимирович, канд. техн. наук, ЗАО «НПО «Эшелон», г. Москва, ab@cnpo.ru

является обязательной активностью экспертов испытательных лабораторий в ходе сертификационных испытаний, выполняемых по линии системы сертификации ФСТЭК России [5]. Данный вид работ выполняется как при сертификации на соответствие требованиям утвержденных ФСТЭК России профилей защиты (ПЗ), в которых в явном виде включены требования семейства доверия «Анализ уязвимостей», так и при испытаниях на соответствие требованиям технических условий [3, 4]. Методология анализа уязвимостей, рекомендуемая ФСТЭК России, заключается в совместном использовании подходов, изложенных в Общей методологии оценки (ГОСТ Р ИСО/МЭК 18045) и международном стандарте ISO/IEC TR 20004, и в общем случае предполагает выполнение следующих шагов [1, 2].

1. Анализ известных (подтвержденных) уязвимостей объекта сертификации. При выполнении данного шага, как правило, осуществляется поиск известных (подтвержденных) уязвимостей в общедоступных источниках информации.

2. Анализ возможности использования (эксплуатации) потенциальных уязвимостей объекта сертификации. При выполнении данного шага определяется перечень потенциальных уязвимостей объекта сертификации и для каждой идентифицированной потенциальной уязвимости разрабатывается и выполняется тест на проникновение.

Поскольку требование по проведению анализа уязвимостей является относительно новым для отечественной системы сертификации, то на текущий момент времени еще не разработаны подробные методические документы, которые могли бы использоваться испытательными лабораториями при проведении анализа уязвимостей. Таким образом, задача разработки и совершенствования методического обеспечения анализа уязвимостей при проведении сертификационных испытаний по требованиям безопасности информации в настоящее время является актуальной.

Цель проведенного исследования состояла в сокращении времени анализа уязвимостей при проведении сертификационных испытаний ПО за счет разработки концепции создания информационных систем автоматизации деятельности по анализу уязвимостей ПО.

Аналитический обзор методов проведения анализа уязвимостей в зарубежных системах сертификации

В ходе исследования был проанализирован опыт зарубежных испытательных лабораторий, проводящих анализ уязвимостей в зарубежных системах сертификации. Напомним, что из-за нововведений в зарубежных системах сертификации отчеты испытательных лабораторий, которые содержат в том числе общие сведения о проведенном анализе уязвимостей, публикуются на официальном сайте систем сертификации. Были проанализированы отчеты испытательных лабораторий за период январь-сентябрь 2016 года (выборка – 33 отчета), опубликованные на сайте NIAP (организации, которая регулирует систему сертификации в США) [3]. Среди проанализированных отчетов большую часть составили отчеты по результатам проведения испытаний на соответствие требованиям ПЗ к сетевым устройствам (19 отчетов). В остальной части отчетов (5 отчетов) были отражены результаты испытаний на соответствие требованиям ПЗ к прикладным программам, операционным системам, средствам управления политиками разграничения доступа и средствам защиты мобильных устройств.

Основные результаты проведенного анализа представлены далее по тексту.

1. В ходе выполнения всех работ выполнялся поиск информации об известных уязвимостях объекта сертификации в общедоступных базах данных. Некоторые испытательные лаборатории выполняли поиск известных уязвимостей не только по ключевым словам, непосредственно связанным с объектом сертификации, но и по идентификационным данным, имеющим отношение к заимствованным компонентам.

2. Только в половине работ испытательные лаборатории выполняли дополнительные тесты на проникновение. В большинстве работ использовался стандартный набор тестов, применимый практически ко всем типам объектов сертификации (например, сканирование сетевых портов). Только в одной работе была представлена информация о проведении тестов на проникновения, основанных на потенциальных уязвимостях объекта сертификации, сформулированных с учетом анализа свидетельства разработчика.

3. Во всех работах, связанных с сертификацией по требованиям ПЗ для сетевых устройств, проводилось фаззинг-тестирование. При этом, как правило, использовались программные средства автоматизации собственной разработки.

4. В своих работах испытательные лаборатории не использовали указания ISO/IEC TR 20004 по формированию перечня потенциальных уязвимостей на основе анализа баз данных CWE и CAPEC. Анализ выполняется только в объеме, соответствующем требованиям ПЗ – дополнительные исследования выполняет только малое число испытательных лабораторий.

Информационные системы автоматизации деятельности по анализу уязвимостей программного обеспечения

По результатам проведенного исследования отечественной и зарубежных систем сертификации были разработаны следующие предложения.

1. Разработка информационной системы автоматизации процесса поиска известных (подтвержденных) уязвимостей ПО. Основными функциональными возможностями системы должны являться:

- возможность поиска известных (подтвержденных) уязвимостей ПО на основе следующих данных: название ПО, номер версии/сборки ПО, характеристики заимствованных компонентов;

- использование Банка данных угроз безопасности информации ФСТЭК России в качестве основного источника известных (подтвержденных) уязвимостей ПО;

- возможность совместного использования информационной системы несколькими экспертами испытательных лабораторий и органов по сертификации.

2. Разработка информационной системы автоматизации деятельности экспертов испытательной лаборатории при разработке тестов проникновения. Предлагаемая к созданию информационная система предназначена для решения следующих задач:

- предоставление заинтересованным лицам информации о потенциальных уязвимостях и шаблонах атак на различные типы ПО [4, 8];

- обучение специалистов в области анализа защищенности: иллюстративный материал (видеоинформация, типовые отчеты), публикуемый в информационной системе, позволит повысить осведомленность специалистов в области анализа уязвимостей [6, 7, 9].

Пополнение перечня шаблонов атак целесообразно выполнять испытательными лабораториями и органами по сертификации, в том числе с учетом результатов анализа уязвимостей, выявленных в сертифицированном ПО.

Потенциальными пользователями предлагаемых к созданию информационных систем являются эксперты испытательных лабораторий, эксперты органов по сертификации. Информационные системы могут быть реализованы в виде веб-приложений, расширяющих функциональные возможности Банка данных угроз безопасности информации ФСТЭК России.

Выводы

В результате проведенного исследования была предложена концепция создания следующих двух информационных систем: информационная система автоматизации процесса поиска известных (подтвержденных) уязвимостей ПО и информационная система автоматизации деятельности экспертов испытательной лаборатории при разработке тестов проникновения. Создание концепций было выполнено на основе анализа особенностей

отечественной и зарубежных систем сертификации, связанных с проведением анализа уязвимостей. Предварительная (теоретическая) оценка показала сокращение времени анализа уязвимостей и, следовательно, времени проведения сертификационных испытаний в целом при использовании указанных информационных систем.

Литература

1. Барабанов А.В., Евсеев А.Н. Вопросы повышения эффективности анализа уязвимостей при проведении сертификационных испытаний программного обеспечения по требованиям безопасности информации // Труды международного симпозиума Надежность и качество. 2015. Т. 1. С. 330-333.
2. Барабанов А.В., Евсеев А.Н. Применение международного стандарта для поиска уязвимостей // Безопасные информационные технологии: Сборник трудов Пятой Всероссийской научно-технической конференции. - М., 2015. - С. 50-52.
3. Барабанов А.В., Марков А.С., Цирлов В.Л. Международная сертификация в области информационной безопасности // Стандарты и качество. 2016. № 7. С. 30-33.
4. Барабанов А.В., Федичев А.В. Разработка типовой методики анализа уязвимостей в веб приложениях при проведении сертификационных испытаний по требованиям безопасности информации // Вопросы кибербезопасности. 2016. № 2 (15). С. 2-8.
5. Марков А.С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации // Оборонный комплекс - научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.
6. Barabanov A., Markov A., Tsirlov V. Procedure for Substantiated Development of Measures to Design Secure Software for Automated Process Control Systems, In: 2016 International Siberian Conference on Control and Communications, SIBCON 2016 - Proceedings 2016. P. 7491660.
7. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls // Journal of Theoretical and Applied Information Technology. 2016. Т. 88. № 1. С. 77-88.
8. Shahriar, H. (2013). Security vulnerabilities and mitigation techniques of web applications. In Proceedings of the 6th International Conference on Security of Information and Networks (Aksaray, Turkey, November 26-28, 2013). SIN '13. ACM, New York, NY, USA, 459-459. DOI:10.1145/2523514.2523589
9. 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.

On Development of Software Application Vulnerability Analysis Information Systems During Software Security Evaluation Barabanov A.V.,¹¹

Abstract. A research of the existing approaches to the vulnerability analysis during software application security evaluation was conducted. The new vulnerability analysis information systems based on features of Russian and international IT security certification schemes were developed. Proposed information systems include: an information system designed to search in public available vulnerabilities database and an information system designed to development of penetration tests.

Keywords: security software evaluation, vulnerability analysis.

¹¹ Alexander Barabanov, Ph.D, CISSP, CSSLP, NPO Echelon, Moscow, ab@cnpo.ru

Реализационные основы доверенной загрузки на средствах виртуализации и вычислительной техники

Бабурин В.Н.¹²

Проведен анализ различных видов средств доверенной загрузки, в том числе: уровня базовой системы ввода-вывода, уровня платы расширения и уровня загрузочной записи. Разработана схема доверенной загрузки виртуальной инфраструктуры с гипервизорами I и II типов. Сделан вывод об актуальности обеспечения доверенной загрузки виртуальных сред.

Ключевые слова: модуль доверенной загрузки, МДЗ, средства виртуализации, гипервизор.

Введение.

Кратко угрозы, связанные с отсутствием доверенной загрузки, проиллюстрированы на рис. 1.



Рис. 1. Пример угроз

Исключение указанной угрозы возможно путем применения специальных средств доверенной загрузки [3].

Рассмотрим особенности загрузки физических и виртуальных и сред.

1. Доверенная загрузка физических сред

Как известно, доверенная загрузка должна обеспечивать [1, 2, 6]:

- блокирование попыток несанкционированной загрузки нештатной операционной системы (ОС) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной ОС;
- контроль доступа пользователей к процессу загрузки ОС;
- контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

Средства доверенной загрузки (СДЗ) подразделяется на три типа:

- СДЗ уровня базовой системы ввода-вывода;
- СДЗ уровня платы расширения;
- СДЗ уровня загрузочной записи.

¹² Бабурин Валерий Николаевич, ЗАО «НПО «Эшелон». v.baburin@npo-echelon.ru

На рис. 2 представлены основные этапы загрузки компьютера.



Рис. 2. Основные этапы загрузки компьютера с микропрограммой BIOS

2. Доверенная загрузка виртуальных сред

Следует указать типовые действия злоумышленника:

- несанкционированное чтение и изменение данных;
- несанкционированное изменение аутентификационной информации;
- внедрение программных закладок и вредоносного ПО.

Ввиду существования угроз виртуальной среды, требование доверенной загрузки относится не только к физическому оборудованию, но и к среде виртуализации (ЗСВ.5):

- в информационной системе должна обеспечиваться доверенная загрузка серверов виртуализации, виртуальных машин (контейнеров) и серверов управления виртуализацией в соответствии с мерой защиты «Обеспечение доверенной загрузки средств вычислительной техники».

- доверенная загрузка должна обеспечивать блокирование попыток несанкционированной загрузки гипервизора, хостовой и гостевых операционных систем.

- доверенная загрузка гипервизоров обеспечивается с использованием средств доверенной загрузки, функционирующих на серверах виртуализации.

- доверенная загрузка виртуальных машин (контейнеров) обеспечивается с использованием многокомпонентных средств доверенной загрузки, отдельные компоненты которых функционируют в гипервизорах.

Рассмотрим этапы доверенной загрузки виртуальной среды с помощью СДЗ уровня базовой системы ввода-вывода [1].

На рис.3 представлен вариант с гипервизором первого типа, который устанавливается непосредственно на сервер виртуализации в качестве системного программного обеспечения.

Модуль доверенной загрузки уровня базовой системы ввода-вывода может быть установлен на платформу еще до установки гипервизора, и именно этот его компонент и будет контролировать безопасность гипервизора.

В каждую виртуальную машину в виртуальный BIOS встраивается свой модуль доверенной загрузки, работа которого направлена на контроль целостности виртуального оборудования, гостевых операционных систем и файлов в них.



Рис. 3. Схема доверенной загрузки уровня BIOS виртуальной инфраструктуры с гипервизором I типа

В случае использования гипервизора II типа его целостность и целостность базовой ОС контролируется модулем доверенной загрузки, встроенным в код BIOS сервера виртуализации [7, 8].

Доверенную загрузку виртуального оборудования и гостевых ОС может осуществлять тот же модуль доверенной загрузки, но установленный уже не на сервер виртуализации, а на виртуальную машину (рис. 4).

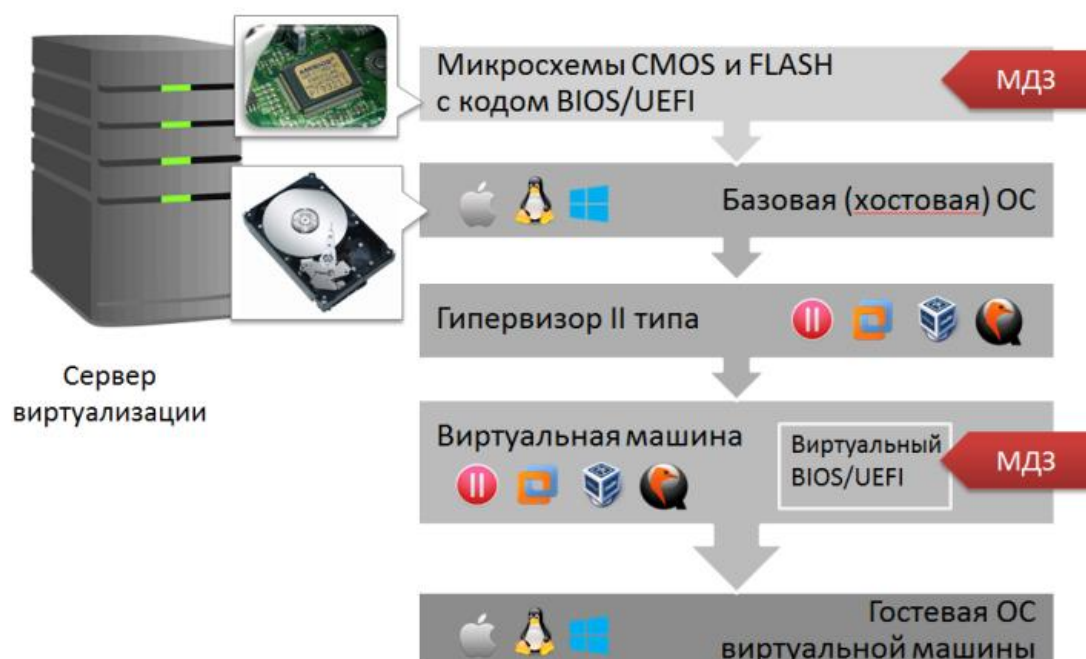


Рис. 4. Схема доверенной загрузки уровня BIOS виртуальной инфраструктуры с гипервизором II типа

Заключение

Проведенное исследование вызвало сделать вывод актуальности угроз, связанных с вредоносным ПО (функционирующего на уровне BIOS/UEFI).

Указанное обуславливает необходимость развития направления программных средств защиты загрузки физических и виртуальных операционных сред.

Предложенные решения реализованы в программном средстве доверенной загрузки «МДЗ-Эшелон» (производство НПО «Эшелон»).

Инновационность и достоверность исследования подтверждена свидетельством Роспатента и патентами [4, 5].

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. Бабурин В.Н., Марков А.С. Концепция доверенной загрузки и ее реализация на средствах виртуализации и вычислительной техники // Информация и безопасность, Т.20, №1.
3. Барабанов А.В., Гришин М.И., Кубарев А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых вредоносных компьютерных программ // Вопросы кибербезопасности. 2014. № 4 (7). С. 41-48.
4. Вареница В.В., Вылегжанин В.В., Марков А.С., Никулин М.Ю., Фадин А.А., Цирлов В.Л. Устройство для доверительной загрузки. Патент на полезную модель RUS 101555, 25.10.2010; 2010143450/08, 20.01.2011, Бюл. № 2. 2 с. URL: <http://elibrary.ru/item.asp?id=18646386>.
5. Веряев А.С., Вылегжанин В.В., Марков А.С., Рязанцев А.А., Фадин А.А., Цирлов В.Л. Способ доверенной загрузки в виртуализированных средах. Патент на изобретение RUS 2581552 24.03.2016; 2014136615; 2016. URL: <http://elibrary.ru/item.asp?id=25916898>.
6. Марков А.С., Пугачев И.Б. Программный метод обеспечения безопасности загрузки операционной среды // Известия Института инженерной физики. 2009. Т. 1. № 11. С. 7-9.
7. Kallenberg C., Wojtczuk R. Speed Racer: Exploiting an Intel Flash Protection Race Condition. URL: http://composter.com.ua/documents/Exploiting_Flash_Protection_Race_Condition.pdf (дата обращения: 01.09.2016).
8. Rutkowska J. Subverting Vista Kernel for Fun and Profit. Black Hat, 2006. 52 p.

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

Realizable Basis for Trusted Download Virtualization and Computing Equipment

Baburin V.¹³

The analysis of different types of trusted boot, including the level of the basic input-output system, the level of the expansion card and boot record level are done. The scheme of the trusted boot virtual infrastructure with hypervisor types I and II is developed. The conclusion about the relevance of letter of attorney download virtual environments.

Keywords: trusted boot module, MCH, virtualization, hypervisor is concluded.

¹³ Valerii Baburin, NPO Echelon. v.baburin@npo-echelon.ru

Информационная система автоматизации процесса поиска подтвержденных уязвимостей программного обеспечения

Барабанов А. В.¹⁴, Вареница В.В.¹⁵, Савченко В.В.¹⁶, Пургин А.Д.¹⁷

Проблема контроля защищённости программного обеспечения (ПО) на сегодняшний день как никогда актуальна и связана с наличием в нём уязвимостей. В данной статье рассматриваются вопросы автоматизации процесса поиска известных уязвимостей в ПО, а также в средах его функционирования и заимствованных сторонних программных компонентах. По результатам исследований была разработана информационная система автоматизации процесса поиска известных уязвимостей ПО, позволяющая минимизировать количество угроз безопасности в инфокоммуникационных системах.

Ключевые слова: безопасность инфокоммуникационных систем, защита информации, анализ общедоступных источников, анализ уязвимостей, автоматизированное обнаружение уязвимостей.

Введение

Проникновение информационных технологий во всевозможные сферы человеческой деятельности приводит к увеличению количества попыток несанкционированного доступа к конфиденциальной информации [1]. Каждый день в различных источниках публикуются данные о выявлении новых уязвимостей программного кода [2]. Разработчики ПО не всегда имеют возможность своевременно получать информацию о новых уязвимостях, в связи с чем существует возможность нарушения конфиденциальности, целостности и доступности информации, обрабатываемой в информационных системах, построенных с использованием ПО [3-8]. Наличие заимствованных компонентов и небезопасной среды функционирования разрабатываемых изделий усугубляют положение [9].

В связи с возникновением данной проблемы появляется необходимость в создании средств информирования разработчиков и потребителей ПО о наличии известных уязвимостей [10, 11]. На данный момент информация о новых уязвимостях публикуется в различных информационных ресурсах: база данных уязвимостей Федеральной Службы Технического и Экспортного Контроля (БДУ ФСТЭК России), базы данных National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE), vulners.com, бюллетенях вендоров [12], а также в иных источниках. Вышеуказанные источники не позволяют автоматически информировать разработчиков и экспертов ИБ об обнаружении новых уязвимостей. Исследование каждого ресурса занимает большое количество времени, в связи с этим разработчик может исследовать не все источники информации [13].

Анализ ресурсов, публикующих информацию об известных уязвимостях

Анализ вышеуказанных ресурсов показал, что на каждом из них существует уникальная информация, без учета которой могут возникнуть новые угрозы безопасности [14]. Например, в базе данных уязвимостей ФСТЭК России присутствует информация о наличии уязвимостей в СУБД «Линтер Бастион», а в базе данных CVE информация об уязвимостях в данном продукте отсутствует.

Поиск уязвимостей в конкретной библиотеке или программном модуле осложняется избыточностью информации и ошибками в алгоритмах поиска. Кроме того, в каждом

¹⁴ Барабанов Александр Владимирович, кандидат технических наук, ЗАО «НПО «Эшелон», Москва, ab@cnpro.ru

¹⁵ Вареница Виталий Викторович, ЗАО «НПО «Эшелон», Москва, v.varenitsa@npo-echelon.ru

¹⁶ Савченко Владислав Вадимович, МГТУ им. Баумана, Москва, vvsavchenko@outlook.com.

¹⁷ Пургин Александр Дмитриевич, МГТУ им. Баумана, Москва, a.purgin@npo-echelon.ru

решении вводятся различные сокращения и наименования ПО, что также осложняет поиск информации. В БДУ ФСТЭК России используются русскоязычные наименования ПО, в базе данных CVE русскоязычные наименования отсутствуют. По результатам анализа была поставлена задача разработки модели информационной системы автоматизации процесса поиска известных (подтвержденных) уязвимостей ПО.

Решение поставленной задачи

Для решения данной проблемы была разработана информационная система автоматизации процесса поиска известных (подтвержденных) уязвимостей (ИС АППИУ) (рис. 1).

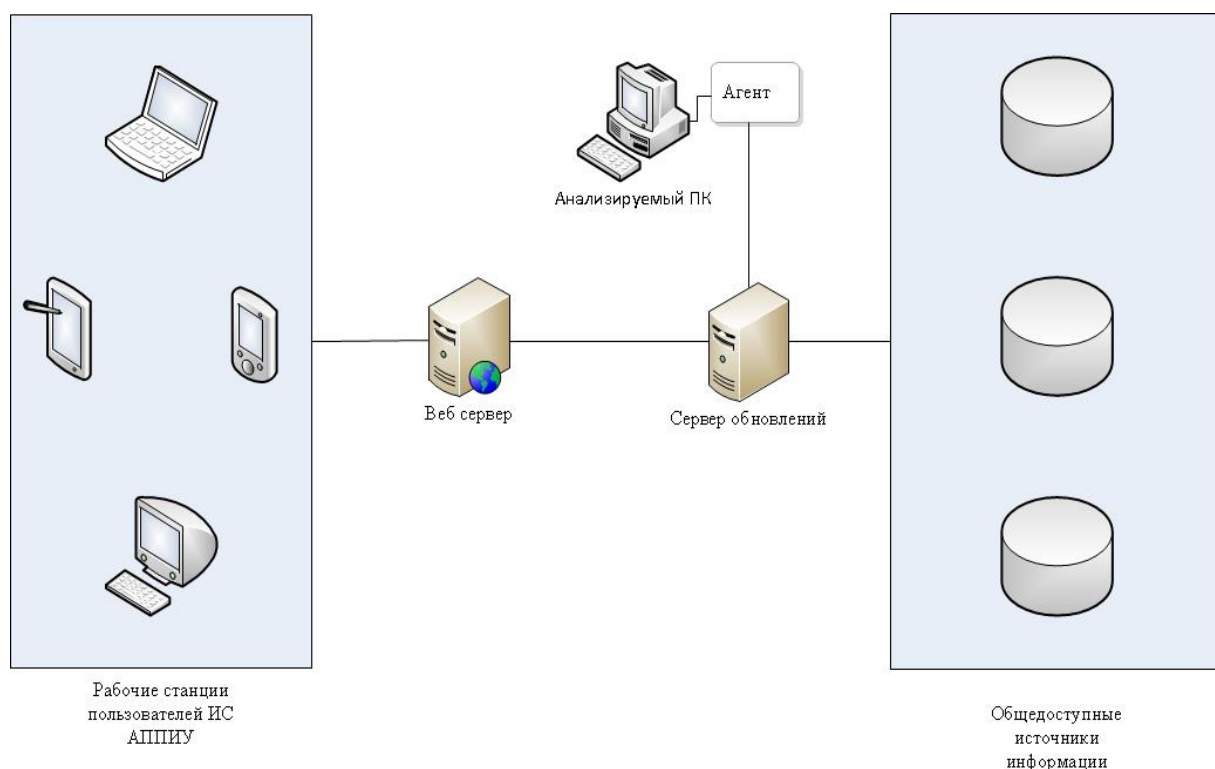


Рис. 1. Модель ИС АППИУ

Ключевую роль в данной системе выполняет сервер обновлений. Его основной задачей является сбор данных со всех известных источников информации – из БДУ ФСТЭК России, базы данных NVD, CVE, Microsoft bulletin ID, Mozilla Security и других. После того, как информация собрана, сервер обновлений приводит её к удобному для обработки виду и обновляет локальную базу данных. Сервер обновлений также может взаимодействовать с агентами, устанавливаемыми на пользовательские АРМ, и собирать информацию о модулях и компонентах, установленных на этих АРМ. На основании этой информации в личный кабинет пользователя автоматически добавляются сведения об актуальных уязвимостях для этих компонентов. Алгоритм работы сервера обновлений можно разделить на 4 взаимосвязанных этапа. На первом шаге происходит считывание информации с общедоступных источников, далее, на втором этапе, полученные данные сортируются по категориям и словарям. На третьем этапе работы сервера обновлений ИС АППИУ происходит удаление избыточности информации и идет формирование вспомогательных и

поисковых словарей. На финальном этапе, разработанное программное обеспечение добавляет найденные уязвимости в локальную базу данных и обновляет поисковый словарь.

С сервером обновлений взаимодействует веб-сервер. Он загружает подготовленную сервером обновлений информацию, и выводит пользователю в удобном для восприятия виде. Основная задача веб-сервера – информирование пользователя о наличии потенциальных уязвимостей, оповещение о появлении новых уязвимостей, а также предоставление отчётных материалов по результатам поиска в общедоступных источниках информации. Пользователь, используя веб-браузер, может ознакомиться с сформированными для него отчётами, а также добавить в список отслеживания новое ПО. При появлении новой уязвимости, пользователь получит информационное сообщение, после чего сможет более подробно ознакомиться с информацией об обнаруженной уязвимости.

Сравнение результатов поиска по общедоступным источникам и АППИУ.

В процессе тестирования ИС АППИУ было сделано следующее:

- выполнен поиск уязвимостей в базе данных CVE, БДУ ФСТЭК России, NVD;
- выполнен поиск уязвимостей с использованием ИС АППИУ;
- произведён анализ и сравнение полученных результатов.

В качестве ПО, в отношении которого производился поиск уязвимостей использовалось ПО Mozilla Firefox 45. Из результатов тестирования (табл. 1) видно, что данный подход является эффективным и позволяет в полной мере исследовать уязвимости в общедоступных источниках.

Таблица 1.

Результаты тестирования ИС АППИУ

№ п/п	Наименование информационной системы	Количество обнаруженных уязвимостей	Примечание
1	http://bdu.fstec.ru	41	Избыточность
2	http://cve.mitre.org	181	Избыточность, повторение, сложно искать по конкретным ОС
3	http://vulners.com	87	Избыточность, повторение, сложно искать по конкретным ОС
4	http://en-US/security/known-vulnerabilities/firefox/	23	--/--
5	ИС АППИУ	25	ИС АППИУ была сконфигурирована на поиск уязвимостей в бюллетени разработчика Mozilla и на поиск неподтверждённых разработчиком уязвимостей.

Выводы

В результате проведенных исследований было установлено, что ИС АПШУ позволяет более точно сформировать перечень потенциальных уязвимостей на основании данных, представленных в общедоступных источниках, отфильтровать избыточную информацию и своевременно информировать разработчика о появлении новых потенциальных уязвимостях.

Эффективность и достоверность решений подтверждена статистикой работы испытательной лаборатории и патентами [15, 16].

Литература

1. Петренко С.А., Петренко А.С. Новая Доктрина информационной безопасности Российской Федерации // Защита информации. Инсайд. 2017. №1 (73). С. 7-14.
2. Марков А.С. Летописи кибервойн и величайшего в истории перераспределения богатства // Вопросы кибербезопасности. 2016. № 1 (14). С. 68-74.
3. Веряев А.С., Фадин А.А. Формализация требований безопасности информации к средствам анализа защищенности // Вопросы кибербезопасности. 2015. № 4 (12). С. 23-27.
4. Волкович Е.К., Мессерле А.А. Защита от вредоносных междоменных запросов // Вопросы кибербезопасности. 2013. № 3. С. 8-11.
5. Калашников А.О., Ермилов Е.В., Чопоров О.Н., Разинкин К.А., Баранников Н.И. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков. Под ред. чл.-корр. РАН Д.А. Новикова. – Воронеж: Издательство «Научная книга». 2013. – 160 с.
6. Кубарев А.В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков // Вопросы кибербезопасности. 2013. № 2. С. 29-33.
7. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1 (2). С. 36-39.
8. Сафин Л.К., Чернов А.В., Александров Я.А., Трошина К.Н. Исследование информационной защищенности мобильных приложений // Вопросы кибербезопасности. 2015. № 4 (12). С. 28-37.
9. Кононов Д.С. Об улучшении избирательности одного алгоритма определения авторства вредоносного кода // Вопросы кибербезопасности. 2016. № 2 (15). С. 29-35.
10. Марков А.С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации // Оборонный комплекс - научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.
11. Markov A., Rautkin Y., Luchin D., Tsirolv V. Evolution of a radio telecommunication hardware-software certification paradigm in accordance with information security requirements // В сборнике: 2015 International Siberian Conference on Control and Communications, SIBCON 2015 - Proceedings 2015. С. 7147139. DOI: 10.1109/SIBCON.2015.7147139.
12. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. №3. С. 56-61.
13. Барабанов А.В., Федичев А.В. Разработка типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации // Вопросы кибербезопасности. 2016. № 2 (15). С. 2-8.
14. Веряев А.С., Барабанов А.В., Марков А.С., Авезова Я.Э., Шахалов И.Ю., Цирлов В.Л. Система оценки защищенности автоматизированных систем на основе выборочного комбинаторного контроля. Патент на полезную модель RUS 148904 10.09.2014. 2014.
15. Вылегжанин В.В., Маркин А.Л., Марков А.С., Уточка Р.А., Фадин А.А., Фамбулов А.К., Цирлов В.Л. Система для определения программных закладок. Патент на полезную модель RUS 114799 29.12.2011. 2012.

Information System for Automation Process of Search for Confirmation Software Vulnerabilities

Barabanov A.V.¹⁸, Varenitsa V.V.¹⁹, Savchenko V.V.²⁰, Purgin A.D.²¹.

In our days the problem of control and security of software is very relevant, and associated with the presence of vulnerabilities in soft. In this article we consider the problem of the need to automate the process of searching for known vulnerabilities in soft, in software operational environment and borrowed a third-party components. According to the research we developed the information system for automation process of search for known (confirmation) software vulnerabilities. This system allowed to minimize the number of security threats in the info-communication systems.

Keywords: security of information systems, data protection, analysis of publicly available sources, vulnerability analysis, automated detection of vulnerabilities.

УДК 004.056.53

Подход к формированию требований по сертификации средств мониторинга событий безопасности на основе «Общих критериев»

А.В. Барабанов²², И.М. Работаев²³, Н.М. Работаев²⁴

В статье рассмотрен подход к формированию базиса для оценки соответствия средств мониторинга событий безопасности (SIEM-системы) по требованиям безопасности информации, основанный на положениях стандарта «Общие критерии». Предложенный подход позволяет унифицировать и детерминировать процесс сертификации SIEM-решений по требованиям безопасности информации в Российской Федерации.

Ключевые слова: сертификация, SIEM, оценка соответствия, «Общие критерии»

Введение

Современное состояние и тенденции развития информационной инфраструктуры большинства организаций, использующих для обмена информацией современные технологии передачи и обработки данных, показывают стремительный рост количества обрабатываемой информации. В условиях постоянно возрастающего информационного потока невозможно выделить значимые для безопасности организации события [1]. Средства мониторинга событий безопасности (SIEM-система) - класс продуктов, используемых в различных информационных системах, которые предназначены для контроля событий безопасности разного уровня. SIEM-система предоставляет возможность своевременного выявления потенциальных нарушителей на основе анализа передаваемых в контролируемой среде данных и действий пользователей [2].

Как известно, все средства защиты информации в Российской Федерации подлежат оценке соответствия требованиям по безопасности информации. Перспективным направлением формирования требований к современным средствам защиты информации

¹⁸ Alexander Barabanov, Ph.D., «NPO-Echelon» CJSC, Moscow, ab@cnpo.ru

¹⁹ Vitaliy Varenitsa, «NPO-Echelon» CJSC, Moscow, v.varenitsa@npo-echelon.ru

²⁰ Vladislav Savchenko, Bauman Moscow State Technical University, Moscow, vvsavchenko@outlook.com

²¹ Alexander Purgin, Bauman Moscow State Technical University, Moscow, a.purgin@outlook.com

²² Барабанов Александр Владимирович, канд. техн. наук, ЗАО «НПО «Эшелон», г. Москва, ab@cnpo.ru

²³ Работаев Никита Максимович, МГТУ им. Н.Э. Баумана, г. Москва, mad.man1394@gmail.com

²⁴ Работаев Илья Максимович, МГТУ им. Н.Э. Баумана, г. Москва, mad.man1394@gmail.com

является использование аппарата ISO 15408 («Общие критерии») [3]. В настоящее время уже разработаны нормативно-правовые акты, касающиеся систем обнаружения вторжений [4], средств антивирусной защиты [5], DLP-решений [6, 7], средств анализа защищенности [8, 9], средств защиты среды виртуализации [10] и др.

Однако нормативно-методическая база, регламентирующая требования к SIEM-продуктам, отсутствует. Таким образом, в настоящее время присутствует явная необходимость формирования нормативных и методических документов, регламентирующих процесс сертификации средств мониторинга событий безопасности, с целью повышения уровня нормализации и детерминированности данного процесса.

Средства мониторинга событий безопасности в рамках существующих нормативных документов

Протоколирование и аудит - группа программно-технических мер по обеспечению информационной безопасности автоматизированных систем. Сервис является одним из основных механизмов безопасности, наряду с аутентификацией, шифрованием, управлением доступа, межсетевым экранированием. Согласно пункту 20 приказа №17 ФСТЭК России, регистрация событий безопасности должна входить в перечень организационных и технических мер защиты информации, реализуемых в информационной системе в рамках ее системы защиты информации. В приказе №17 ФСТЭК России представлен перечень мер по регистрации событий безопасности, которые необходимы для всех классов защищенности информационных систем. Приказ №21 ФСТЭК России также включает регистрацию событий безопасности в необходимый набор мер по обеспечению безопасности персональных данных и определяет базовый функционал данной группы мер (сбор, хранение, защита информации о событиях). Также определяется перечень мер протоколирования и аудита, необходимых для реализации, с целью обеспечения соответствующих уровней защищенности персональных данных. Для реализации средств протоколирования и аудита на практике применяются системы, построенные на основе концепции SIEM систем.

SIEM (Security Information and Event Management) - система управления информацией и событиями безопасности. Основная цель построения и использования SIEM - повысить уровень информационной безопасности за счет обеспечения в режиме, близком к реальному времени, мониторинга, возможности манипулировать информацией о безопасности и осуществлять проактивное управление событиями безопасности [2, 11].

Термин "проактивный" обозначает "действующий до того, как ситуация станет критической". Проактивное управление подразумевает интеллектуальный подход к управлению событиями, использование автоматических механизмов анализа уже собранной информации для прогноза о возможных небезопасных состояниях защищаемой системы и предотвращения таких состояний. Источниками информации для SIEM являются различные компоненты контролируемой информационной инфраструктуры - сетевое оборудование, средства защиты информации, базы данных, приложения.

Подход к формированию требований по сертификации средства мониторинга событий безопасности

Существуют два принципиально разных подхода к формированию требований безопасности информации, предъявляемых к изделиям информационных технологий [11]. Первый подход состоит в использовании строго заданных требований безопасности информации. Примерами данного подхода являются руководящие документы Гостехкомиссии России, в основу которых был положен подход, используемый при написании «Оранжевой книги». Второй подход основан на методологии документа «Общие критерии», принятого в качестве государственного стандарта Российской Федерации [3]. На основе данного подхода ФСТЭК России уже разработаны нормативные документы

нового поколения, предъявляющие требования к системам обнаружения вторжений и средствам антивирусной защиты. Второй подход является более перспективным при использовании в формировании и других средств защиты информации, например, SIEM систем.

В соответствии с выбранным подходом формулируется перечень функциональных требований безопасности и требований доверия к безопасности. Основанием для формирования данного перечня является анализ существующих SIEM систем. Базис формируется из набора представленных в "Общих критериях" требований с учетом специфики данного класса изделий информационных технологий. Анализ аспектов среды безопасности позволил сформулировать перечень функциональных требований безопасности (таблица 1), которые целесообразно предъявлять к SIEM-системам.

Таблица 1.

Функциональные требования безопасности, предъявляемые к SIEM-системам

Класс ФТБ (в соответствии с ГОСТ Р ИСО/МЭК 15408-2)	Наименование функциональной возможности	Краткое описание
FAU_GEN.1	Генерация данных аудита	Класс определяет требования по регистрации событий, относящихся к безопасности, которые подконтрольны SIEM-системе.
FAU_GEN.2	Ассоциация идентификатора пользователя	
FAU_SAR.1	Просмотр аудита	Класс определяет требования по предоставлению уполномоченным пользователям возможность получать и интерпретировать информацию из журналов регистрации событий.
FAU_SAR.2	Ограниченный просмотр аудита	
FAU_STG.1	Защищенное хранение журнала аудита	Класс определяет требования, при выполнении которых SIEM-система способна создавать и сопровождать журнал аудита безопасности.
FAU_ARP.1	Сигналы нарушения безопасности	Класс определяет реакцию SIEM-системы на обнаружение событий, указывающих на возможное нарушение безопасности.
FAU_SAA.1	Анализ потенциального нарушения	Классы определяют требования по анализу показателей функционирования информационной системы и данных аудита в целях поиска возможных или реальных нарушений безопасности. Этот анализ может использоваться для поддержки как обнаружения вторжения, так и автоматической реакции на ожидаемое нарушение безопасности.
FAU_SAA.2	Выявление аномалии, основанное на профиле	
FAU_SAA.3	Простая эвристика атаки	
FAU_SAA.4	Сложная эвристика атаки	
FIA_AFL.1	Обработка отказов аутентификации	Класс содержит требования к определению числа неуспешных попыток аутентификации администратора и к действиям SIEM-системы при превышении ограничений на неуспешные попытки аутентификации.
FIA_ATD.1	Определение атрибутов пользователя	Класс определяет требования для ассоциации атрибутов безопасности (например, ролей) с администраторами.
FIA_UAU.1	Выбор момента аутентификации	Класс определяет типы механизмов аутентификации администратора, предоставляемые SIEM-системой.

FIA_UID.1	Выбор момента идентификации	Класс определяет условия, при которых от администратора должна требоваться собственная идентификация до выполнения при посредничестве SIEM-системы каких-либо других действий, требующих идентификации.
FMT_MOF.1	Управление режимом выполнения функций безопасности	Классы позволяет уполномоченным пользователям управлять функциями из числа функций безопасности SIEM-системы.
FMT_MTD.1	Управление данными функций безопасности SIEM-системы	
FMT_SMR.1	Роли управления безопасностью	Класс предназначен для управления назначением различных ролей.

Выводы

Предложенный в настоящей работе подход позволяет нормализовать процесс оценки соответствия средств мониторинга событий безопасности требованиям безопасности информации. Представленный подход может найти практическое применение в процессе проведения сертификационных испытаний в системе сертификации средств защиты информации ФСТЭК России.

Литература

1. Петренко А.С., Петренко С.А. Проектирование корпоративного сегмента СОПКА // Защита информации. Инсайд. 2016. №6 (72). С. 47-52.
2. Марков А.С., Фадин А.А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80-81.
3. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации "Общим Критериям" // Информационные технологии. 2015. Т. 21. № 4. С. 264-270.
4. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. С. 31-33.
5. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация средств антивирусной защиты по новым требованиям безопасности информации // Вестник МГТУ им. Н. Э. Баумана. Сер. "Приборостроение". 2012. Спецвыпуск № 5 "Информатика и системы управления". С. 272-278.
6. Барабанов А.В., Гришин М.И., Марков А.С. Формирование требований к сертификационным испытаниям DLP-систем по требованиям безопасности информации // Инженерный журнал: наука и инновации. 2013. № 2 (14). С. 25.
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. Веряев А.С., Фадин А.А. Формализация требований безопасности информации к средствам анализа защищенности // Вопросы кибербезопасности. 2015. № 4 (12). С. 23-27.
9. Markov A.S., Fadin A.A., Veryaev A.S. Formalization of Requirements for Security Analysis Tools of Information Systems. Proceedings of the 3rd International Conference «Information Technologies for Intelligent Decision Making Support» (May 1821), Ufa, Russia, 2015, Vol. 1, pp. 116-118.
10. Юдичев Р.М., Горюнов М.Н. Оценка и ранжирование функциональных возможностей средств защиты среды виртуализации // Автоматизация и управление в технических системах. 2015. № 1 (13). С. 92-100.
11. 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.

Approach to Formation of Requirements for SIEM Certification on the Basis of Common Criteria

A.V. Barabanov²⁵, I.M. Rabotaev²⁶, N.M. Rabotaev²⁷

In the article the approach to basis formation for information security requirements compliance assessment of security information and event management systems is considered. The approach is based on Common Criteria standard provisions. The offered approach allows determining and unifying certification of SIEM solutions on information security requirements in the Russian Federation.

Keywords: certification, SIEM, compliance assessment, Common criteria.

УДК: 004.056: 004.73

Методика оценки доверия в беспроводной сенсорной сети

Басан А. С.²⁸, Басан Е. С.²⁹

Разработанная методика оценки доверия в беспроводной сенсорной сети на основе анализа поведения узла, а также показателей остаточная энергия и загруженность узла, использует оценку вероятности отклонения текущего значения узла от доверительного интервала. Показана возможность выявлять атаки на отказ в обслуживании.

Ключевые слова: атаки, теория вероятности, сенсорные узлы, угрозы, безопасность

Введение

На сегодня все большую популярность набирают беспроводные системы мониторинга и управления объектами на базе беспроводных сенсорных сетей (БСС) [1]. С точки зрения безопасности основным недостатком БСС является наличие большого количества уязвимостей, как: физическая незащищённость узлов; отсутствие инфраструктуры; динамически изменяющаяся топология; ограниченность ресурсов узла-сенсора; изменение количественного и качественного состава сети; ограниченная пропускная способность [2]. При этом существует большое количество атак на БСС, которые не являются характерными для компьютерных сетей. Разрабатываемая методика основана на вычислении доверия в БСС. Анализ схем вычисления доверия в БСС показал, что существует большое количество подходов, которые основываются на распределенном и централизованном вычислении значения доверия [3]. Недостатком существующих систем доверия является то, что за основу вычисления доверия берется соотношение между успешными и неуспешными событиями узла. При этом если узел проводит атаку при отсутствии неуспешных событий, то ни одна система не способна распознать злоумышленника.

Разработка методики оценки доверия

Представленная методика определения доверия в сети, включает вычисление прямого и централизованного значений доверия. За основу вычисления прямого значения доверия взята теорема Байеса, в которой в качестве априорной вероятности выступает бета-распределение. Помимо этого, вводятся коэффициенты, присваиваемые каждому типу пакетов относительно их значимости в сети, позволяющие достаточно гибко

²⁵Alexander Barabanov, Ph.D., «NPO-Echelon» CJSC, Moscow, ab@cnpo.ru

²⁶Ilya Rabotaev, Bauman Moscow State Technical University, Moscow, mad.man1394@gmail.com

²⁷Nikita Rabotaev, Bauman Moscow State Technical University, Moscow, mad.man1394@gmail.com

²⁸Басан А. С., кандидат технических наук, Южный Федеральный Университет г. Таганрог, tfrtu@mail.ru

²⁹Басан Е. С., Южный федеральный университет, г. Таганрог, ele-barannik@yandex.ru

контролировать вычисление доверия. А также фактор наказания, который контролирует значимость неуспешных событий сети. Отличием данной методики является способ вычисления централизованного значения доверия, который включает в себя анализ вероятности попадания загруженности узла L и от остаточной энергии узла $Q(E)$ в заданный доверительный интервал, который вычисляется для группы узлов сети за текущий промежуток времени. Вероятность попадания в доверительный интервал позволяет оценить, не превышают ли показания узла максимально или минимально допустимые. Данное сопоставление позволяет обнаружить активные атаки типа отказ в обслуживании на основе проверки отклонения текущих показателей узла от ожидаемых. А также вычислить злоумышленника в случае, если он имеет большие энергетические ресурсы, чем максимально допустимый уровень энергии в сети.

1. Узел сенсор **A** проводит наблюдение за узлом соседом **B** за время Δt и получает данные D , которые разделяет на 4 группы по типу пакетов и высчитывает для каждого количество успешных s и неуспешных f событий.

2. Вычисляется значения весовых коэффициентов (выполняется один раз) для каждой группы пакетов (d_1, d_2, d_3, d_4), каждая из данных групп имеет вес/значимость w_i . Весовые коэффициенты вычисляются на основе анализа атак: $P(A) = \frac{ai}{N} = w_i$, где: a_i - число раз, которое встречается i -ая группа данных встречается при реализации атаки, а N - общее количество атак.

3. Вычисляется фактор наказания, чтобы повысить значимость неуспешных событий введем фактор наказания: $\gamma = 1 - \frac{f}{D}$, где: f - неуспешные события, D - все события.

4. Вычисляется значение доверия на основе использования бета-функции. При определении доверия, с точки зрения использования функции распределения репутации узла (представленной бета-функцией распределения), используется математическое ожидание распределения вероятностей, представляющее репутацию между двумя узлами. Репутация $R_{A,B}$ узла B , измеряемая узлом A . Математическое ожидание от функции репутации имеет следующий вид [4]:

$$T[R_{A,B}] = M[\text{Beta}\{s_{A,B}(\Delta t) + 1, f_{A,B}(\Delta t) + 1\}] = \frac{s_{A,B}(\Delta t) + 1}{s_{A,B}(\Delta t) + f_{A,B}(\Delta t) + 2},$$

где: T – доверие узла A относительно узла B .

5. Вычисляется суммарное прямое значение доверия, с весовыми коэффициентами для каждого подмножества операций и фактором наказания.

6. Центральный узел (ЦУ) использует нормальный закон распределения для показателей загруженности L и остаточной энергии $Q(E)$.

7. ЦУ устанавливает границы доверительного интервала для нормального распределения, для показателей остаточная энергия $Q(E)$ и загруженность узла L . Вычисляет нижнюю границу доверенного интервала для остаточной энергии a_{min} и верхнюю границу для загруженности узла b_{max} .

8. ЦУ оценивает вероятность попадания текущего значения загруженности и остаточной энергии в доверительный интервал для каждого узла.

$$P_{Q(E)}(a_{min} < Q(E)_i < a_{max}) = \Phi\left(\frac{a_{max} - \overline{Q(E)}_e}{\sigma_{Q(E)}_e}\right) - \Phi\left(\frac{a_{min} - \overline{Q(E)}_e}{\sigma_{Q(E)}_e}\right)$$

$$P_L(b_{min} < L_i < b_{max}) = \Phi\left(\frac{b_{max} - \overline{L}_e}{\sigma_{L_e}}\right) - \Phi\left(\frac{b_{min} - \overline{L}_e}{\sigma_{L_e}}\right),$$

где: Φ - функция Лапласа; $P_{Q(E)}$, P_L – вероятность попадания остаточной энергии узла и уровня загруженности узла в пределах доверительного интервала, значения для выборочного математического ожидания $\overline{Q(E)}$, $\overline{L_e}$ и среднеквадратического отклонения, вычисляются на основании показателей двух соседних интервалов.

9. ЦУ использует теорему Байеса для получения централизованного значения доверия путем комбинирования значений P_{QE} , P_L и вычисляет итоговое значение доверия:

$$T_{cent} = P(T_{cent} | P_{Q(E)}) \cdot P(T_{cent} | P_L),$$

$$P(T_{sum} | T_{dir}, T_{cent}) = P(T_{sum} | T_{dir}) \cdot P(T_{sum} | T_{cent}).$$

Оценка эффективности разработанной методики определения доверия и выводы

Для оценки эффективности разработанной методики определения доверия была разработана модель кластерной БСС с помощью симулятора NS-2.35. На сеть проводится ряд атак: Сибиллы, блокирования узла, блокирования узла с наличием условий, туннельная атака, отказ в обслуживании [5]. Для определения эффективности использовались параметры: надежность, энергетическая эффективность, точность определения доверенного/не доверенного узла [6]. При оценке уровня доверия проводилось сравнение со следующими аналогами: RFSN, LTDS, BTMS. Достоинством разработанной МОД является способность обнаруживать атаки злоумышленника при отсутствии неуспешных событий. Данное преимущество вытекает из способа вычисления централизованного значения доверия в сети. К примеру, при реализации атаки Сибиллы злоумышленник, представлялся несколькими объектами сети и перенаправлял на себя все маршруты, тем самым перехватывал информацию. МОД способна выявить злоумышленника, так как он будет иметь намного больший уровень загруженности, чем соседние узлы.

Литература

1. Yenumula B. Trust-based approach in wireless sensor networks using an agent to each cluster. International Journal of Security, Privacy and Trust Management, Vol.1, No.1, P. 19-36. February 2012.
2. Абрамов Е.С., Басан Е.С., Лакшми В. Разработка защищенного протокола управления мобильной кластерной сенсорной сетью / Известия ЮФУ. Технические науки. № 2 (151). 2014. С. 101-107.
3. K. Govindan, P. Mohapatra. Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey. In IEEE Communications Surveys & Tutorials (Volume:14, Issue: 2), P. 279 - 298, 2012.
4. R. Feng, X. Han, Q. Liu, and N. Yu. A Credible Bayesian-Based Trust Management Scheme for Wireless Sensor Networks. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks. P. 1-9. 2015.
5. Абрамов Е.С., Басан Е.С. Анализ сценариев атак на беспроводные сенсорные сети / Материалы XIII Международной научно-практической конференции «ИБ-2013» / Ч.1. – Таганрог: ТТИ ЮФУ, 2012. – С.60-72.
6. Басан А.С., Басан Е.С., Макаревич О.Б. Development of the Hierarchal Trust Management System for Mobile Cluster-based Wireless Sensor Network. Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks, 2016, pp.116-122.

The Method of the Trust Estimation in a Wireless Sensor Network

Basan A.S., Basan E.S.³⁰

The developed method of estimation of the trust in a wireless sensor network based on the analysis behavior of node, as well as analysis of residual energy and node workload, use estimation of the probability of deviation from the current node value of the confidence interval. What makes it possible to detect attacks such as denial of service, Sybil attack, attack on the depletion of resources. These attacks more difficult to detect and analogues are not able to identify them as analyze only the ratio of successful / unsuccessful node events.

Keywords: attacks, evidence theory, sensor nodes, vulnerabilities, ensuring security/

³⁰ Basan A.S., Southern Federal University, Taganrog, tffrtu@mail.ru,
Basan E.S., Southern Federal University, Taganrog, ele-barannik@yandex.ru

Алгоритм установления виртуального соединения на абонентском доступе сети передачи данных учебного лабораторного стенда

Бельфер Р.А.³¹, Кулинич Р.С.³², Прищепин Е.П.³³

Приводится алгоритм установления коммутируемого виртуального канала на участке удаленного абонентского доступа сети передачи данных на базе виртуальных каналов. Этот алгоритм служит для создания программного обеспечения одной из сетей передачи данных учебного лабораторного стенда, который находится в состоянии реализации студентами кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана.

Ключевые слова: коммутируемый виртуальный канал, центр коммутации пакетов, информационная безопасность, передача и данных

Введение

В работе [1] приводятся общие положения по созданию на кафедре “Информационная безопасность” МГТУ им. Н.Э. Баумана учебного лабораторного стенда (УЛС) сети передачи данных с высокими показателями информационной безопасности и надежности. Создание такого стенда предназначено для получения студентами научно-практических знаний, которые позволят использовать их в работе на предприятиях, создающих подобные сети. Для реализации УЛС необходимо составить алгоритмы установления/разъединения соединения, передачи данных по этому соединению и других функций. При этом необходимо учесть требования обеспечения информационной безопасности (ИБ). В работе [2] предлагается алгоритм обеспечения ИБ на удаленном абонентском доступе сети передачи данных (ПД) на базе технологии виртуальных каналов. Этот алгоритм относится к одному из способов обеспечения ИБ - взаимной аутентификации.

В настоящей работе продолжаются работы по созданию этой сети ПД [3]. Предлагается алгоритм установления виртуального соединения (коммутируемого виртуального канала, КВК) [3] на абонентском доступе этой сети передачи данных УЛС с учетом обеспечения информационной безопасности.

1. Исходные данные

На рис. 1 приведена конфигурация сети ПД учебного лабораторного стенда, на примере которой приводится настоящая работа.

Здесь представлены две резервные ветви (пучок маршрутизаторов из двух путей маршрутизации), включающих абонентский доступ к транспортной сети, трех центров коммутации пакетов (ЦКП) в каждом. К оконечным ЦКП в каждом пути (ЦКП1.1, ЦКП3.1 для первого пути маршрутизации и ЦКП1.2, ЦКП3.2 для второго пути маршрутизации) подключены оконечные пункты (а, b и др.), а ЦКП2.1 и ЦКП2.2 являются транзитными соответственно для первого и второго пути маршрутизации.

Оконечные пункты обмениваются данными одновременно по двум путям маршрутизации (рис.1).

³¹ Бельфер Рувим Абрамович, МГТУ им. Н.Э. Баумана, к.т.н., доцент, a.belfer@yandex.ru

³² Кулинич Роман Сергеевич, МГТУ им. Н.Э. Баумана, kulinichrs@gmail.com

³³ Прищепин Егор Павлович, МГТУ им. Н.Э. Баумана, egor.prishchepin@gmail.com

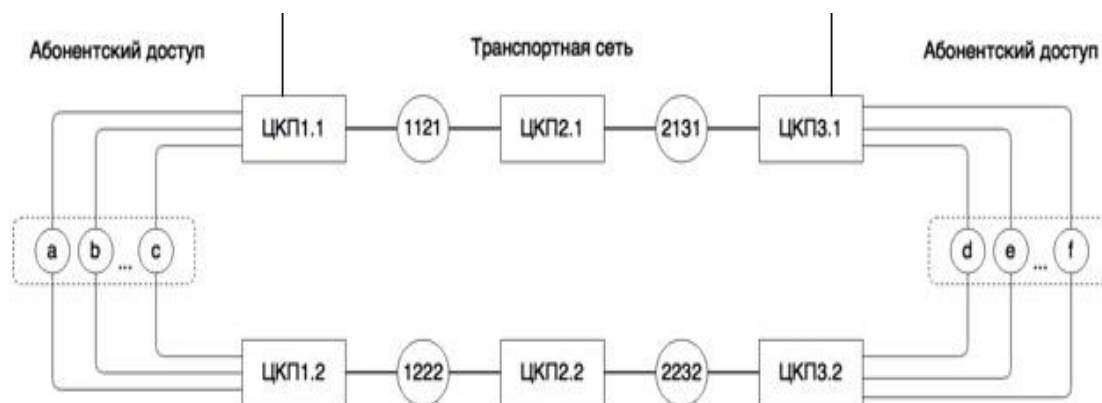


Рис.1. Конфигурация лабораторного стенда сети ПД

Для выполнения этих алгоритмов во всех оконечных пунктах и оконечных ЦКП сети ПД предварительно следует создать следующие общие программы и установить исходное состояние некоторых характеристик:

1. программу формирования синхронизации сообщений с помощью синхронизирующего байта («01111110»);
2. программу формирования контрольно-проверочной комбинации циклического кода;
3. назначить физические адреса оконечным пунктам;
4. составить таблицу маршрутизации ЦКП по физическим адресам в оконечных ЦКП.

В таблице маршрутизации ЦКП 1.1 оконечным ЦКП назначения при установлении КВК является ЦКП 3.1 и, наоборот, в таблице маршрутизации ЦКП 3.1 оконечным ЦКП назначения при установлении КВК является ЦКП 1.1. То же самое относится и ко второму пути маршрутизации. Поскольку настоящая работа посвящена алгоритму установления КВК только на абонентском доступе, то в таблице маршрутизации указываются только имитаторы каналов связи (буферы): 1121 (между ЦКП1.1 и ЦКП2.1), 3121(между ЦКП3.1 и ЦКП2.1), 1222 (между ЦКП1.2 и ЦКП2.2), 3222 (между ЦКП3.2 и ЦКП2.2).

Таблица 1.

Таблица маршрутизации по физическим адресам

	ЦКП 1.1	ЦКП 3.1	ЦКП 1.2	ЦКП 3.2
ЦКП 1.1		1121		
ЦКП 3.1	3121			
ЦКП 1.2				1222
ЦКП 3.2			3222	

Создать в каждом оконечном ЦКП (ЦКП1.1 и ЦКП1.2) начальное содержание очереди свободных номеров $O_{свн}$ и соответствующие очереди занятых номеров $O_{зан}$ и их значения. Длина ячейки под номер - 2 байта. Заполнить на период отладки ПО в сумме 64 значения $O_{свн}$ и $O_{зан}$.

Для окончечных ЦКП1.1 и ЦКП1.2 примем $O_{свн}: \{9; 2; 5; 11; 21; 18; 19...4; 7\}$. $O_{зан}: \{3; 1; 6...8; 10\}$.

Для окончечных ЦКП3.1 и ЦКП3.2 примем $O_{свн}: \{14; 12; 15; 11; 17; 19; 18...9; 3\}$. $O_{зан}: \{13; 6; 5...18; 16\}$.

Назначить исходное состояние КВК на окончечном пункте - 0 (1- установление КВК).

2. Алгоритм установления и сброса КВК на абонентском доступе сети ПД

Алгоритм установления КВК на абонентском доступе сети ПД включает реализацию в следующей последовательности:

1. алгоритм установления КВК с учетом обеспечения ИБ, включая изложенную в [2] взаимную аутентификацию на абонентском доступе, окончечный пункт которого является источником установления КВК;

2. алгоритм создания сессионных ключей;

3. алгоритм установления КВК с учетом обеспечения ИБ, включая изложенную в [2] взаимную аутентификацию на абонентском доступе, окончечный пункт которого является пунктом назначения установления КВК.

2.1. Алгоритм создания сессионных ключей

Для обеспечения ИБ сети ПД требуется создание сессионных ключей шифрования адресной части заголовка сообщений Каб и сквозного шифрования информационной части сообщений между окончечными пунктами КВК ($K_{СКВ}$), ключа целостности ($K_{Цаб}$) адресной части заголовка сообщений на абонентском участке, ключа целостности $K_{ЦСКВ}$ информационной части пакета данных.

$$K_{аб} = \text{hash}(K, \text{Адроп}), \quad (1)$$

где K - головной секретный ключ, созданный при выполнении протокола взаимной аутентификации на абонентском доступе [2];

Адроп - адрес окончечного пункта.

$$K_{СКВ} = \text{hash}(K, I_{ц}, \text{Адроп}), \quad (2)$$

где $I_{ц}$ - идентификатор ЦКП. (3)

$$K_{Цаб} = \text{hash}(K, K_{аб}, I_{ц}, \text{Адроп}). \quad (4)$$

$$K_{ЦСКВ} = \text{hash}(K, K_{СКВ}, I_{ц}, \text{Адроп}). \quad (5)$$

Все эти ключи создаются на окончечном пункте и в двух окончечных ЦКП абонентского доступа (каждого пути маршрутизации абонентского доступа принятой конфигурации сети ПД).

Длина ключей выбирается в зависимости от принятого протокола шифрования. При этом необходимо учесть, что бы длина профиля сообщения была равна длине ключа протокола шифрования. Примером несовпадения может быть например длина ключа протокола шифрования DES равна 56 бит, а длина профиля сообщения протокола MD5 равна 128 бит.

Приведенное создание ключа сквозного шифрования $K_{СКВ}$ и ключа целостности $K_{ЦСКВ}$ информационной части пакета данных относится только к абонентскому участку с окончечным пунктом - инициатором установления соединения.

На абонентском участке назначения вместо этого выполняется протокол передачи этих ключей из окончечного ЦКП (ЦКП 3.1 и ЦКП 3.2) в окончечный пункт. После установления (разд. 2.2) доверия открытого ключа получателя P_R (оконечного пункта назначения) источник I (ЦКП 3.1 и ЦКП 3.2) отправляет в окончечный пункт получателя R два зашифрованных этим ключом сообщения: $P_R(K_{СКВ})$ и $P_R(K_{ЦСКВ})$. Получатель R с помощью своего закрытого ключа S_R расшифровывает $K_{СКВ}$ и $K_{ЦСКВ}$: $S_R P_R(K_{СКВ})$ и $S_R P_R(K_{ЦСКВ})$ [5].

3. Алгоритм установления и КВК

Алгоритм установления КВК состоит из двух фаз – установление и подтверждение. Алгоритм установления КВК на абонентском участке оконечного пункта - отправителя запроса на соединение незначительно отличается от алгоритма установления КВК на абонентском участке оконечного пункта – получателя запроса на соединение.

3.1. Алгоритм установления КВК на абонентском участке оконечного пункта - отправителя запроса на соединение

Назначить состояние КВК на оконечном пункте - 1 (установление КВК).

1. Сформировать и передать от оконечного пункта (например в пункте *a* на рис. 1) в ЦКП1.1 и ЦКП1.2 сообщение об инициализации установления КВК. Формат этого сообщения состоит из трех полей - тип сообщения -1, конфигурация сети "1" (1 байт), физический адрес исходящего оконечного пункта (для примера пункта *a* -101 и физический адрес пункта назначения (для примера пункта *f* -501). Физические адреса сообщения шифруются и обеспечивается их целостность с помощью соответственно ключей шифрования Каб и целостности Кцаб (разд. 2.1). Алгоритмы шифрования и целостности определяются при согласовании ассоциации безопасности SA при выполнении взаимной аутентификации [2]. Протоколы шифрования и целостности определяются при использовании индекса согласованных параметров SPI(A).

2. Произвести в оконечных ЦКП1.1 и ЦКП1.2 абонентского доступа дешифрацию и проверку целостности принятого сообщения.

3. Подготовка к передаче от оконечного ЦКП (в примере ЦКП1.1 и ЦКП1.2) в оконечный пункт сообщения с уникальным номером LCN, стоящим первым в $O_{свн}$. Согласно данным в разделе 1 это $LCN=9$.. Откорректировать $O_{свн}$: {2; 5,11,21; 18;19...4; 7} и $O_{зан}$: {3; 1; 6...8; 10; 9}, а так же характеристики этих очередей. Запомнить в оконечном ЦКП1.1 (ЦКП1.2) логический адрес $LCN=9$ оконечного пункта.

4. Создать сообщение в ЦКП1.1 и ЦКП1.2 из двух полей - тип сообщения - 2, $LCN=9$.

5. В оконечном ЦКП (в примере ЦКП1.1 и ЦКП1.2) зашифровать с использованием ключа Каб сообщение (тип 2) и сформировать проверку его целостности сообщения типа 2 аналогично приведенному в п.1 в отношении сообщения типа 1.

6. Запомнить в оконечном ЦКП1.1 (ЦКП1.2) логический адрес $LCN=9$ оконечного пункта. Отправить от ЦКП1.1 и ЦКП1.2 сообщение типа 2 в оконечный пункт.

7. Произвести в оконечном пункте дешифрацию и проверку целостности принятого сообщения.

8. Отправить в оконечные ЦКП (в примере ЦКП1.1 и ЦКП1.2) от оконечного пункта зашифрованное с проверкой целостности сообщение Запрос Вызова (ЗВ) на установление КВК аналогично приведенным мерам ИБ в п.1 в отношении сообщения типа 1. Формат сообщения ЗВ (подлежащее шифрованию и обеспечению целостности) состоит из следующих полей - тип сообщения, LCN, физические адреса оконечных пунктов отправителя и получателя, контрольно-проверочная комбинация КПК. Напомним, что КВК устанавливается между оконечными пунктами с физическими адресами 101 (*a*) и 501 (*f*) - см. (рис.1)

9. Расшифровать в оконечном ЦКП (в примере ЦКП1.1 и ЦКП1.2) с использованием ключа Каб сообщение ЗВ и проверить целостность с использованием ключа Кцаб .

10. Подготовить сообщение ЗВ к передаче из оконечного ЦКП (в примере ЦКП1.1 и ЦКП1.2) в смежные ЦКП в соответствии с таблицей маршрутизации по физическим адресам (табл.1). В данной конфигурации сети ПД (рис.1) эти сообщения передаются в имитаторы каналов связи. Для первого пути маршрутизации - 1121, для второго - 1222.

Для этого необходимо выбрать первый уникальный номером LCN в $O_{свн}$ (п. 5). Таким является LCN=2. Заменить в ЗВ LCN=9 на LCN=2. Откорректировать $O_{свн}$: {5; 11; 21; 18; 19...4; 7} и $O_{зан}$: {3; 1; 6...8; 10; 9; 2}, а так же характеристики этих очередей.

11. Составить строку таблицы маршрутизации ЦКП1.1 и ЦКП1.2 (табл. 2) по логическим адресам, соответствующую передаче сообщения от оконечного пункта. Эта и последующие таблицы маршрутизации в остальных ЦКП составляются при установлении КВК для маршрутизации в сети ПД по логическим адресам служебных сообщений (по установлению/разъединению КВК и др.), информационных сообщений и их восстановлению при искажениях в канале связи. В составе приведенной строки маршрутизации в табл.2 для рассматриваемого примера КВК входят значения для входящих сообщений в оконечный ЦКП1.1 (ЦКП1.2) и для исходящих из него сообщений. Как видно из таблицы в первую строку входят значения для устанавливаемого КВК:

- 1) LCN входящего сообщения (9);
- 2) адрес источника поступления входящего сообщения (оконечный пункт);
- 3) LCN исходящего сообщения (2);
- 4) адрес поступления исходящего сообщения (имитатор канала 1121 (1222));
- 5) признак использования $O_{свн}$ LCN ЦКП (да или нет). При использовании свободного LCN при установлении КВК необходимо на этапе разъединении этого КВК откорректировать очереди $O_{свн}$ и $O_{зан}$. В данной строке таблицы при составлении входящего и исходящего сообщений ЗВ использовали $O_{свн}$ для LCN.

Таблица 2.

Таблица маршрутизации по логическим адресам в оконечных ЦКП1.1 (ЦКП1.2)

Входящее сообщение в оконечный ЦКП			Исходящее сообщение из оконечного ЦКП		
LCN	Освн	Адрес источника поступления	LCN	Освн	Адрес поступления (канальный регистр или оконечный пункт)
9	да	Окон. пункт	2	да	1121 (1222)
2	нет	1121 (1222)	9	нет	Окон. пункт
22	нет	1121 (1222)	5	да	Окон. пункт
5	нет	Окон. пункт	22	нет	1121 (1222)
11	да	Окон. пункт	21	да	1121 (1222)
21	нет	1121 (1222)	11	нет	Окон. пункт

3.2. Алгоритм установления КВК на абонентском участке оконечного пункта - назначения запроса на соединение

1. Зашифровать сообщение Запрос Вызова на установление КВК в ЦКП (ЦКЗ1.1 и ЦКПЗ.2) ключом Каб и предусмотреть проверку на целостность ключом Кцаб по протоколам с использованием индекса согласованных параметров SPI(A). Используются указанные ключи и протоколы, полученные при выполнении п.2.1 настоящего раздела. Отметим, что они могут отличаться на этом абонентском участке от используемых на абонентском участке оконечного пункта - источника запроса на соединение

2. Отправить ЗВ в оконечный пункт назначения (f).

3. Отправить ЗВ по открытому физическому адресу в оконечный пункт назначения (в примере f , адрес 501). Расшифровать и проверить целостность сообщения ЗВ в оконечном пункте.

3.3. Алгоритм подтверждения установления КВК на абонентском участке

Алгоритм ПО функции подтверждения установления КВК осуществляется передачей другого типа сообщения ВП (Вызов Принят) по тому же пути маршрутизации в противоположном направлении передаче сообщения Запрос Вызова. При этом коммутация сообщения ВП производится по логическим адресам LCN, а не по физическим адресам (как это имеет место при коммутации ЗВ). Ниже приводится последовательность этапов этого алгоритма на участке абонентского участка оконечного пункта - отправителя запроса на соединение.

Для этого необходимо составить еще одну строку таблицы 2 маршрутизации оконечных ЦКП1.1 (ЦКП1.2), соответствующую приему ВП от имитатора канала (буфера) и передаче сообщения ВП в оконечный пункт. Рассмотрим составление этой строки только в таблице 2, соответствующей передаче сообщения из оконечного пункта источника ЗВ в имитаторы каналов 1121, 1222.

1. В новой строке устанавливаются значение LCN=2 входящего ВП из канального процессора 1121 (1222) в оконечный ЦКП1.1 (ЦКП1.2), оконечного пункта в оконечный ЦКП, LCN=9 исходящего ВП в оконечный пункт. Признак использования Освн не относится ни к одному LCN.

2. На основании таблицы маршрутизации ЦКП1.1 и ЦКП1.2 (табл. 2) заменить в сообщении ВП LCN=2 на LCN=9;

3. Зашифровать и обеспечить целостность сообщения ВП теми же ключами и протоколами, что и сообщения ЗВ в разд. 3.1.

4. Отправить сообщение ВП в оконечный пункт с LCN=9.

5. Расшифровать и проверить целостность сообщения ВП в оконечном пункте. При этом используются те же ключи и протоколы, что и в разд. 3.1.

6. Назначить состояние КВК на оконечном пункте - 2 (КВК установлен).

4. Установление и подтверждение установления нескольких КВК

Приведенный выше алгоритм установленного соединения обозначим коммутируемым виртуальным каналом КВК1. В настоящем разделе приведем результаты установления и подтверждения установления еще двух КВК (КВК2 и КВК3). Рассмотрим составление дополнительной строки так же только в таблице 2, соответствующей передаче сообщения из оконечного пункта источника ЗВ в имитаторы каналов 1121, 1222.

4.1. Установление и подтверждение установления КВК2, инициатором которого является оконечный пункт, взаимодействующий с оконечными ЦКП3.1 и ЦКП3.2.

После завершения установления КВК1, описанного в разделах 2-5 состояние очередей $O_{свн}$ и $O_{зан}$ следующее.

Для оконечных ЦКП1.1 и ЦКП1.2 $O_{свн}$: {5; 11; 21; 18; 19...4; 7}. $O_{зан}$: {3; 1; 6...8; 10; 9; 2}.

После установления и подтверждения установления КВК2, инициатором которого является оконечный пункт, взаимодействующий с оконечными ЦКП3.1 и ЦКП3.2. состояние очередей $O_{свн}$ и $O_{зан}$ следующее.

Для оконечных ЦКП1.1 и ЦКП1.2 $O_{свн}$: {11; 21; 18; 19...4; 7}. $O_{зан}$: {3; 1; 6...8; 10; 9; 2; 5}.

Таблица маршрутизации 2 дополнена двумя строками маршрутизации для КВК2.

4.2. Установление и подтверждение установления КВК3, инициатором которого является оконечный пункт, взаимодействующий с оконечными ЦКП1.1 и ЦКП1.2.

После установления и подтверждения установления КВК3, инициатором которого является оконечный пункт, взаимодействующий с оконечными ЦКП1.1 и ЦКП1.2. состояние очередей $O_{свн}$ и $O_{зан}$ следующее.

Для конечных ЦКП1.1 и ЦКП1.2 $O_{свн}$: {18;.19...4; 7}. $O_{зан}$: {3; 1; 6...8; 10; 9; 2; 5; 11;.21}.

Таблица маршрутизации 2 дополнена двумя строками маршрутизации для КВКЗ.

Выводы

Приведенные общие положения алгоритмов позволяют проводить работы по созданию учебного лабораторного стенда сети передачи данных на базе виртуальных каналов с высокой информационной безопасностью и надежностью.

Выпущенные методические указания к лабораторным работам в этой области и создание лабораторного стенда могут быть использованы студентами для получения знаний, которые позволят использовать их для практических работ на предприятиях, создающих такие сети передачи данных.

В настоящее время работа по учебному лабораторному стенду сети передачи данных находится в состоянии практической реализации ПО функций установления/разъединения КВК, передачи данных и информационной безопасности. На данном этапе стенд представляет имитацию на одном компьютере одной из конфигураций сети ПД.

В УЛК могут использоваться так же стандартные и нестандартные протоколы безопасности, включая разработки студентов и аспирантов.

Литература

1. Матвеев В.А., Бельфер Р.А. Общие положения алгоритмов учебного лабораторного стенда сети передачи данных на базе виртуальных каналов. // Электросвязь –2016 –№8 –С. 51-55.
2. Бельфер Р.А., Зенькович С.А., Куянов М.С., Мерзляков Д.И. Алгоритм взаимной аутентификации на абонентском доступе сети передачи данных в учебном лабораторном стенде (настоящий сборник).
3. Матвеев В.А., Бельфер Р.А. Учебное пособие для разработки студентами программного обеспечения сети передачи данных и планирование создания лабораторного стенда сети с высоким уровнем безопасности и надежности //Сб. трудов XXV Всерос. конф. «Информатизация и информационная безопасность правоохранительных органов». – М.: Академия управления МВД России –2016, С. 51-55.
4. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи. Учебник для ВУЗов. Спб. // БХВ-Санкт-Петербург. –2011 –400 с.
5. Бельфер Р.А. Сети и системы связи (технологии, безопасность) /Учеб. пособие по дисциплине «Сети и системы связи»: электронное учеб. изд. //– М.: МГТУ им. Н.Э. Баумана –2012 –723 с.

Algorithm to Establish a Virtual Connection to the Subscriber in the Data Network of Laboratory Network Model

R.A. Belfer³⁴, R.S. Kulinich³⁵, E.P. Prischepin³⁶,

Abstract. An algorithm for establishing a switched virtual channel to the remote subscriber access site data network based on virtual channels. This algorithm is used to create a software-based security and reliability of one of the networks of educational laboratory bench data, which is in the implementation of the students of the department "Information Security" of the Bauman Moscow State Technical University.

Keywords: Switched Virtual Circuit, packet switching center, Information Security, data network.

³⁴ Belfer Reuben, Ph.D., Bauman Moscow State Technical University, Moscow, a.belfer@yandex.ru

³⁵ Kulinich Roman, Bauman Moscow State Technical University, Moscow, kulinichrs@gmail.com

³⁶ Prischepin Egor, Bauman Moscow State Technical University, Moscow, egor.prishchepin@gmail.com

Генерация узоров кровеносных сосудов человека для создания базы данных искусственных биометрических образов

Безик О.В.³⁷, Басараб М.А.³⁸

Предложен алгоритм синтеза цифровых изображений, содержащих узоры, имитирующие рисунок кровеносных сосудов ладони человека. Генерация двумерного рисунка сосудистого русла основана на рекурсивном алгоритме построения фрактального дерева Пифагора с ветвями, описываемыми кривыми Безье 4-го порядка. Разработанная программа «Pattern creator» позволяет автоматически создавать базы данных искусственных узоров кровеносных сосудов.

Ключевые слова: биометрическая аутентификация, рисунок кровеносных сосудов, фрактал, кривая Безье.

Введение

Создание больших естественных баз биометрических образов часто сталкивается с объективными трудностями, в связи с чем приходится прибегать к использованию искусственно синтезированных (синтетических) образов. Государственный стандарт ГОСТ Р 52633.2 [1] определяет требования к формированию баз искусственных биометрических образов, дополняющих неполную базу естественных образов «Свой» или «Чужой» до полной базы, используемой для тестирования средств высоконадежной биометрической аутентификации (СВБА).

Существует ряд решений для контролируемого обеспечения доступа с применением методов биометрической аутентификации по цифровому изображению рисунка сосудистого русла кровотока человека (сетчатка глаза, палец, наружная или тыльная сторона ладони) [2,3]. Однако, несмотря на наличие алгоритмов синтеза кровеносных узоров [4-6], не существует удовлетворительных решений, позволяющих в автоматическом режиме в необходимом объеме создавать базы данных, которые могут быть применены для тестирования СВБА. Некоторые алгоритмы предназначены для моделирования участков кровеносной системы в целях протезирования либо исследования процессов гемодинамики [7]. В связи с этим, разработка быстрых алгоритмов и программного инструментария такого рода представляют собой важную задачу.

1. Алгоритм генерации узора искусственных кровеносных сосудов

Рассмотрим способ создания уникальных двумерных искусственных узоров сосудистого русла пользователя, основанный на рекурсивном алгоритме построения фрактального множества «дерево Пифагора» (рис.1) [8]. Для создания реалистичных узоров кровеносных сосудов необходимо наделить дерево Пифагора дополнительными свойствами: различной длиной и шириной ветвей, изгибом, а также разнообразием углов их ветвления. С этой целью была модифицирована стандартная процедура построения обнаженного дерева Пифагора и получен алгоритм *Tree_vessels*. Рост новых ветвей происходит до тех пор, пока переменная длины ствола, l , не станет меньше либо равной переменной «ветвистости» дерева, Ψ , начальное значение которой выбирается случайно в диапазоне от 15 до 30.

³⁷ Безик Олег Викторович, МГТУ им. Н.Э. Баумана, г. Москва, o.bezick@yandex.ru

³⁸ Басараб Михаил Алексеевич, доктор физико-математических наук, профессор, МГТУ им. Н.Э. Баумана, г. Москва, basarab.iu8@gmail.com

На каждом новом уровне рекурсии толщина ветвей уменьшается на определенное значение. Для второго и последующих уровней рекурсии были введены два различных значения толщины правых и левых «поддеревьев», d_1 , d_2 , а также углы их роста, α_1 , α_2 , определяемые с помощью углов из предыдущего уровня рекурсии, с добавлением или вычитанием значений, полученных с помощью генераторов случайных чисел.

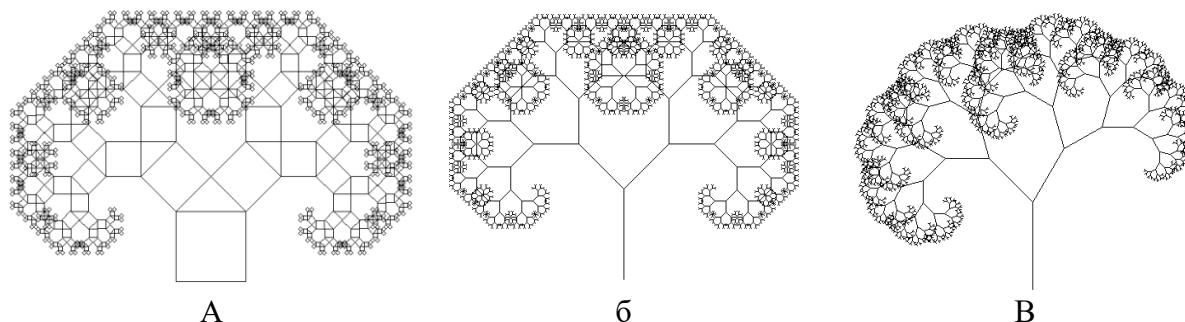


Рис. 1. Виды деревьев Пифагора: а) классическое дерево; б) обнаженное; в) обдуваемое обнаженное

Для имитации извилистости кровеносных сосудов были использованы кривые Безье 4-го порядка [9], задаваемые двумя конечными (P_0 и P_3) и двумя контрольными (C_1 и C_2) точками (рис. 2):

$$B(t) = (1-t)^3 P_0 + 3t(1-t)^2 C_1 + 3t^2(1-t) C_2 + t^3 P_3, \quad t \in [0; 1]. \quad (1)$$

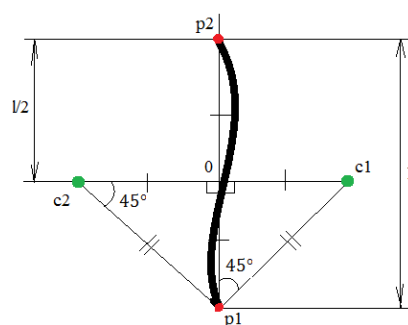


Рис. 2. Построение кривой Безье четвертого порядка в функции *Tree_vessels*

Итоговое обнаженное дерево Пифагора («сосудистое дерево») напоминает рисунок кровеносных сосудов ладони человека (рис. 3).

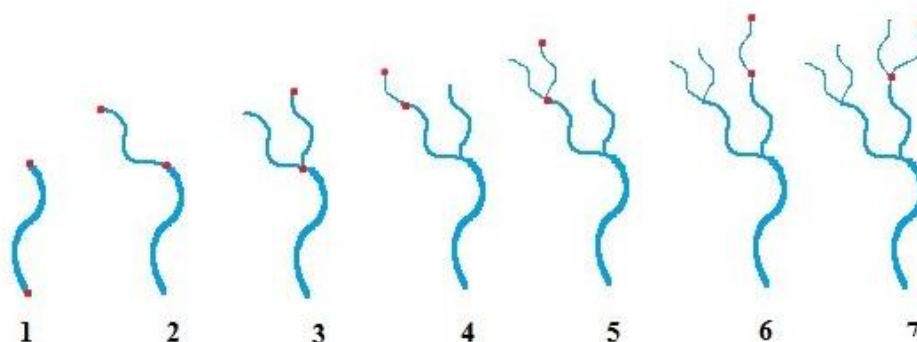


Рис. 3. Рост сосудистого дерева по алгоритму *Tree_vessels*

2. Программное обеспечение для генерации узоров искусственных кровеносных сосудов

Алгоритм *Tree_vessels* лёг в основу программы «Pattern creator», написанной на языке C# и позволяющей в автоматическом режиме создавать цифровые монохромные изображения узоров искусственных кровеносных сосудов. Результатом работы является база различных цифровых изображений в формате .bmp, размером 192x192 пикселя (рис. 4). Для придания узору большей реалистичности использовались три сосудистых дерева, построенных процедурой *Tree_vessels* с различными значениями переменных. Это позволило более тонко контролировать процесс роста дерева и создавать уникальные узоры кровеносных сосудов.

Наряду с углами роста и переменной Ψ были рандомизированы значения всех переменных, позволяющих влиять на форму сосудов. Случайным образом определялась первоначальная толщина ствола до ветвления, а координаты корневой точки случайным образом выбирались из множества точек, расположенных в нижней центральной части изображения, благодаря чему обеспечивался рост деревьев снизу-вверх.

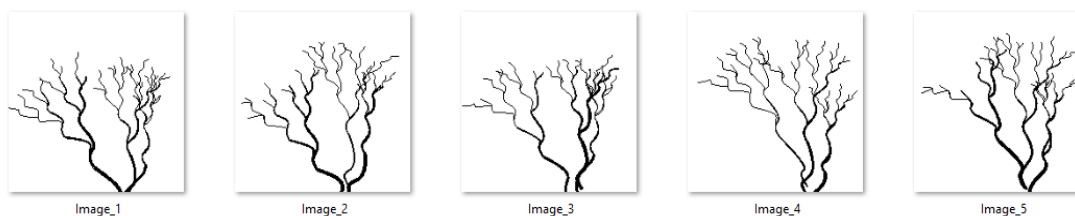


Рис. 4. Изображения с узором искусственных кровеносных сосудов, созданные с помощью программного обеспечения «Pattern creator»

Для оценки уникальности узоров были сгенерированы 3 независимых тестовых выборки по 300 изображений. Сравнивались фрактальная размерность Минковского D_M [8] и коэффициент заполнения, посчитанный по формуле:

$$K = m_T / N_T, \quad (2)$$

где m_T – количество пикселей, занимаемых на изображении T узорами сосудистого русла; N_T – общее количество пикселей изображения T .

Примерно в 15 % случаев было обнаружено совпадение коэффициента заполнения. Случаев совпадения фрактальной размерности Минковского зафиксировано не было, что говорит о полной уникальности сгенерированных изображений по этому показателю.

Выводы

Описан фрактальный алгоритм генерации сосудистого дерева. Разработанная программа позволила создавать цифровые изображения, содержащие уникальные узоры искусственных кровеносных сосудов. В качестве перспективы дальнейшего исследования рассматривается обобщение алгоритма на трехмерный случай.

Литература

1. ГОСТ Р 52633.2-2010. Защита информации. Техника защиты информации. Требования к формированию баз синтетических биометрических образов, предназначенных для тестирования средств высокондежной биометрической аутентификации.
2. Yousefi F., Analysis of methods for finger vein recognition // Thesis of the requirements for the degree of Master of Science in Medical Informatics Department, Middle East Technical University M.S., Department of Medical Informatics, November 2013.
3. Jadhav M., Nerkar P.M., FPGA-Based Finger Vein Recognition System for Personal Verification // Int. J. of Engineering Research and General Science, Vol. 3, Issue 4, Part-2, July-August, 2015.

4. Jimenez-Carretero D., San Jose Estepar R., Diaz Cacio M., Ledesma-Carbayo M.J., Automatic Synthesis of Anthropomorphic Pulmonary CT Phantoms // PLoS ONE 11(1): e0146060, doi:10.1371/journal.pone.0146060, 2016.
5. Ballerini L., Fiorini S., De Biasi M., Trucco E., Ruggeri A., Automatic Generation of Synthetic Retinal Fundus Images // STAG: Smart Tools & Apps for Graphics, 2014.
6. Lazaro S., Modelling of Realistic Blood Vessel Geometry // Bachelor Thesis, Hannover, September 28, 2011.
7. Tien J., Golden A.P., Tang M.D., Engineering of Blood Vessels // Department of Biomedical Engineering, Boston University, Boston, Massachusetts, 2005.
8. Морозов А.Д. Введение в теорию фракталов. – Москва-Ижевск: Институт компьютерных исследований, 2002.
9. Роджерс Д., Адамс Дж. Математические основы машинной графики. – М.: Мир, 2001.

Generation of Human Blood Vessels Patterns for Creation of a Database of Artificial Biometric Images

Bezick O.V.³⁹, Basarab M.A.⁴⁰

The main purpose of this study is to develop an algorithm of a creation of digital images, which would contain simulating human blood vessels patterns, which could be used for a revision of biometric authentication systems. There is a brief overview of Russian technical standards (GOST) that define the requirements for the formation of artificial biometrics images. We describe a unique algorithm for the generation of a two-dimensional picture of a vascular bed, based on a recursive algorithm for the construction of a naked Pythagoras tree, there is its pseudo. We present a developed in the framework of this research program «Pattern creator» which creates patterns of artificial blood vessels. We provide an estimation of a uniqueness of the artificial blood vessels generated by our program.

Keywords: biometric authentication, pattern of blood vessels, fractal, Besier curve.

³⁹ Oleg Bezick, Bauman Moscow State Technical University, Moscow, o.bezick@yandex.ru

⁴⁰ Mikhail Basarab – Dr. Sci. (Eng.), Professor, Bauman Moscow State Technical University, Moscow, basarab.iu8@gmail.com

Алгоритм взаимной аутентификации транспортной части сети передачи данных в учебном лабораторном стенде

Бельфер Р. А.⁴¹, Кулинич Р. С.⁴², Прищепин Е. П.⁴³

Приводятся общие положения алгоритмов установления соединения, используемых в учебном лабораторном стенде сети на базе виртуальных каналов. Для этих алгоритмов характерно выполнение высоких требований информационной безопасности и надежности. В настоящее время на кафедре “Информационная безопасность” МГТУ им. Н.Э. Баумана проводится работа по созданию учебного лабораторного стенда сети передачи данных. В данный момент работа находится в состоянии реализации алгоритмов, рассматриваемых в настоящей работе.

Ключевые слова: коммутируемый виртуальный канал, коммутация пакетов, коммутация каналов, центр коммутации пакетов, сеть энергосбережения

Введение

К некоторым технологическим сетям передачи данных (ПД) и сетям спецназначения предъявляют высокие требования по обеспечению информационной безопасности и надежности. Примером такой технологической сети является сеть энергосбережения smart grid [1,2]. В резолюции конференции «Информационной технологии на службе оборонно-промышленного комплекса России 2015» отмечается отсутствие популяризации отечественных разработок в области телекоммуникационного оборудования, слабой поддержки российских производителей со стороны государства; отсутствие единой современной системы объединенных коммуникаций в сфере ОПК [3]. Настоящая работа посвящена разработке взаимной аутентификации транспортной части сети передачи данных в учебном лабораторном стенде (УЛС). На участке между центрами коммутации необходимо реализовать алгоритмы:

согласования характеристик смежных ЦКП для взаимной аутентификации
передача ключа сквозного шифрования между ЦКП.
создания сессионных ключей

Конфигурация сети УЛС

На рис. 1 приведена конфигурация сети ПД УЛС, построенной на базе виртуальных каналов.



Рис.1. Конфигурация лабораторного стенда сети ПД

На (рис. 1) приведены следующие обозначения:

ЦКП – это центр коммутации пакетов;

a, b ... c – оконечные пункты одного абонентского доступа;

⁴¹ Бельфер Рувим Абрамович, доцент, МГТУ им. Н.Э. Баумана, к.т.н., a.belfer@yandex.ru

⁴² Кулинич Роман Сергеевич, МГТУ им. Н.Э. Баумана, kulinichrs@gmail.com

⁴³ Прищепин Егор Павлович, МГТУ им. Н.Э. Баумана, egor.prishchepin@gmail.com

d, e... f – оконечные пункты другого абонентского доступа;

1121, 2131, 1222, 2232 – каналы связи между ЦКП.

ЦКП составляют транспортную часть сети передачи данных УЛС.

2. Взаимная аутентификация смежных ЦКП

В разделе приводится описание одного из вариантов для УЛС алгоритма информационной безопасности (ИБ) – создание головных секретных ключей и взаимная аутентификация смежных ЦКП. Головные секретные ключи служат для создания ключей шифрования адресной части пакетов (канальное шифрование) и ключей целостности сообщений. Для принятой конфигурации сети ПД при отсутствии отказов каналов связи существуют два пути маршрутизации. Алгоритм рассматривается на примере установления коммутируемого виртуального канала (КВК) между оконечными пунктами а и f. При отсутствии отказов в каналах связи соединение производится по двум путям маршрутизации:

1) а – ЦКП1.1 – ЦКП2.1 – ЦКП3.1 – f;

2) а – ЦКП1.2 – ЦКП2.2 – ЦКП3.2 – f.

Для приведенного выше первого пути маршрутизации, в котором оконечный пункт а является источником сообщения запроса на установление КВК с оконечным пунктом f. (а – ЦКП1.1, ЦКП1.1 - ЦКП2.1, ЦКП2.1 - ЦКП3.1), (ЦКП3.1 - f). Предложения по алгоритмам ИБ на абонентских участках между оконечным пунктом и ЦКП приведены в работе [1].

2.1. Согласование характеристик, протоколов безопасности и параметров смежных ЦКП для взаимной аутентификации

Прежде, чем приступить к предлагаемым алгоритмам ИБ между смежными ЦКП необходимо из одного ЦКП смежному с ним ЦКП передать сообщение, включающее:

конфигурацию сети ПД (CON);

протоколы и параметры для согласования (т.е. создать защищенную связь или ассоциацию безопасности SA) [4,5]:

протоколы шифрования E (DES, TDEA, AES, ГОСТ 28147-89 и др.);

протоколы хеширования H (MD5, SH1 и др.);

длина ключа LK;

протоколы аутентификации сообщений (HMAC, MAC и др.);

длина профиля сообщений LH;

Установление защищенной связи состоит из ответного сообщения, включающего согласованные протоколы и параметры. Инициатором (I) первого сообщения является тот ЦКП, который ближе к оконечному пункту, отправившему запрос на установление коммутируемого виртуального канала. Для приведенного выше примера на участке ЦКП1.1 - ЦКП2.1 инициатором I является ЦКП1.1, а получателем (R) ЦКП2.1. На участке ЦКП2.1 - ЦКП3.1 инициатором является ЦКП2.1, а получателем (R) ЦКП3.1.

Приведем состав сообщений. Сообщение 1 от инициатора соединения (I) к приемнику (R): SAI = CON, E, H, LK, LH, CI=hash(ИЦИ, ИЦР). Здесь приняты обозначения: ИЦИ, - идентификатор ЦКП - инициатора, ИЦР - идентификатор ЦКП - получателя. Примем для УЛК идентификаторами ЦКП цифровые значения без точки. Сообщение 2 от R в I: R посылает: SAR=E, H, LK, LH, CR=hash(ИЦР, ИЦИ), CI=hash(ИЦИ, ИЦР), SPIa. Здесь так же ИЦ для одного сообщения относится к ЦКП1.1, а для другого - к ЦКП1.2. Все параметры в сообщении 2 являются согласованными.

2.2. Алгоритм создания головных ключей и взаимной аутентификации

2.2.1. Создание головных ключей

В разделе приводится описание алгоритма создания головного секретного ключа. Это одинаково относится к каждому из двух путей маршрутизации. Предлагаемый протокол включает обмен четырьмя сообщениями между смежными ЦКП. В нем используется

протокол Диффи-Хэллмана, для формирования общего секрета DH, а так же DHI – сообщение зашифрованное ключом источника и DHR – сообщение зашифрованное ключом получателя.

Полученное значение общего ключа смежных ЦКП (DH) используется для создания в этих ЦКП трех других общих ключей.

$$\text{KEYD} = \text{hash}(\text{KEY}|\text{DH}|\text{CI}|\text{CR}|), \text{ где } \text{KEY} = \text{hash}(\text{NI}|\text{NR}) \quad (6)$$

$$\text{KEYA} = \text{hash}(\text{KEY}|\text{KEYD}|\text{DH}|\text{CI}|\text{CR}|) \quad (7)$$

$$\text{KEYE} = \text{hash}(\text{KEY}|\text{KEYA}|\text{DH}|\text{CI}|\text{CR}|) \quad (8)$$

KEYE используется для шифрования сертификатов при взаимной аутентификации смежных ЦКП (сообщения 3 и 4).

KEYD используется для создания сессионного ключа канального шифрования Кцц адресной части заголовка сообщений и сессионного ключа Кццц его целостности.

KEYA используется для аутентификации и шифрования сообщений подготовки создания сессионных ключей Кцц и Кццц.

Сообщения 3 и 4 реализуют взаимную аутентификацию смежных ЦКП с использованием сертификатов.

2.2.2. Взаимная аутентификация ЦКП

Сообщение 3 I в R посылает:

сертификат I, зашифрованный ключом KEYE: $\text{KEYEPI}|\text{SU}|\text{CI}(\text{h}(\text{PI}))$, где PI - открытый ключ источника I, SU - закрытый ключ выдавшего сертификат удостоверяющего центра УЦ, h(PI) - хэш-функция PI. Для упрощения изложения в открытой части настоящего и всех остальных сертификатов оставим только один параметр - открытый ключ) и цепочку сертификатов. На приеме в R производится дешифрация сертификата I ключом KEYE и проверка подлинности открытого ключа I (PI);

цепочку из двух сертификатов, приведенных ниже. На приеме в R производится дешифрация сертификата I ключом KEYE и проверка подлинности открытого ключа I (PI) [4];

SI [h(DHI, DHR, CI, CR, SAI, ПЦИ)] - хэш-функция (DHI, DHR, CI, CR, SAI, ПЦИ), зашифрованная закрытым ключом источника I (SI). На приеме в R с помощью открытого ключа приемника PI производится проверка целостности значений DHI, DHR, CI, CR, SAI, ПЦИ. Успешная проверка показывает завершение аутентификации источника I.

Сообщение 4 R в I посылает:

сертификат R, зашифрованный ключом KEYE и цепочку сертификатов. На приеме в I производится дешифрация сертификата R и проверка подлинности открытого ключа R. Принцип алгоритма выполнения этих функций аналогичен обработке сертификатов в сообщении 3 и подлежит самостоятельной проработке;

SR h[(DHR, DHI, CR, CI, SAI, ПЦR)] - хэш-функция (DHR, DHI, CR, CI, SAI, ПЦR), зашифрованная закрытым ключом получателя R (SR). На приеме в I с помощью открытого ключа получателя PR производится проверка целостности значений DHR, DHI, CR, CI, SAI, ПЦR. Успешная проверка показывает завершение аутентификации получателя R и соответственно взаимной аутентификации смежных ЦКП.

2.2.3. Проверка целостности значений DHI, DHR, CI, CR, SAI, ПЦИ

Для разработки программного обеспечения, реализующего алгоритм проверки целостности значений DHI, DHR, CI, CR, SAI, ПЦИ в сообщении 3 SI [h(DHI, DHR, CI, CR, SAI, ПЦИ)] необходимо убедиться в том, что

$$\text{PI SI [h(DHI, DHR, CI, CR, SAI, ПЦИ)]} = \text{h(DHI, DHR, CI, CR, SAI, ПЦИ)}. \quad (18)$$

Как видно из этого равенства, необходимо вычислить хэш-функцию значения (DHI | DHR | CI | CR | SAI | ПЦИ), где "|" означает конкатенацию. Проверка производится после того, получатель R убедился в достоверности открытого ключа источника I (PI).

2.2.4. Проверка целостности значений DHI, DHR, CI, CR, SAI, ЦР

Для разработки программного обеспечения, реализующего алгоритм проверки целостности значений DHR, DHI, CR, CI, SAI, ЦР в сообщении 4 {SR h[(DHR, DHI, CR, CI, SAI, ЦР)]}, необходимо убедиться в том, что

$$\text{PRSR } h[(\text{DHR}, \text{DHI}, \text{CR}, \text{CI}, \text{SAI}, \text{ЦР})] = h[(\text{DHR}, \text{DHI}, \text{CR}, \text{CI}, \text{SAI}, \text{ЦР})].$$

(19)

Как видно из этого равенства, необходимо вычислить хэш-функцию значения (DHR | DHI | CR | CI | SAI | ЦР), где "|" означает конкатенацию. Проверка производится после того, инициатор I убедился в достоверности открытого ключа получателя R (PR).

2.3. Передача ключей сквозного шифрования между ЦКП

Для обеспечения ИБ информационной части пакета данных "из конца в конец" от источника к получателю в зашифрованном виде передается ключ шифрования информационной части пакета данных (КСКВ) и ключ целостности этих данных (КЦСКВ) [1]. Эти ключи передаются из ЦКП, который выполнял функцию получателя на предыдущем участке (абонентском или между смежными ЦКП) при установлении коммутируемого виртуального канала. После установления доверия открытого ключа получателя PR источник I отправляет в R два сообщения: PR(КСКВ) и PR(КЦСКВ). Получатель с помощью своего закрытого ключа SR расшифровывает КСКВ и КЦСКВ: SRPR(КСКВ) и SRPR(КЦСКВ). Для обеспечения целостности принятых ключей КСКВ и КЦСКВ источник I отправляет получателю R эти ключи, зашифровав их хэш-функцию своим закрытым ключом. На приеме это сообщение SI(h(КСКВ,КЦСКВ)) расшифровывается открытым ключом получателя

$$\text{PISI}(h(\text{КСКВ}, \text{КЦСКВ})) = h(\text{КСКВ}, \text{КЦСКВ}), \quad (20)$$

что позволяет проверить целостность ключей КСКВ и КЦСКВ.

На участке между смежными ЦКП создаются сессионный ключ канального шифрования адресной части заголовка пакета данных Кцц и сессионный ключ целостности Кццц.

3. Создание сессионных ключей

3.1. Согласование протоколов безопасности и параметров смежных ЦКП для создания сессионных ключей

Прежде, чем приступить к созданию сессионных ключей между смежными ЦКП необходимо согласовать протоколы безопасности и параметры, т.е. создать защищенную связь или ассоциацию безопасности (SA) [3]:

- протоколы шифрования;
- протоколы аутентификации;
- протоколы хеширования;
- длина ключа LK;
- длина профиля сообщений LH;

Установление защищенной связи состоит из обмена тремя сообщениями.

Сообщение 1 от инициатора соединения (I) к приемнику (R): SAI, CI XOR CR, NI, Hash1. Здесь приняты обозначения: SAI - предлагаемые для согласования протоколы и параметры, CI и CR, - приведены выше значения, NI - случайное число. Hash1 - функция хеширования используется получателем при приеме сообщения для аутентификации источника.

Сообщение 2 от R в I: R посылает: SARR, CI + CR, NRR, Hash2. Здесь приняты обозначения: SARR - согласованные протоколы и параметры, а так же SPIS (Security Parameter Index) - индекс согласованных параметров получателя и источника на этапе создания сессионных ключей.

CI и CR, - приведены выше значения, NRR - случайное число. Hash2 - функция

хеширования используется источником при приеме сообщения для аутентификации получателя.

Сообщение 3 от I в R: I посылает: CI + CR, NRR, Hash3. Hash3 - функция хеширования используется источником для подтверждения аутентификации получателя.

Алгоритм использования функций хеширования Hash1, Hash2, Hash3 для аутентификации подлежит согласованию. При этом во всех случаях общими ключами источника и получателя является ключ KEYA, создание которого приведено ранее в разделе "Алгоритм создания головных ключей и взаимной аутентификации смежных ЦКП".

1.3.2 Создание сессионных ключей

Как отмечено в работе [2], в смежных ЦКП для шифрования/дешифрования адресной части сообщений создаются сессионный ключ канального шифрования Кцц и для обеспечения их целостности - сессионный ключ целостности Кццц. Как было отмечено выше (раздел разделе "Алгоритм создания головных ключей и взаимной аутентификации смежных ЦКП") для этой цели используется ключ KEYD.

$$Кцц = h(KEYD | SPIS | NII | NRR). \quad (21)$$

$$Кццц = h(KEYD | SPIS | NRR | NII). \quad (22)$$

Эти ключи периодически регенерируются, не проводя при этом расчет ключа KEYD. При регенерации используются другие случайные числа NII и NRR.

Ключ KEYD в открытом виде не хранится, а шифруется в с помощью открытого ключа в I и расшифровывается с помощью закрытого ключа в I.

Длина ключей выбирается в зависимости от принятого протокола шифрования. При этом необходимо учесть, что бы длина профиля сообщения была равна длине ключа протокола шифрования. Примером несовпадения может быть например длина ключа протокола шифрования DES равна 56 бит, а длина профиля сообщения протокола MD5 равна 128 бит.

Аналогичная процедура производится в получателе R.

Выводы

Приведенные общие положения алгоритмов позволяют проводить работы по созданию учебного лабораторного стенда сети передачи данных на базе виртуальных каналов с высокой информационной безопасностью и надежностью.

Выпущенные методические указания к лабораторным работам в этой области и создание лабораторного стенда могут быть использованы студентами для получения знаний, которые позволят использовать их для практических работ на предприятиях, создающих такие сети передачи данных. В настоящее время работа по учебному лабораторному стенду сети передачи данных находится в состоянии практической реализации ПО функций установления/разъединения КВК, передачи данных с учетом обеспечения информационной безопасности.

На данном этапе стенд представляет имитацию на одном компьютере приведенной на рисунке 1 одной из конфигураций сети ПД.

В УЛК могут использоваться так же стандартные и нестандартные протоколы безопасности, включая разработки студентов и аспирантов.

Литература

1. Матвеев В.А., Бельфер Р.А. Общие положения алгоритмов учебного лабораторного стенда сети передачи данных на базе виртуальных каналов. // Электросвязь –2016 –№8 –С. 51-55.
2. Бельфер Р.А., Зенькович С.А., Куянов М.С., Мерзляков Д.И. Алгоритм взаимной аутентификации на абонентском доступе сети передачи данных в учебном лабораторном стенде (настоящий сборник).
3. Матвеев В.А., Бельфер Р.А. Учебное пособие для разработки студентами программного обеспечения сети передачи данных и планирование создания лабораторного стенда сети с высоким уровнем

безопасности и надежности //Сб. трудов XXV Всерос. конф. «Информатизация и информационная безопасность правоохранительных органов». – М.: Академия управления МВД Россия –2016, Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи. Учебник для ВУЗов. СПб. // БХВ- Санкт-Петербург. –2011 –400 с.

Бельфер Р.А. Сети и системы связи (технологии, безопасность) /Учеб. пособие по дисциплине «Сети и системы связи»: электронное учеб. изд. //– М.: МГТУ им. Н.Э. Баумана –2012 –723 с.

Algorithm of the Mutual Authentication in the Transport Data Network Model

R.A. Belfer⁴⁴, R.S. Kulinich⁴⁵ E.P. Prischepin⁴⁶

We give the general provisions of the mutual authentication algorithms used in the model of network based on virtual channels. The network characterized on high information security requirements. Currently, the department "Information Security" Bauman MSTU is working on the creation of educational model of data network and is in the implementation under consideration in the algorithms.

Key words: Switched Virtual Circuit, packet switching center Information Security, smart grid, Information Security, reliability, data network.

⁴⁴ Belfer Reuben, Ph.D., Bauman University, a.belfer@yandex.ru

⁴⁵ Kulinich Roman, Bauman Moscow State Technical University, kulinichrs@gmail.com

⁴⁶ Prischepin Egor, Bauman Moscow State Technical University, egor.prishchepin@gmail.com

Обеспечение информационной безопасности дистанционного банковского обслуживания
Бердюгин А.А.⁴⁷

***Аннотация.** В статье рассматриваются вопросы внедрения в кредитных организациях технологии дистанционного банковского обслуживания (ДБО) и появление новых источников банковских рисков, на которые в большей степени оказали влияние технологии ДБО. Приведены последствия распространения компьютерных преступлений, определены актуальные задачи в сфере безопасного применения технологий ДБО.*

***Ключевые слова:** дистанционное банковское обслуживание, Интернет, компьютерные преступления, кредитная организация, информационная безопасность.*

Введение

Сегодня Интернет предоставляет необъятный массив информации, открывающий широкие возможности для развития бизнеса. Банковская деятельность чрезвычайно консервативна и, казалось бы, она менее всего нуждается в новациях в части применения новых технологий и инструментария. Тем не менее именно банковское сообщество в наш информационный век весьма активно и заинтересованно откликнулось на возможности использования новых достижений в области информационных технологий и средств связи. Кредитные организации нашли в информационных технологиях не только действенное средство учета, мониторинга, контроля за движением и хранением мировых денежных потоков, но и мощнейший инструмент воздействия на существование самой денежно-финансовой и банковской системы, средство защиты этой системы и ее участников, а также эффективный инструмент регулирования сложных банковских процессов [1].

Развитие рынка – стремительное, потенциал – огромный

Электронный контент производится и потребляется сегодня с огромной скоростью. По данным последнего пресс-релиза Международного союза электросвязи (МСЭ) за июль 2016 г., количество пользователей интернета в мире составляет 3,5 миллиарда человек. По оценке ООН, численность мирового населения в 2015 году достигла 7,3 миллиарда. В период с 2000 по 2015 год удельный вес пользователей интернета увеличился почти в семь раз – с 6,5 до 43 процентов мирового населения. По оценкам экспертов рынка, потенциал развития интернет-банкинга огромен. Аудитория российской зоны Интернета уже сейчас насчитывает более 30 млн пользователей и, согласно данным опросов, каждый третий готов управлять своим банковским счетом через Сеть. Рынок интернет-торговли увеличивается на 30–50% ежегодно, а число абонентов мобильной связи уже существенно превышает численность населения России. Можно утверждать, что прирост клиентской базы через мобильные сервисы значительно увеличится в ближайшие годы [3]. Формируется благоприятная почва для развития электронных платежных сервисов. Однако при работе банка с клиентами проблемы обслуживания – отнюдь не редкость. Это доказывают даже звонки в колл-центры кредитных организаций.

Проблемы и задачи

Наряду с очевидными преимуществами ДБО приносит и ряд проблем:

- технологический прогресс в банковской сфере обуславливает постоянное отставание нормативной базы, регламентирующей данный бизнес;

⁴⁷ Бердюгин Александр Александрович, Финансовый университет при Правительстве Российской Федерации, Москва, a40546b@gmail.com

- применение новых технологий для выполнения банковских операций и обслуживания клиентов может снизить надежность и устойчивость кредитных организаций;

- технологические нововведения в банковской деятельности могут привести к ослаблению контроля над кредитными организациями со стороны регулятора.

Отсюда вытекают самые неотложные задачи в сфере безопасного применения технологий ДБО:

- совершенствование нормативной базы;

- адаптация контроля надежности банковских автоматизированных систем к условиям ДБО;

- повышение качества подготовки специалистов регулирующих и контрольных органов в сфере ДБО.

Помимо этого, надзорные и регулирующие органы должны обеспечить юридическую основу, которая сделает дистанционные платежи полностью легитимными. Она может включать:

- законодательство, регулирующее услуги денежных переводов с низким риском (переводы небольших денежных сумм, не предусмотренные традиционным банковским законодательством);

- разрешение небанковским организациям осуществлять транзакции (банковскому агенту или провайдеру денежных переводов принимать наличные, поступающие с электронных устройств);

- по возможности, реализация законодательных актов в виде системы, не затрагивающей потребительский интерфейс [2].

Мошенничество и безопасность информации в системах ДБО

За 6–7 лет мошенничество в системах ДБО прошло путь от единичных случаев до криминального бизнеса с оборотом примерно 100 млн долл. в год. В нашей стране все начиналось в 2006–2007 гг. с редких краж средств банковских клиентов – физических лиц. Тогда это было легко: банки, заботясь об удобстве работы клиентов, для подтверждения платежа в большинстве случаев требовали ввести лишь обычный пароль, который можно было узнать, установив и настроив кейлоггер⁴⁸. Скретч-карты⁴⁹, ключи электронно-цифровой подписи (ЭЦП), отправка одноразовых паролей на мобильный телефон широкого распространения не имели – поддержка таких средств защиты была реализована в ДБО ограниченного числа банков. Мошенники могли украсть у одного клиента лишь небольшую сумму, что было связано с ограничениями на сумму платежа, которые устанавливали сотовый оператор и банк. Отличительная особенность мошеннических платежей того времени – преступники, перестраховываясь, работали в системе ДБО через анонимные прокси-серверы, находящиеся в других странах. Это, с одной стороны, в немалой степени затрудняло работу правоохранительных органов в проведении оперативно-розыскных мероприятий. С другой стороны, эта особенность позволяла антифрод-системам (системам обнаружения мошеннических платежей в ДБО) просто и эффективно обнаруживать факт хищения средств. Ограниченность функций ДБО физических лиц не позволяла злоумышленникам воспользоваться всеми преимуществами дистанционного обслуживания, в частности, перечислять большие суммы непосредственно на банковские карты. Поэтому функции специализированного программного обеспечения, с помощью

⁴⁸ Кейлоггер (от англ. key – клавиша и logger – регистрирующее устройство) – программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя: нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д.

⁴⁹ Скретч-карта (scratch card) – карта из картона или пластика с нанесенной на ней (под защитным непрозрачным и стирающимся слоем) некой секретной информацией.

которого похищались данные для аутентификации в ДБО, расширились – помимо логина и пароля злоумышленники могли копировать файлы, содержащие ключи ЭЦП.

Автоматизация криминала

Развитие программного обеспечения, используемого злоумышленниками, дало возможность автоматизировать кражи секретной информации клиента, требуемой для входа и создания платежа в системе ДБО (т. е. логина, пароля, секретного ключа клиента, а также IP-адреса сервера ДБО, с которым работает клиент). Вся собранная информация автоматически интегрировалась на центральном сервере, и преступникам достаточно было последовательно заходить в систему ДБО под собранными учетными записями клиентов и выводить средства с их счетов. Ущерб от мошенничества в ДБО уже в 2009 г. возрос практически в три раза, что заставило кредитные организации создавать внутренние подразделения для контроля транзакций. Тогда же стали разрабатываться первые автоматизированные системы мониторинга транзакций. И все же гораздо большую угрозу информационной безопасности в системах ДБО представляет утечка конфиденциальной информации, произошедшая из-за халатности или в результате злонамеренных действий инсайдеров. Как показывают экспертные опросы, более всего банки озабочены прямыми финансовыми убытками от утечки конфиденциальной информации (46,0%). На втором месте – ухудшение имиджа и общественного мнения (42,3%), на третьем – потеря клиентов (36,9%), далее идут снижение конкурентоспособности (25,2%), юридические издержки (10,0%) и др.

Выводы

Из вышесказанного следуют выводы:

- современный банковский бизнес будет стремиться расширять применение дистанционных банковских услуг;
- коммерческие банки будут вынуждены конкурировать с различными организациями, осуществляющими аналогичные услуги и постоянно снижающими комиссию за транзакции;
- регулирующим органам следует в кратчайшее время принять необходимые нормативные и законодательные акты в сфере ДБО;
- идеальных способов и средств обеспечения информационной безопасности в сетевых структурах до настоящего времени не существует. Каждое из возможных средств защиты имеет индивидуальные недостатки;
- с клиентами кредитных организаций, пожелавшими использовать технологии ДБО, следует проводить разъяснительную работу и инструктажи по порядку хранения носителей с конфиденциальной информацией, а также информировать их о наиболее распространенных способах мошенничества в системах ДБО;
- необходимо совершенствовать способы наблюдения и контроля со стороны регулирующих и надзорных органов за применением банковскими организациями технологий ДБО (включая возможность их использования в целях легализации преступных доходов).

Проблем, сложностей и рисков, возникающих в связи с внедрением интернет-технологий в банковскую сферу, немало. Но очевидно также, что потребность в наличных деньгах будет постоянно уменьшаться – их в определенной степени заменят электронные деньги.

Литература

1. Интернет-технологии в банковском бизнесе: перспективы и риски : учебно-практическое пособие / Ю. Н. Юденков, Н. А. Тысячникова, И. В. Сандалов, С. Л. Ермаков. – 2-е изд., стер. – М. : КНОРУС, 2014.
- 2 *Кинг Бретт*. Банк 3.0. Почему сегодня банк – это не то, куда вы ходите, а то, что вы делаете. – М.: ЗАО «Олимп – Бизнес», 2014. – 520 с.

3. Горчакова М. Е. Дистанционное банковское обслуживание : учебное пособие. – Иркутск : Изд-во БГУЭП, 2009.

4. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. – СПб. : Питер, 2008.

5. Ревенков П.В., Бердюгин А.А. Основные направления обеспечения кибербезопасности в условиях ДБО // Банковское дело. 2015. № 7 (259). С. 66-71.

Рецензент: Алексей Сергеевич Марков, доктор технических наук, старший научный сотрудник, профессор кафедры ИУ-8 МГТУ им.Н.Э.Баумана, a.markov@bmstu.ru

Providing Information Security of Remote Banking Services

Berdyugin A.⁵⁰

Abstract. This article discuss the challenges of introduction in the credit institutions of technology remote banking service (RBS), the emergence of new sources of banking risks, which are more influenced by technologies RBS. Are adduced the consequences of the spread of computer crimes and urgent themes in the field of the safe use of technologies RBS.

Keywords: remote banking services, Internet, computer crimes, credit institution, information security.

УДК 621.391

Алгоритм взаимной аутентификации на абонентском доступе сети передачи данных в учебном лабораторном стенде

Бельфер Р.А.⁵¹, Куянов М.С.⁵², Мерзляков Д.И.⁵³ Зенькович С.А.⁵⁴

Приводится алгоритм взаимной аутентификации абонентского доступа сети передачи данных на базе виртуальных каналов. Этот алгоритм служит для создания программного обеспечения информационной безопасности и надежности одной из сетей передачи данных учебного лабораторного стенда, который находится в состоянии реализации студентами кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана.

Ключевые слова: Switched Virtual Circuit (коммутируемый виртуальный канал), центр коммутации пакетов ЦКП, smart grid (сеть энергосбережения), Information Security (информационная безопасность), reliability (надежность), data network (сеть передачи данных).

Введение

В работах [1,2] показана актуальность проводимых преподавателями и студентами кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана работ по созданию учебного лабораторного стенда сети (УЛС) с высоким уровнем безопасности, надежности и другим характеристикам. При этом отмечается, что полученные знания и опыт по созданию УЛС могут быть использованы при разработках отечественных сетей связи в сети

⁵⁰ Berdyugin Alexander Alexandrovich, Financial University under the Government of the Russian Federation, Moscow, a40546b@gmail.com

⁵¹ Бельфер Рувим Абрамович, МГТУ им. Н.Э. Баумана, к.т.н., a.belfer@yandex.ru

⁵² Куянов Максим Сергеевич, МГТУ им. Н.Э. Баумана, m_aksakov@mail.ru

⁵³ Мерзляков Даниил Иванович, МГТУ им. Н.Э. Баумана, merzdan@gmail.com

⁵⁴ Зенькович Станислав Александрович, МГТУ им. Н.Э. Баумана, stanislav.zen@ya.ru

энергосбережения [3-5]. Это же относится и к службе оборонно-промышленного комплекса России [6]. В работе [2], посвященной общим положениям алгоритмов учебного лабораторного стенда сети передачи данных (ПД) на базе виртуальных каналов. В настоящей работе предлагается один из возможных алгоритмов создания способов обеспечения информационной безопасности (ИБ) абонентского доступа одной из конфигураций приведенной в этой работе сети ПД. Рассмотрению подлежат следующие способы обеспечения ИБ из приведенных в Рекомендации Международного Союза Электросвязи (ITU-T) E.408 – аутентификация, неотказуемость авторства, конфиденциальность данных, безопасность связи, целостность данных, готовность [7].

1. Конфигурация сети

На рис. 1 приведена конфигурация сети ПД учебного лабораторного стенда, на которой рассматриваются поставленные в настоящей работе задачи.

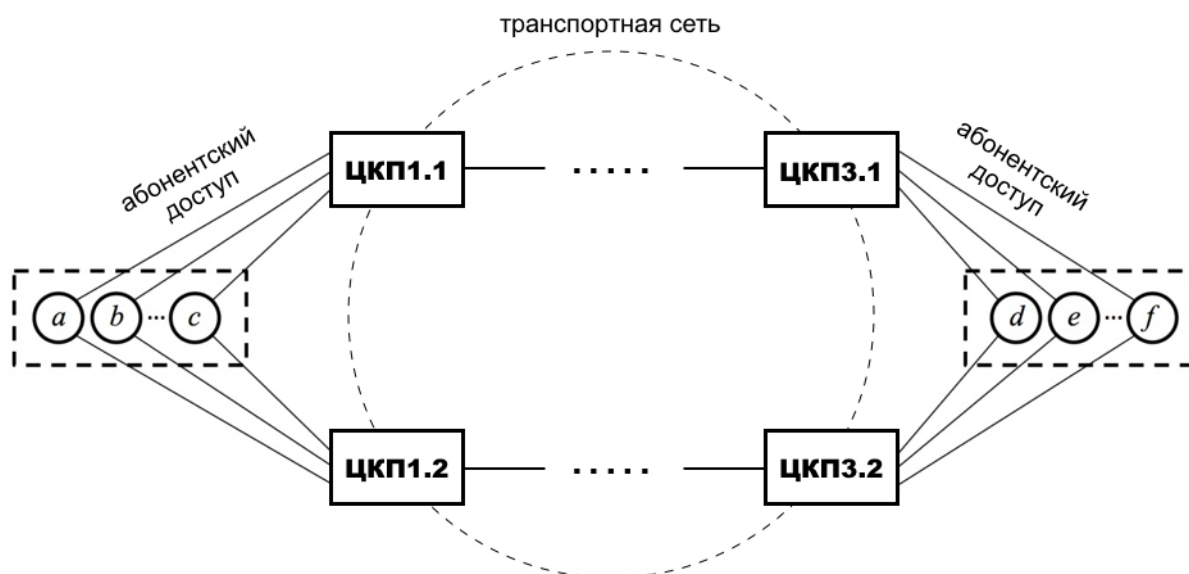


Рис. 1. Конфигурация сети ПД

Как видно из рисунка, надежность обеспечивается дублированием путей маршрутизации. Сеть ПД состоит из абонентского доступа и транспортной сети. Каждый путь маршрутизации состоит из трех центров коммутации пакетов в каждом. К двум оконечным ЦКП подключены оконечные пункты. Доступ оконечных пунктов (a,b,...c, d,e,...f) к центру коммутации пакетов удаленный. Оконечные пункты на участке абонентского доступа (между оконечным пунктом и ЦКП) для обеспечения требований надежности обмениваются данными одновременно по двум ветвям.

В настоящей работе в УЛС на участке абонентского доступа сети ПД на базе виртуальных каналов рассматриваемой конфигурации предлагается алгоритм взаимной аутентификации оконечного пункта и оконечного ЦКП (абонентский доступ). Работа относится к первому этапу создания УЛС, когда программное обеспечение абонентского доступа и транспортной сети ПД в одном компьютере.

2. Взаимная аутентификации оконечного пункта и ЦКП

2.1. Согласование характеристик, протоколов безопасности и параметров взаимодействующих узлов абонентского доступа

Как отмечено в [2], таких сетей ПД в УЛС могут быть несколько и каждая с различными требованиями ИБ, надежности и других характеристик. Эти сети могут

отличаться конфигурацией (обозначим через CON). ЦКП и взаимодействующий с ним оконечный пункт создают защищенную связь (ассоциацию безопасности SA, Security Association) [7], согласовывая протоколы и параметры:

- 1) протоколы шифрования E (DES, TDEA, AES, ГОСТ 28147-89 и др.);
 - 2) протоколы хэширования H (MD5, SHA1 и др.);
 - 3) протоколы аутентификации сообщений (HMAC, MAC и др.)
 - 4) длина ключа L_K ;
 - 5) длина профиля сообщений L_H ;
- и другие параметры.

В УЛК могут использоваться так же нестандартные протоколы, включая разработки студентов и аспирантов.

Все SA хранятся в базе данных. Каждый SA имеет маркер данных, включающий:

- индекс SPI (Security Parameter Index), включающий набор характеристик, протоколов безопасности, параметров и идентификатор конфигурации сети CON;
- адрес источника и пункта назначения. Обозначим источник сообщения (оконечный пункт) через I. Например, на принятой конфигурации сети рис.1 оконечный пункт *a* посылается первое сообщение с набором SPI в два адреса – ЦКП1.1 и ЦКП1.2). Обозначим получатели этого сообщения (в принятой конфигурации сети ЦКП1.1 и ЦКП1.2) через R. В ответ на принятое сообщение в адрес оконечного пункта (в примере в оконечный пункт *a*) из каждого получателя R отправляется согласованный набор характеристик, протоколов безопасности и параметров. Обозначим индекс согласованного набора характеристик, протоколов безопасности и параметров через индекс согласованных параметров безопасности SPI(A).

В настоящей работе в УЛК рассматривается сеть ПД на базе виртуальных каналов, соединение в которой называется коммутируемым виртуальным каналом (КВК).

Установление SA на абонентском участке инициатора установления КВК предшествует взаимной аутентификации на абонентском участке. Примем, что таким инициатором является пункт *a* (рис.1). Алгоритм установления SA в этом случае следующий.

Сообщение 1 от инициатора согласования I посылается (для принятой конфигурации посылает два сообщения – в ЦКП1.1 и в ЦКП1.2): приемнику (R): CON, E, H, L_K , L_H , $C = \text{hash}(\text{АДР}_O, I_{Ц})$. Здесь приняты обозначения: АДР_O – адрес оконечного пункта (в примере адрес пункта *a*), $I_{Ц}$ – идентификатор ЦКП. Поскольку оконечный пункт принятой конфигурации взаимодействует с двумя ЦКП, то для одного сообщения $I_{Ц} = 1$ относится к ЦКП1.1, а $I_{Ц} = 2$ для ЦКП1.2).

Сообщение 2 от R в I (для принятой конфигурации посылает два сообщения – от ЦКП1.1 и от ЦКП1.2): CON, E, H, L_K , L_H , $C = \text{hash}(I_{Ц}, \text{АДР}_O)$, SPI(A). Все параметры в сообщении являются согласованными. SPI(A) – индекс согласованных параметров получателя и источника используется при передаче пакетов данных по установленному соединению.

Рассмотрим установление SA на абонентском участке пункта назначения установления КВК. Для принятой конфигурации и рассматриваемого примера установления КВК таким участком абонентского доступа примем взаимодействие ЦКП3.1 и ЦКП3.2 с оконечным пунктом *f* (рис.1). Это следует после успешного завершения взаимной аутентификации на абонентском участке источника установления КВК и производится на этапе установления КВК.

Возможны два варианта установления SA в этом случае. В первом варианте функцию источника I первого сообщения выполняет оконечный пункт назначения при установлении КВК (в данном примере оконечный пункта *f*). При этом следует из оконечных ЦКП (в примере ЦКП3.1 и ЦКП3.2) передать в оконечный пункт назначения сообщение о

поручении полномочий инициатора согласования SPI. После получения этого сообщения алгоритм согласования характеристик, протоколов безопасности и параметров взаимодействующих узлов абонентского доступа не отличается от приведенного выше. При этом следует учесть другие идентификаторы: $I_{ц}=31$ относится к ЦКПЗ.1, а $I_{ц}=32$ для ЦКПЗ.2).

Во втором варианте функцию источника I первого сообщения выполняют оконечные ЦКП (в примере ЦКПЗ.1 и ЦКПЗ.2), функцию получателя R – оконечный пункт (в примере – f).

Сообщение 1 от I в R (для принятой конфигурации посылает два сообщения – от ЦКПЗ.1 и от ЦКПЗ.2) совпадает по составу с предыдущим сообщением 2, за исключением, отсутствия SPI(A) – индекса согласованных параметров.

Сообщение 2 от R в I совпадает по составу с предыдущим сообщением 1, за исключением, включения дополнительно SPI(A) – индекса согласованных параметров других идентификаторов $I_{ц}=31$ относится к ЦКПЗ.1, а $I_{ц}=32$ для ЦКПЗ.2).

2.2. Алгоритм взаимной аутентификации оконечного пункта и ЦКП, создание головного ключа

Ниже приводится описание для рассматриваемой конфигурации УЛС алгоритма взаимной аутентификации оконечного пункта и двух подключенных к нему удаленным доступом ЦКП, создание головного секретного ключа. Рассматривается конфигурация сети ПД с дублированием путей маршрутизации, что требует взаимную аутентификацию одного оконечного пункта с каждым из двух взаимодействующих с ним ЦКП. Головной секретный ключ служит для создания ключей канального и сквозного шифрования и ключа целостности сообщений.

На абонентском участке, иницирующего установление КВК, оконечный пункт направляет в оба оконечных ЦКП (в конфигурации рис.1 ЦКП1.1 и ЦКП1.2) сообщение Запрос Вызова (ЗВ) на установление КВК. Это сообщения коммутируются в транспортной сети и поступают на оконечные ЦКП абонентского участка пункта назначения (в конфигурации рис.1 ЦКПЗ.1 и ЦКПЗ.2).

Предлагаемый протокол включает обмен двумя типами сообщений между оконечным пунктом и каждым из оконечных ЦКП.

Инициатором первого типа сообщения протокола взаимной аутентификации на абонентском участке является оконечный ЦКП. Обозначим его I. Для принятой дублированной схемы таких сообщений два – по числу оконечных ЦКП на каждом абонентском доступе. Приемник этого сообщения (оконечный пункт) обозначим R.

Сообщение 1 I в R посылает:

- сертификат источника I, полученный в удостоверяющем центре УЦИ – УЦИ $\langle\langle I \rangle\rangle = P_I S_{УЦИ}(h(P_I))$, где P_I – открытый ключ источника I, $S_{УЦИ}$ – $S_{УЦИ}$ – закрытый ключ УЦИ, $h(P_I)$ – хэш-функция P_I . Для упрощения изложения в открытой части сертификатов оставим только один параметр – открытый ключ.
- цепочку из двух сертификатов, приведенные ниже в следующем разделе. На приеме производится проверка подлинности открытого ключа I (P_I) [7];
 i – случайное число, сгенерированное I для защиты от угрозы «повтор аутентификации».

Сообщение 2 R в I посылает:

- сертификат R и цепочку сертификатов. На приеме в I производится проверка подлинности открытого ключа I;
 r – случайное число, сгенерированное R для защиты от угрозы «повтор аутентификации»;

головной секретный ключ K , зашифрованный открытым ключом I (т.е. P_I). K – случайное число, сгенерированное R . На приеме в I производится расшифровывание главного секретного ключа K закрытым ключом источника S_I .

- S

R

h

R На приеме в I производится проверка, является ли значение R_I тем же самым, которое было отправлено в сообщении 1 (защита от угрозы «повтор аутентификации»).

Успешная проверка принятого сообщения завершает аутентификацию получателя R .

Сообщение 3 I в R посылает:

- S – хэш-функция (R_I, R_R, K) , зашифрованная закрытым ключом получателя S_R . На приеме в I с помощью открытого ключа получателя P_R производится проверка целостности значений R_I, R_R, K ;
- R_R . На приеме в R производится проверка, является ли значение R_R тем же самым, которое было отправлено в сообщении 2 (защита от угрозы «повтор аутентификации»);
- K – хэш-функция (R_R, K) , зашифрованная закрытым ключом источника S_I . На приеме в R с помощью открытого ключа источника P_I производится проверка целостности значений R_R, K .

Успешная проверка принятого сообщения завершает аутентификацию получателя R .

2.3. Алгоритм проверки подлинности открытых ключей сертификатов

Из приведенного алгоритма взаимной аутентификации окончного пункта и ЦКП рассматриваемого варианта УЛС следует: а) разработать алгоритм проверки подлинности открытых ключей источника и получателя; б) составить и отладить программное обеспечение этого алгоритма.

Для разработки программного обеспечения, имитирующего алгоритм протокола взаимной аутентификации окончного пункта и ЦКП необходимо составить программное обеспечение, имитирующее сертификаты:

1. источника, выданный в удостоверяющем центре УЦИ;
2. получателя, выданный в удостоверяющем центре УЦР;
3. общего удостоверяющего центра УЦО, выданный в удостоверяющем центре УЦР;
4. удостоверяющего центра УЦИ, выданный в общем удостоверяющем центре УЦО;
5. общего удостоверяющего центра УЦО, выданный в удостоверяющем центре УЦИ;
6. удостоверяющего центра УЦР, выданный в общем удостоверяющем центре УЦО;

При составлении ПО, имитирующего сертификат, необходимо: создать открытый и закрытый ключ сертификата; вычислить хэш-функцию открытого ключа сертификата; произвести шифрование закрытым ключом удостоверяющего центра (выдавшего сертификат) хэш-функцию открытого ключа.

Приведем алгоритм проверки подлинности открытого ключа I (P_I) в сообщении 1. Допустим, что I отправил следующие сертификаты. Для упрощения в составе сертификатов оставим только один параметр – открытый ключ.

R получил сертификат I , выданный в удостоверяющем центре УЦИ – УЦИ $\langle\langle I \rangle\rangle = P_I S_{уци}(h(P_I))$. Здесь $S_{уци}$ – закрытый ключ УЦИ, $h(P_I)$ – хэш-функция P_I .

R получил так же цепочку из двух сертификатов:

1. Сертификат удостоверяющего центра УЦО, выданный в удостоверяющем центре УЦР – УЦР $\langle\langle УЦО \rangle\rangle = P_{уцо} S_{уцр}(h(P_{уцо}))$. Здесь $S_{уцр}$ – закрытый ключ УЦР, h (

$P_{УЦО}$) – хэш-функция $P_{УЦО}$. В УЦР выдан сертификат получателя R. Поэтому достоверное знание открытого ключа R ($P_{УЦР}$) позволяет проверить достоверность открытого ключа удостоверяющего центра УЦО ($P_{УЦО}$). Для этого следует расшифровать $h(P_{УЦО})$ с помощью достоверного ключа $P_{УЦР}$. $\{h(P_{УЦО}) = P_{УЦР} S_{УЦР}(h(P_{УЦО}))\}$ и сравнить с $h(P_{УЦО})$, полученным из открытой части сертификата.

2. Сертификат удостоверяющего центра УЦИ, выданный в общем удостоверяющем центре УЦО $\ll UCI \gg = P_{УЦИ} S_{УЦО}(h(P_{УЦИ}))$. Здесь $S_{УЦО}$ – закрытый ключ УЦО, $h(P_{УЦИ})$ – хэш-функция $P_{УЦИ}$.

Достоверное знание открытого ключа $P_{УЦО}$ позволяет проверить достоверность открытого ключа удостоверяющего центра УЦИ ($P_{УЦИ}$). Алгоритм проверки аналогичен приведенному выше алгоритму проверки достоверности открытого ключа удостоверяющего центра УЦО ($P_{УЦО}$).

Полученное достоверное знание открытого ключа источника $P_{УЦИ}$ позволяет аналогично проверить достоверность открытого ключа (P_I) в сертификате источника – УЦИ $\ll I \gg = P_I S_{УЦИ}(h(P_I))$, убедившись, что $P_{УЦИ} S_{УЦИ}(h(P_I)) = h(P_I)$. Покажем это на примере, в котором примем $h(P_I) = 88$, $P_{УЦИ} = 7$, $S_{УЦИ} = 23$. Приведенные цифровые значения взяты из примера в Приложении работы [5]. В этом примере значение $p = 187$. $P_{УЦИ} S_{УЦИ}(h(P_I)) = h(P_I): (88^{23} \bmod 187)^7 \bmod 187 = 88$. Приведенный пример полезен для разработки ПО.

Алгоритм проверки подлинности открытого ключа R (P_R) в сообщении 2 аналогичен приведенному выше алгоритму проверки достоверности открытого ключа источника (P_I) и подлежит самостоятельной проработке.

Проверка целостности значений R_I, R_R, K

Для разработки программного обеспечения, реализующего алгоритм проверки целостности значений R_I, R_R, K в сообщении 2 $\{S_R[h(R_I, R_R, K)]\}$ необходимо убедиться в том, что $P_R \{S_R[h(R_I, R_R, K)]\} = [h(R_I, R_R, K)]$. Алгоритм этой проверки основан на том же принципе, что проверка подлинности открытых ключей в сертификате, алгоритм которой приведен выше. Как видно из этого равенства, необходимо вычислить хэш-функцию значения $(R_I | R_R | K)$, где "|" означает конкатенацию. Проверка производится после того, инициатор I убедился в достоверности открытого ключа получателя P_R .

Проверка целостности значений R_R, K

Для разработки программного обеспечения, реализующего алгоритм проверки целостности значений R_R, K в сообщении 3 $\{S_I[h(R_R, K)]\}$ необходимо убедиться в том, что Принцип этой проверки аналогичен приведенной выше проверке целостности значений R_I ,

Выводы

Предложенный алгоритм взаимной аутентификации на абонентском доступе сети ПД позволяет студентам кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана разрабатывать ПО учебного лабораторного стенда сети с высоким уровнем безопасности и надежности.

Литература

1. Матвеев В.А. Учебное пособие для разработки студентами программного обеспечения сети передачи данных и планирование создания лабораторного стенда сети с высоким уровнем безопасности и надежности

/ В.А. Матвеев., Р.А. Бельфер // Информатизация и информационная безопасность правоохранительных органов: сб. науч. тр. / Академия управления МВД России. – Москва, 2016. – С. 51-55.

2. Матвеев В.А. Общие положения алгоритмов учебного лабораторного стенда сети передачи данных на базе виртуальных каналов. / В.А. Матвеев., Р.А. Бельфер // Электросвязь. – 2016. – №8. – С. 51-55.

3. Victor O. K. Li; Felix F. Wu; Jin Zhong. Communication Requirements for Risk-Limiting Dispatch in Smart Grid, Communications Workshops (ICC), 2010 IEEE International Conference on, 2011, 1 – 5 pp.

4. A.G. Merkulov, V.P. Shuvalov. Analytical Study of Principles Organization of Convergent Packet DPLC Networks with Transition from Frame Relay to IP Technology with Examples of Projects Implemented in Kazakhstan // International Siberian Conference on Control and Communications, IEEE SIBCON 2015. Russia, Omsk. 2015, p p. 1-10.

5. Осорин М., Лашкевич В.. Концепция Smart Grid – новый вектор развития. / М. Осорин, В. Лашкевич // IT-MANAGER. – 2011. – №6. – С. 34-38.

6. Резолюция конференции “Информационные технологии на службе оборонно-промышленного комплекса России 2015. Connect, 2015. – №9. – С. 78-88.

7. Бельфер Р.А. Сети и системы связи (технологии, безопасность) / Учеб. пособие по дисциплине «Сети и

с

и

с

т

е

м

ы

с

е

д

е

з

н

е

»

:

э

л

е

к

т

р

о

н

н

о

е

у

ч

е

б

.

и

з

д

⁵⁵ Belfer Ruvim Abramovich, Bauman Moscow State Technical University, Senior Researcher, Associate Professor, Ph.D., a.belfer@yandex.ru

⁵⁶ Kuianov Maksim Sergeevich, Bauman Moscow State Technical University, m_aksakov@mail.ru

⁵⁷ Merzlyakov Daniil Ivanovich, Bauman Moscow State Technical University, merzdan@gmail.com

⁵⁸ Zenkovich Stanislav Aleksandrovich, Bauman Moscow State Technical University, stanislav.zen@ya.ru

**Алгоритм функции установления виртуального соединения
многомаршрутной сети ПД в учебном лабораторном стенде**
Бельфер Р.А.⁵⁹, Мазуров А.М.⁶⁰

Приводится алгоритм установления коммутируемого виртуального канала учебного лабораторного стенда сети передачи данных в многомаршрутной конфигурации. Для заказчиков таких сетей характерны высокие требования информационной безопасности, надежности и задержки. В настоящее время на кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана проводится работа по созданию учебного лабораторного стенда сети передачи данных и находится в состоянии реализации рассматриваемых в работе алгоритмов.

Ключевые слова: коммутируемый виртуальный канал, центр коммутации пакетов ЦКП, сеть энергосбережения, информационная безопасность, надежность, задержка, сеть передачи данных.

Введение

Из резолюции IV конференции «Информационные технологии на службе оборонно-промышленного комплекса России 2015» [1] следует важность работ по созданию телекоммуникационного оборудования, отмечается отсутствие современной системы объединенных коммуникаций в сфере ОПК. В работах [2,3] отмечается актуальность создания отечественных сетей передачи данных (ПД) с высокими показателями информационной безопасности, надежности, задержки и других характеристик. В них освещаются общие положения по созданию на кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана учебного лабораторного стенда (УЛС) сети передачи данных на базе виртуальных каналов. Такая сеть связи должна объединять не только сети в сфере ОПК, но и другие сети связи в соответствии с классификацией Федерального закона «О связи» [4] - сети специального назначения, технологические сети (как например, сети энергосбережения энергоснабжения smart grid [5,6]).

В настоящей работе предлагается создание такого УЛС сети ПД, который обеспечивает указанные высокие требования за счет создания пучка маршрутов между конечными пунктами включающего несколько путей маршрутизации.

1. Конфигурация сети учебного лабораторного стенда ПД

На (рис.1) приведена конфигурация сети ПД для УЛС, позволяющая создавать между конечными пунктами соединения с пучком маршрутов, включающий несколько путей маршрутизации.

Каждый путь маршрутизации состоит из трех центров коммутации пакетов (ЦКП) в каждом. К двум конечным ЦКП в каждом пути маршрутизации (ЦКП1.1, ЦКП3.1 и ЦКП1.2, ЦКП3.2) подключены конечные пункты, а ЦКП2.1 и ЦКП2.2 являются транзитными. Доступ конечных пунктов ($a, b, \dots, c$ и $d, e, \dots, f$) к центру коммутации пакетов удаленный. Конечные пункты (ЦКП) на участке абонентского доступа обмениваются данными одновременно по четырем маршрутам. Это обусловлено тем, что такая конфигурация обеспечивает выполнение строгих требований по задержке сообщений, не прибегая к повторам из буфера сообщений при искажении в каналах.

⁵⁹ Бельфер Рувим Абрамович, доцент, МГТУ им. Н.Э. Баумана, к.т.н., a.belfer@yandex.ru

⁶⁰ Мазуров Артем Михайлович, МГТУ им. Н.Э. Баумана, artemmazurov@gmail.com

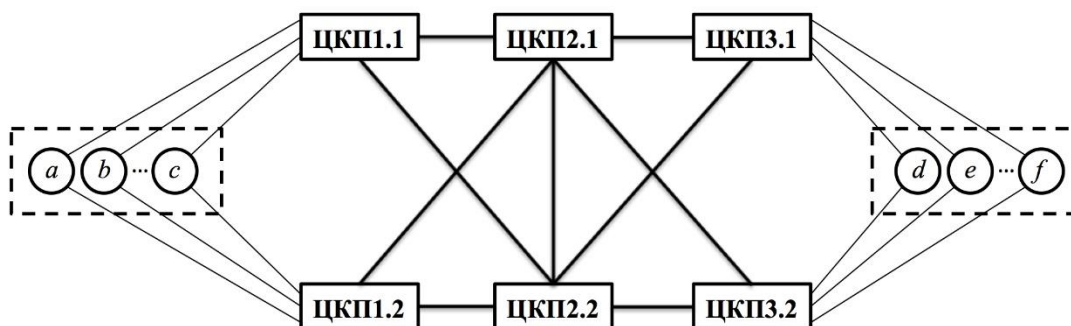


Рис.1. Конфигурация сети ПД

2. Составление путей маршрутизации в оконечном пункте

В каждом оконечном пункте хранится таблица маршрутизации.

Пример пучка маршрутов КВК из четырех путей маршрутизации между a и f при отсутствии отказов каналов связи:

- 1) $a - \text{ЦКП1.1} - \text{ЦКП2.1} - \text{ЦКП3.1} - f$
- 2) $a - \text{ЦКП1.2} - \text{ЦКП2.2} - \text{ЦКП3.2} - f$
- 3) $a - \text{ЦКП1.1} - \text{ЦКП2.2} - \text{ЦКП3.1} - f$
- 4) $a - \text{ЦКП1.2} - \text{ЦКП2.1} - \text{ЦКП3.2} - f$

Примем следующие физические адреса для оконечных пунктов: 101 (a), 201 (b), 301 (c), 401 (d), 501 (e), 601 (f). Также примем следующие физические адреса для ЦКП: 11 (ЦКП1.1), 21 (ЦКП2.1), 31 (ЦКП3.1), 12 (ЦКП1.2), 22 (ЦКП2.2), 32 (ЦКП3.2). В таком случае таблица маршрутизации в оконечном пункте a для КВК с оконечным пунктом f будет иметь вид указанный в (таб.1).

Таблица 1.

Таблица маршрутизации в оконечном пункте a для КВК с оконечным пунктом f

Номер пути маршрута	Физический адрес исходящего оконечного пункта	Физический адрес пункта назначения	Путь (маршрут) по физическим адресам ЦКП от исходящего оконечного пункта до пункта назначения (каждый адрес 2 байта)
1	101	601	11 21 31
2	101	601	12 22 32
3	101	601	11 22 31
4	101	601	12 21 32

3. Предварительные этапы алгоритма установления КВК

Прежде чем разработать алгоритм функции установления виртуального соединения многомаршрутной сети ПД в лабораторном учебном стенде необходимо реализовать алгоритмы следующих функций:

3.1. Взаимная аутентификация на абонентском участке сети [7] и между смежными ЦКП [8].

3.2. Создание сессионных ключей на абонентском участке сети [7] и между смежными ЦКП [8]. В указанных работах такими ключами являются - ключ адресной части

заголовка сообщений K_{AB} , ключ сквозного шифрования $K_{СКВ}$, ключ целостности адресной части сообщения адресной части заголовка сообщений на абонентском участке $K_{ЦАБ}$, ключ целостности $K_{ЦСКВ}$ информационной части пакета данных.

После успешного завершения пунктов 3.1 и 3.2 алгоритм установления КВК производится в следующей последовательности:

3.3. Составляются строки таблицы маршрутизации по физическим адресам для каждого оконечного пункта.

3.4. Составляется очередь свободных номеров $O_{свн}$ в каждом ЦКП.

4. Алгоритм функции установления КВК на абонентском участке

Настоящий раздел посвящен алгоритму функции установления КВК на абонентском участке оконечного пункта - отправителя запроса на соединение. Описание данного алгоритма производится на примере установления КВК между оконечными пунктами a и f .

4.1. Назначается состояние КВК на оконечном пункте (в качестве примера отправителем запроса на соединение выступает оконечный пункт a) - 1 (установление КВК). Сформировать и передать от оконечного пункта в смежный с ним оконечный ЦКП (ЦКП1.1 и ЦКП1.2) сообщение об инициализации установления КВК. Формат этого сообщения состоит из четырех полей - тип сообщения "1" (1 байт), область использования сети "1" (1 байт), конфигурация сети "1" (1 байт), физический адрес исходящего оконечного пункта - 101 (2 байта), физический адрес пункта назначения - 601 (2 байта). Все поля зашифровываются с помощью ключей абонентского участка $K_{аб}$. В оконечном ЦКП производится его расшифровка. Ключи абонентского участка $K_{аб}$ обеспечивают также целостность передаваемых данных.

4.2. Подготавливается и отправляется от оконечного ЦКП в оконечный пункт зашифрованное с использованием ключа $K_{аб}$ сообщение состоящее из двух полей - тип сообщения = 2 (1 байт), $LCN = 9$ (1 байт), стоящим первым в $O_{свн}$. Корректируются $O_{свн}$ и $O_{зан}$, а так же характеристики этих очередей. Запоминается в оконечном ЦКП логический адрес LCN оконечного пункта.

4.3. В оконечном пункте расшифровывается LCN ключом $K_{аб}$, проверяется целостность сообщения с использованием ключа $K_{ЦАБ}$ и запоминается.

4.4. От оконечного пункта отправляются сообщения Запрос Вызова (ЗВ) на установление КВК в оконечные ЦКП (ЦКП1.1 и ЦКП1.2) для каждого пути маршрутизации зашифрованное ключом $K_{аб}$ и предусмотренное проверкой на целостность ключом $K_{ЦАБ}$ по протоколам, приведенным по индексу согласованных параметров $SPI(A)$ [7]. Формат сообщения ЗВ (подлежащее шифрованию и обеспечению целостности) состоит из следующих полей - тип сообщения (1 байт), LCN (1 байт), физические адреса оконечных пунктов отправителя и получателя (по 2 байта каждый), цепочка пути маршрутизации, состоящая не более чем из 12-х адресов ЦКП по 2 байта каждый (24 байта), контрольно-проверочная комбинация КПК (2 байта).

4.5. Расшифровываются в оконечных ЦКП с использованием ключа $K_{аб}$ сообщения ЗВ и проверяются целостность с использованием ключа $K_{ЦАБ}$.

4.6. Из каждого ЗВ извлекается значение поля содержащее цепочку пути маршрутизации, по которым должен пройти маршрут. Для приведенной конфигурации сети ПД на (рис.1): ЦКП1.1 - 11|21|31 и 11|22|31, ЦКП1.2 - 12|22|32 и 12|21|32. Проверяется, что первый физический адрес соответствует адресу текущего ЦКП. Далее цепочка пути маршрутизации сдвигается на 2 байта влево для последующей передачи в ЗВ (для ЦКП1.1 - 21|31 и 22|31, для ЦКП1.2 - 22|32 и 21|32). После этого первым физическим адресом в цепочке пути маршрутизации будет адрес следующего пункта, в который необходимо направить ЗВ

(для ЦКП1.1 - 21 и 22, для ЦКП1.2 - 22 и 21, в зависимости от маршрута переданного от оконечного пункта). В случае если первый физический адрес в цепочке пути маршрутизации отсутствует, установление КВК в транспортной сети завершено. Следовательно, установление КВК завершается на оконечном пункте назначения.

4.7. Подготавливается сообщение ЗВ к передаче из оконечного ЦКП (в примере ЦКП1.1 и ЦКП1.2) в смежные ЦКП в соответствии с полученным физическим адресом в п.4.6. Для этого необходимо выбрать первый уникальный номером LCN в О_{свн}. Например LCN=2. Заменить в ЗВ LCN=9 на LCN=2. Откорректировать О_{свн} и О_{зан}, а так же характеристики этих очередей.

4.8. Составляются строки таблицы маршрутизации [9] для ЦКП1.1 (таб.2) и для ЦКП1.2 (таб.3) по логическим адресам. В составе приведенной строки маршрутизации в (таб.2) и (таб.3) для рассматриваемого примера КВК входят значения для входящих сообщений в оконечный ЦКП (ЦКП1.1 и ЦКП1.2) и для исходящих из него сообщений. Как видно из таблицы в первую строку входят значения для устанавливаемого КВК:

- LCN входящего сообщения (9);
- физический адрес источника входящего сообщения (оконечный пункт);
- LCN исходящего сообщения (2);
- физический адрес получателя исходящего сообщения (транзитный ЦКП);
- признак использования Освн для получения LCN (да или нет).

Таблица 2.

Таблица маршрутизации по логическим адресам в оконечных ЦКП1.1

Номер пути маршрута (таб.1)	Входящее сообщение в оконечный ЦКП			Исходящее сообщение из оконечного ЦКП		
	LCN	Освн	Адрес источника	LCN	Освн	Адрес получателя
1	9	да	101	2	да	21
1	2	нет	21	9	нет	101
3	13	да	101	5	да	22
3	5	нет	22	13	нет	101

Таблица 3.

Таблица маршрутизации по логическим адресам в оконечных ЦКП1.2

Номер пути маршрута (таб.1)	Входящее сообщение в оконечный ЦКП			Исходящее сообщение из оконечного ЦКП		
	LCN	Освн	Адрес источника	LCN	Освн	Адрес получателя
2	20	да	101	33	да	21
2	33	нет	21	20	нет	101
4	29	да	101	27	да	22
4	27	нет	22	29	нет	101

Выводы

Предложенный алгоритм функции установления виртуального соединения

многомаршрутной сети ПД позволяет студентам кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана разрабатывать ПО учебного лабораторного стенда сети с высоким уровнем безопасности, надежности и низкой задержки. Настоящая работа требует дальнейшего продолжения исследования и развития алгоритма.

Литература

1. Резолюция конференции “Информационные технологии на службе оборонно-промышленного комплекса России 2015. Connect, 2015 №9, С.78-88.
2. В.А. Матвеев, Р.А. Бельфер. Учебное пособие для разработки студентами программного обеспечения сети передачи данных и планирование создания лабораторного стенда сети с высоким уровнем безопасности и надежности. Сборник трудов XXV Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов» - М.: Академия управления МВД России, 2016, С. 51-55.
3. В.А. Матвеев, Р.А. Бельфер. Общие положения алгоритмов учебного лабораторного стенда сети передачи данных на базе виртуальных каналов. Электросвязь 2016, №8, С. 51-55.
4. Федеральный закон Российской Федерации №126-ФЗ от 7.07.2003 (редакция от ноября 2015 г.) «О связи».
5. Victor O. K. Li; Felix F. Wu; Jin Zhong. Communication Requirements for Risk-Limiting Dispatch in Smart Grid, Communications Workshops (ICC), 2010 IEEE International Conference on, 2010, 1 – 5 pp.
6. Меркулов А.Г. Повышение эффективности корпоративных пакетных ЦВЧ сетей электроэнергетических компаний с использованием методов перехода от технологии Frame Relay к IP-технологии. Автореферат диссертации кандидата технических наук. Уфимский государственный авиационный технический университет. Уфа, 2015, 135 с.
7. Бельфер Р.А., Зенькович С.А., Куянов М.С., Мерзляков Д.И. Алгоритм взаимной аутентификации на абонентском доступе сети передачи данных в учебном лабораторном стенде (настоящий сборник).
8. Бельфер Р.А., Кулинич Р.С., Прищепин Е.П., Алгоритм взаимной аутентификации транспортной сети передачи данных в учебном лабораторном стенде (настоящий сборник).
9. Бельфер Р.А., Кулинич Р.С., Прищепин Е.П., Алгоритм установления виртуального соединения на абонентском доступе сети передачи данных учебного лабораторного стенда (настоящий сборник).

Algorithm Function of Establishing Virtual Connections Multipath Data Transmission Network in Educational Laboratory Stands

R.A. Belfer, A.M. Mazurov⁶¹

An algorithm for establishing switched virtual channel training laboratory bench data network in the multipath configuration. For customers, these networks are characterized by high information security requirements, reliability and latency. Currently, the department of Information Security Bauman University (BMSTU) working on the creation of educational laboratory bench data network and is in the implementation of consideration in the algorithms.

Keywords: Switched Virtual Circuit, packet switching, circuit switching, packet switching center, smart grid, Information Security, reliability, задержка, data network.

⁶¹ R.A. Belfer, Bauman University (Bauman Moscow State Technical University), Ph.D., a.belfer@yandex.ru; and A.M. Mazurov, Bauman University (Bauman Moscow State Technical University), artemmazurov@gmail.com

**Создание области загружаемых файлов для обеспечения безопасности
электронно-библиотечной системы**
Булдакова Т.И.⁶², Александров М.Ю.⁶³

Рассматриваются принципы создания области хранения данных, загружаемых пользователями при работе с электронным документооборотом в электронной библиотечной системе (ЭБС). Производится оценка угроз и анализируются методы предотвращения проникновений в систему. Вырабатываются рекомендации по защите хранилища ЭБС.

Ключевые слова: электронная библиотечная система, защита информации, антивирусная защита, файловое хранилище, информационная система, документооборот

Введение

За последнее десятилетие произошли существенные изменения в структуре всей информационно-библиотечной системы, были введены новые формы и методы комплектования библиотечных фондов, произошла смена приоритетов в области информационной деятельности. Все это способствовало стремительному росту образовательных электронных ресурсов в российском Интернет-пространстве, что в корне изменило систему организации хранения и доступа к информации, в том числе в сфере научной и образовательной литературы.

Федеральные государственные образовательные стандарты высшего образования накладывают на высшие учебные заведения ряд требований по использованию электронно-библиотечных систем, что в свою очередь повышает требования по информационной безопасности [1].

В настоящее время трудно представить успешное функционирование большинства информационных систем, которые позволяют автоматизировать сбор и обработку данных, без области хранения информации. Обычно для хранения и доступа к данным, содержащим сведения о некоторой предметной области, создается хранилище данных.

Принципы создания области хранения данных

Плохо организованный проект создания хранилища данных (ХД), даже при качественном проектировании, ведет в более чем 50% случаев к краху проекта

Организация любого проекта разработки ХД (используемая бизнес-модель) во многом определяет его успешность. В основу организационной структуры проекта, как правило, закладывается некоторая модель жизненного цикла создаваемого объекта.

Архитектура области хранения данных базы данных (БД) корпоративного хранилища, как правило, состоит из следующих областей (рис. 1):

- 1) область временного хранения данных, которая включает:
 - область стейджа, которая предназначена для временного хранения данных, извлеченных из систем-источников, и является промежуточным слоем между операционными системами компании и хранилищем данных;
 - интерфейсы обмена данными с другими системами в виде таблиц БД, в которых хранятся подготовленные для передачи в другие информационные системы данные из области постоянного хранения данных;
- 2) область постоянного хранения данных, которая включает:

⁶² Булдакова Т.И., д-р техн. наук, профессор, МГТУ им. Н.Э. Баумана. Москва, buldakova@bmstu.ru

⁶³ Александров Михаил Юрьевич, МГТУ им. Н.Э. Баумана. Москва, mikke_13@mail.ru

- детальные данные, приведенные к структуре модели данных корпоративного хранилища и прошедшие очистку и обогащение;
 - агрегаты, т.е. сгруппированные по времени (чаще просуммированные) детальные данные;
 - витрины данных, представляющие тематические наборы данных, хранящихся в виде, пригодном для их анализа (например, схема «звезда»);
- 3) метаданные, которые являются важной частью архитектуры хранилища данных. Метаданные – это данные, описывающие правила, по которым «живет» хранилище. Например, с точки зрения БД хранилища, метаданными является описание структур таблиц, взаимосвязей между ними, правил секционирования, описание витрин данных и т.п.

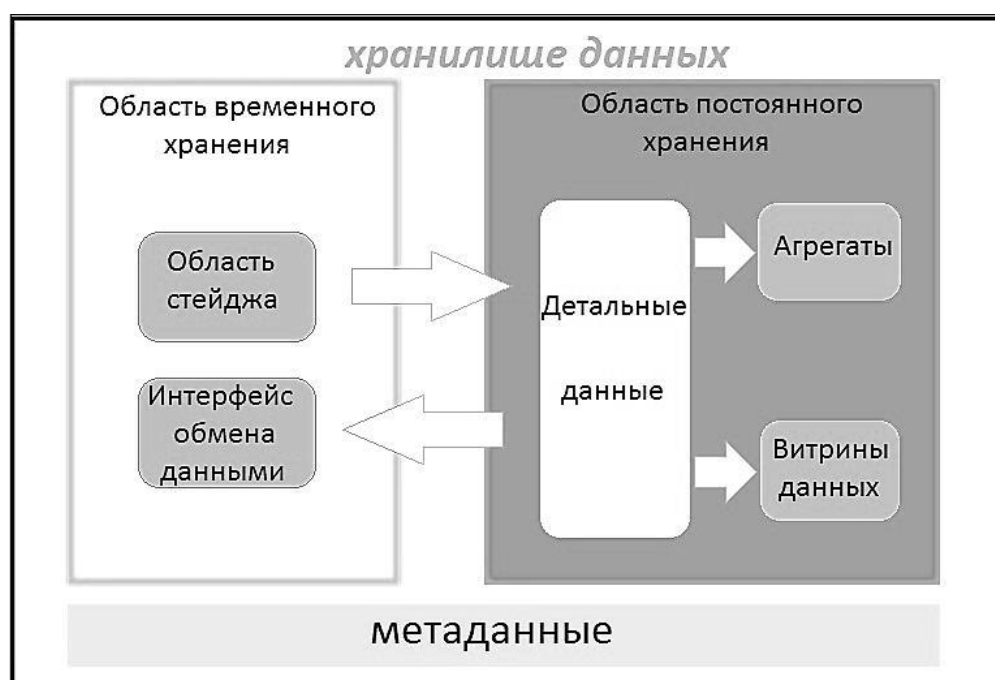


Рис. 1. Схема организации областей хранения данных

Обычно приведенные выше области хранения данных реализуются в виде отдельных схем одной или нескольких баз данных.

Описание области временного хранения данных

Область временного хранения данных является промежуточным слоем между источниками данных и областью постоянного хранения. В данной области сохраняются загружаемые данные (в форматах doc, pdf, ppt, xls и т.д.) пользователей ЭБС и данные, извлеченные из других источников (СУБД, csv, dbf, xml файлов, web-сервисов и т.д.), а также производится их очистка, проверка на вирусы, трансформация, обогащение, подготовка к загрузке в область постоянного хранения. Область временного хранения служит для сбора всех необходимых данных перед началом трансформации.

Одной из наиболее важных задач при построении хранилища данных является определение соответствия сущностей систем-источников данных и сущностей модели ХД. Обычно подобное соответствие представляет собой отношение десятков таблиц систем-источников к десяткам таблиц области постоянного хранения данных.

Правильно организованная область временного хранения данных позволяет значительно упростить организацию процессов загрузки, а также повысить безопасность данных при выгрузке из области временного в область постоянного хранения.

Анализ угроз информационной безопасности в ЭБС

Считается, что для защиты систем электронного документооборота (СЭД) достаточно использования электронно-цифровой подписи (ЭЦП), однако в большинстве случаев разработчики не поясняют, как правильно использовать ЭЦП, какая нужна инфраструктура и какие защищенные сервисы необходимо развернуть на ее основе [2].

В общем случае к задаче создания защищенной СЭД необходимо подходить с точки зрения классической защиты информационной системы [3], обеспечивая решение таких задач, как:

- аутентификация пользователей и разделение доступа;
- подтверждение авторства электронного документа;
- контроль целостности электронного документа;
- конфиденциальность электронного документа;
- обеспечение юридической значимости электронного документа.

Если раньше обеспечивалась защита непосредственно самих электронных документов или информационных ресурсов, содержащих документы, то теперь изменяются основной вектор атак и, соответственно, объект защиты [4]. Кроме традиционных атак на информационные ресурсы все чаще их объектом становится взаимодействие «человек – электронный документ», «человек – информационный ресурс». Таким образом, защищать надо не столько сами документы, сколько системы передачи, обработки и хранения электронных документов при доступе пользователей к работе с электронными документами.

Рекомендации по защите хранилища ЭБС

Любая СЭД, претендующая на звание «защищенной», должна как минимум предусмотреть механизм защиты от основных ее угроз: обеспечение сохранности документов, обеспечение безопасного доступа, обеспечение подлинности документов, протоколирование действия пользователей. Рассмотрим эти составляющие.

1. Обеспечение сохранности документов

СЭД должна обеспечить сохранность документов от потери и порчи и иметь возможность их быстрого восстановления. По статистике, в 45% случаях потери важной информации приходится на физические причины (отказ аппаратуры, стихийные бедствия и подобное), 35% обусловлены ошибками пользователей и менее 20% — действием вредоносных программ и злоумышленников. Сюда следует также отнести возможность восстановления не только данных, но и самой системы в случае ее повреждения.

2. Обеспечение безопасного доступа

Этот момент обычно понимают под безопасностью СЭД, чем часто ограничивают понятие безопасности систем. Безопасный доступ к данным внутри СЭД обеспечивается аутентификацией и разграничением прав пользователя.

Здесь необходимо заострить внимание на методах аутентификации. Самый распространенный из них, конечно, парольный. Основные проблемы, которые сильно снижают надежность данного способа — это человеческий фактор. Даже если заставить пользователя использовать правильно сгенерированный пароль, в большинстве случаев его можно легко найти на бумажке в столе или под клавиатурой.

3. Разграничения прав пользователя

В любой системе обязательно должно быть предусмотрено разграничение прав пользователя — и чем гибче и детальнее, тем лучше.

4. Конфиденциальность

Огромным преимуществом для конфиденциальности информации обладают криптографические методы защиты данных. Их применение позволят не нарушить конфиденциальность документа даже в случае его попадания в руки стороннего лица.

5. Обеспечение подлинности документов

Сегодня основным и практически единственным предлагаемым на рынке решением для обеспечения подлинности документа является метод электронно-цифровой подписи [5, 6]. Основной принцип работы ЭЦП основан на технологиях шифрования с асимметричным ключом. Имеется «закрытый» ключ, который позволяет зашифровать информацию, и имеется «открытый» ключ, при помощи которого можно эту информацию расшифровать, но с его помощью невозможно «зашифровать» эту информацию. Таким образом, владелец «подписи» должен владеть «закрытым» ключом и не допускать его передачу другим лицам, а «открытый» ключ может распространяться публично для проверки подлинности подписи, полученной при помощи «закрытого» ключа.

6. Защищенный обмен XML данными

XML-подписи — это цифровые подписи, разработанные для операций на основе XML. Важное свойство XML-подписи заключается в возможности применения нескольких цифровых подписей к одному документу. Благодаря этому, с одним XML-документом могут работать сразу несколько пользователей, применяя новую подпись поверх той, что уже была создана другим пользователем.

Добавление цифровой подписи позволяет быть уверенным, что данные XML-документа находятся в безопасности.

Таким образом, можно сделать следующий вывод.

Разработка средств защиты документооборота в ЭБС должна проводиться с учетом защиты от выявленных угроз и возможных информационных рисков, для которых определяются способы защиты, и на основе предложенного показателя оценки ее эффективности [7]. При этом учитываются требования, которые предъявляются к созданию таких систем, а именно:

- организация защиты информации осуществляется с учетом системного подхода, обеспечивающего оптимальное сочетание взаимосвязанных методологических, организационных, программных, аппаратных и иных средств;
- система должна развиваться непрерывно, так как способы реализации угроз информации непрерывно совершенствуются;
- правильно организованная область временного хранения данных позволяет значительно упростить организацию процессов загрузки, а также повысить безопасность данных при выгрузке из области временного в область постоянного хранения.

Для оценки эффективности защиты информации в ЭБС можно применить показатели, предложенные в работе [2].

Выводы

Безопасность электронно-библиотечной системы в значительной степени зависит от качества организации хранилища данных и, в частности, области временного хранения данных. Оценку защищенности информационных ресурсов целесообразно проводить по показателям эффективности защиты систем электронного документооборота.

Литература

1. Дворкина М.Я., Елицина Е.Ю. Дистанционное библиотечное обслуживание: сущность и реализация в современных условиях // Библиотековедение. 2015. № 5. С. 38-43.
2. Булдакова Т.И., Глазунов Б.В., Ляпина Н.С. Оценка эффективности защиты систем электронного документооборота // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. Т. 1. № 2. С. 52-56.

3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. М.: ДиаСофт, 2002. 693 с.
4. Сабанов А.А. Некоторые аспекты защиты электронного документооборота // Connect! Мир связи. 2010. № 7. С. 62–64.
5. Черкасов Д.Ю., Иванов В.В. Защита документов при помощи электронной цифровой подписи // Economics. 2016. № 6 (15). С. 51-53.
6. Новицкая Е.А., Перова М.В. Применение электронной подписи в системах электронного документооборота // Перспективы развития информационных технологий. 2015. № 26. С. 80-85.
7. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2). С. 28-35.

Creation of Territory Downloadable Files for Secure E-Library Systems Buldakova T.I.⁶⁴, Aleksandrov M.Y⁶⁵

The principles of creating a storage area for files uploaded by users when working with e-library systems are considered. The estimation of threats and analyzes the methods of prevention Intrusion into the system. Explore ways of antivirus protection storage of e-library systems. Develop recommendations for the protection of e-library systems.

Kewwords: e-library, data protection, virus protection, file storage information system, document flow.

УДК 004.056.53

Возможный подход к оценке средств защиты информации

Бондарев В. В.⁶⁶

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

Ключевые слова: защита информации, средства защиты информации, мера, оценка.

Введение

В работе рассмотрен оригинальный подход к сравнению средств защиты информации, отличный от известных [1-5].

Оценка систем. Под оценкой понимается установление степени ответственности объекта нормам, требованиям, эталонам. Отображением объекта в средстве оценки является мера объекта – единство качественной и количественной определенности объекта: $M = (\text{качество}, \text{количество})$. *Качество* – совокупность свойств, отличающая данный объект от другого объекта. *Количество* – выражение однородности объектов. Оценка систем сводится к измерению – оценке соответствия меры системы некоторым эталонам, критериям.

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.

⁶⁴ Buldakova T.I., Ph.D, Professor, Bauman Moscow State Technical University, buldakova@bmstu.ru

⁶⁵ Aleksandrov M.Y, Bauman Moscow State Technical University, mikke_13@mail.ru

⁶⁶ Бондарев Валерий Валериевич, кандидат военных наук, МГТУ им. Н.Э.Баумана, bondarevvv@mail.ru

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.

Описание средства защиты информации в виде меры

Представим меру в виде

$$M = \begin{bmatrix} C_1, C_2, C_3 \dots, & C_n \\ v_{c_1} v_{c_2} v_{c_3} & v_{c_n} \end{bmatrix}, \quad (1)$$

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)

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

Мера предмета деятельности

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

Близость мер определяется одним из возможных показателей:

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

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

где N_{M_K} , N_{M_Π} – мощности M_K , M_Π ; N_{M_Π} – 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.

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

Методика оценки близости мер

1. Объединяем мощности множеств C в M_0 , M_3 : N_{C^0} , N_{C^3} .

2. Представляем $M_0 \cap M_3$ 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 .

Выводы

Сделана попытка добиться максимальной объективности при сравнении различных средств защиты информации. Предлагаемая методика была апробирована на практике. Были рассмотрены шесть наиболее широко применяемых (согласно статистике портала Securitylab.ru) сканеров уязвимостей: Nessus (версия 3.2.1); MaxPatrol (версия 8.0.1178); Internet Scanner (версия 7.2.58); Retina Network Security Scanner (версия 5.10.2.1389); Shadow Security Scanner (SSS) (версия 7.141.262); NetClarity Auditor (версия 6.1). В результате применения методики первое место занял сканер MaxPatrol, на втором месте – сканер Nessus. Эти результаты были подтверждены экспериментальными исследованиями.

Литература

- 1.Абрамов А.В., Панасенко С.П., Петренко С.А. Типовые схемы защиты сетей // Вопросы защиты информации. 2006. № 4. С. 29-35.
- 2.Быков А.Ю., Панфилов Ф.А., Зенькович С.А. Модель и методы многокритериального выбора классов защищенности для объектов распределенной информационной системы и размещения баз данных по объектам // Вопросы кибербезопасности. 2016. № 2 (15). С. 9-20.
- 3.Кондаков С.Е. Анализ и синтез комплекса средств защиты информации // Вопросы кибербезопасности. 2013. № 2. С. 20-24.
- 4.Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции // Вопросы кибербезопасности. 2016. № 1 (14). С. 17-23. 3
- 5.Чобанян В.А., Шахалов И.Ю., Райков О.В. Некоторые аспекты расчета эффективности средств защиты информации перспективных автоматизированных систем военного назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2014. № 7-8. С. 46-49.

Possible Approach to Assessment of Means of Information Protection

V.V.Bondarev⁶⁷

The problems of the comparative evaluation of information security with a campaign based on the concept of a measure - the unity of the qualitative and quantitative determination of the object.

Keywords: information security, data protection, measure, estimate.

УДК 003.26.004.7.004.9

Стеганографические методы защиты проектной документации САПР в аудиосигналах Будюкина Е.Н.⁶⁸

Рассмотрены теоретические основы сокрытия секретных данных на примере различных стеганографических методов. К рассмотренным методам относятся метод фазового кодирования, кодирование наименее значащих бит и сокрытие данных с использованием эхо-сигнала. Методы основаны на сокрытии секретных данных в аудиосреде. Было проведено сравнение предложенных методов и рассмотрены их особенности. На основе полученных результатов были выявлены положительные и отрицательные аспекты каждого из методов.

Ключевые слова: безопасность, стеганография, защита, фазовое кодирование, кодирование наименее значащих бит, эхо-сигнал.

⁶⁷ Bondarev Valeriy, P.H.D., Bauman MSTU, Moscow, bondarevvv@mail.ru

⁶⁸ Будюкина Елена Николаевна, МГТУ им. Н.Э. Баумана, г. Москва, elena_budyukina@mail.ru

Введение

После изучения публикаций по данной тематике [1,2] можно сделать вывод, что защита проектной документации в системах CAD/PLM/CAM при передаче и хранении является актуальной задачей. В данной публикации рассматриваются методы цифровой стеганографии, скрывающие информацию в потоках оцифрованных сигналов, имеющих аналоговую природу. Это направление очень популярно, так как существует множество особенностей слухового аппарата человека, позволяющих удачно использовать аудиосигналы с целью стеганографической защиты конфиденциальной информации. В публикации рассмотрены и проанализированы три стеганографических метода. Так же описаны достоинства и недостатки каждого из методов.

1. Кодирование наименее значащих бит

Младшие разряды цифровых отсчетов содержат очень мало полезной информации о текущих параметрах звука и визуального образа. Их заполнение ощутимо не влияет на качество восприятия и дает возможность сокрытия нужной информации. На этом основывается метод замены наименьшего значащего бита. Данный метод является наиболее простым стеганографическим методом и является очень распространенным.

В основе метода лежит принцип замены бит исходного контейнера, вносящих наименьший аддитивный вклад в сигнал, на биты сообщения, которое необходимо скрыть [3].

Младший бит байта аудиоконтейнера заменяется на бит сообщения. Пример замены бит представлен на рисунке 1. Младший бит имеет наименьший аддитивный вклад, поэтому искажение, вносимое в аудиофайл, незначительно, и не обнаруживается слуховой системой человека.

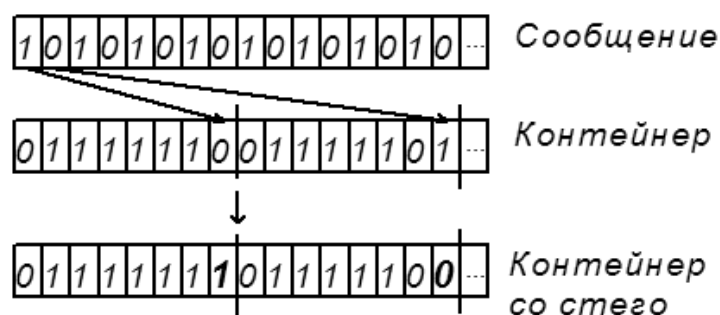


Рис. 1. Пример сокрытия первых бит сообщения

Иногда младшие биты не могут быть обработаны устройствами вывода и изменяются при сжатии файла [4]. Следовательно, некоторая зашифрованная информация может быть потеряна.

Несмотря на возможность искажения извлеченных данных при внешнем воздействии на контейнер, метод имеет высокую пропускную способность. Также данный метод оказался нетребователен к вычислительным ресурсам и его можно применять к большинству форматов мультимедийных файлов.

2. Фазовый метод кодирования

Одним из методов для сокрытия данных в файлах звукового формата является метод фазового кодирования. Встраивание сведений происходит в частотной области сигнала [5]. Алгоритм встраивания основывается на замене фазы первого сегмента аудио на опорную фазу. Опорная фаза формируется в зависимости от того, какие данные необходимо скрыть. Незначительное изменение относительных фаз не ощутимо слухом человека, поэтому

данный метод является одним из наиболее эффективных, так как незначительно искажает начальное стегосообщение. Не ощутимы на слух только относительные фазы, но разница фаз между сегментами значительно искажает начальный контейнер. Данный метод идеально подходит для передачи таких данных как пароли или секретные ключи.

Преимуществами метода оказались его устойчивость к различным воздействиям на контейнер, и высокая эффективность по критерию соотношения сигнал-шум. Недостатком схемы, построенной на основе метода фазового кодирования является низкая пропускная способность. Пропускная способность варьируется от 8 до 32 бит/с в зависимости от звукового контекста. При проведении анализа работы рассматриваемого метода было определено оптимальное соотношение скрываемого файла к исходному аудио-контейнеру для обеспечения наилучшего сокрытия данных, которое составило 5%.

3. Сокрытие данных с использованием эхо-сигнала

Существует еще один стеганографический метод, а именно метод, позволяющий внедрять данные в аудиосигнал-контейнер путем введения в него эхо-сигнала. Существует несколько параметров эхо-сигнала, с помощью изменений которых осуществляется встраивание данных. Этими параметрами являются начальная амплитуда, скорость затухания и сдвиг (время задержки между исходным сигналом и его эхо). На рисунке 2 представлены регулируемые параметры эхо-сигнала.

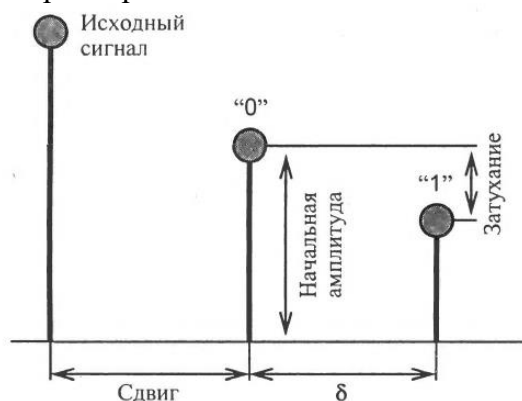


Рис. 2. Регулируемые параметры эхо-сигнала

При постепенном уменьшении сдвига между первичным и эхо-сигналом происходит смешивание двух сигналов. При определенном значении задержки эхо-сигнал начинает восприниматься как добавочный резонанс. Значение задержки зависит от исходной записи, типа звука и от слушателя, поэтому оптимальное значение задержки определить очень сложно. В публикации [6] авторы метода пришли к выводу, что для большинства звуков и слушателей смешивание двух сигналов происходит при задержке приблизительно равной одной миллисекунде.

Для того чтобы внедрить данные применяется стеганокодер. Он использует два времени задержки: одно для представления двоичного нуля, а другое – для представления двоичной единицы. Оба времени значительно меньше допустимого времени задержки сигнала и слуховая система человека не способна распознать эхо. Помимо этого, для уменьшения порога чувствительности человеческого слуха в данном методе применяется также установка уровня начальной амплитуды и времени затухания.

После проведения исследований по работоспособности метода были получены результаты. Было выявлено, что с помощью данного метода возможно скрывать информацию в потоке аудиоданных, а также в последствии из этого потока извлекать зашифрованные данные. Пропускная способность при этом приблизительно равна 16 бит/с. Однако, этот метод не оказался универсальным. В ряде случаев при попытке извлечь из аудиосигнала зашифрованные данные, эти данные были неправильно распознаны и не

соответствовали исходному секретному файлу. На основе полученных результатов можно сделать вывод о том, что реализуемый метод плохо подходит для данных, в которых малейшее изменение критично.

Заключение

Рассмотренные в данной публикации стеганографические методы имеют ряд своих достоинств и недостатков. По проведенному анализу временных, амплитудно-частотных характеристик аудиоконтейнеров, можно сделать вывод, что каждый из методов обеспечивает качественную защиту конфиденциальных данных от несанкционированного доступа. В зависимости от важности качества или объема скрываемых данных можно выбрать оптимальный метод или совокупность методов.

Литература

1. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Защита проектной документации от несанкционированного доступа // 9 Международная конференция «Эффективные методы автоматизации подготовки и планирования производства»: труды. (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С.141-144.
2. Волосатова Т.М., Чичварин И.Н. Специфика информационной безопасности САПР// Известия высших учебных заведений. Машиностроение (специальный выпуск.) – 2012. С. 12 – 20.
3. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Информационные технологии. Приложение. 2012, №5. С.1- 32.
4. Чичварин Н.В., Волосатова Т.М. Метод сокрытия данных в стереофонических аудиофайлах [Электронный ресурс]// Наука и образование: электронное научно-техническое издание. 09, сентябрь 2015. URL: <http://engbul.bmstu.ru/file/802177.html> (дата обращения 05.10.16)
5. Волосатова Т. М., Чичварин Н.В. Информатика и лингвистика. Учебное пособие. М.: ИНФРА-М, 2016. 196 С.
6. Bender W., Gruhl B., Morimoto N., Lu A. Techniques for data hiding // IBM systems journal. 1996. Vol. 35. № 3.
7. Глинская Е.В., Чичварин Н.В. Информационная безопасность открытых каналов передачи проектной документации, продуцируемой в САПР // Вопросы кибербезопасности. 2014. № 4 (7). С. 11-22.

Научный руководитель: Волосатова Тамара Михайловна, канд. техн. наук, доцент, МГТУ им. Н.Э. Баумана, г.Москва, tamaravol@gmail.com

Steganography Methods of Protection Cad Project Documentation in Audio Signals

Budyukina E.N.⁶⁹

Abstract. The theoretical foundations of concealment of confidential data on the example of different steganographic methods. There is described the following methods: phase encoding method, the encoding of the least significant bits and concealment of data using echo. The methods are based on concealment of sensitive data in audio file. Comparison of the proposed methods were done and reviewed their features. Positive and negative aspects of each method were identified on the basis of the results obtained.

Keywords: security, steganography, protection, phase coding, the least significant bit of the echo signal.

⁶⁹ Budyukina E.N. Bauman MSTU, Moscow

Модель угроз безопасности при дистанционном мониторинге состояния человека

Булдакова Т.И.⁷⁰, Кривошеева Д.А.⁷¹

Работа выполнена при финансовой поддержке РФФИ (проект 16-07-00878).

Статья посвящена вопросу обеспечения безопасности передаваемых данных в системах дистанционного мониторинга. Проанализирована модель возможных угроз для системы дистанционного мониторинга состояния здоровья человека. Продемонстрировано, что ранее предложенные подходы к обеспечению безопасности, не являются эффективными. Предложен альтернативный подход, основанный на реконструкции модели сложной системы по регистрируемым биосигналам.⁷²

Ключевые слова: информационная безопасность, телемедицина, биосигналы, криптографические ключи.

Введение

В настоящее время виртуальные структуры здравоохранения активно внедряются в жизнь населения, поскольку они ускоряют и облегчают взаимодействие медицинского персонала с пациентом, а также позволяют пользоваться услугами медицинских центров удаленно [1, 2]. Создаваемые инфраструктуры здравоохранения дают возможность решить актуальную на сегодняшний день задачу непрерывного дистанционного мониторинга состояния здоровья человека [3]. Однако при этом возникает проблема с обеспечением целостности, конфиденциальности и доступности передаваемых физиологических данных [4, 5].

Проблема защиты данных в системах дистанционного мониторинга

Развитие телекоммуникационных технологий позволяет удаленно обращаться к датчикам, установленным на теле человека, в независимости от его местоположения [6, 7]. Далее биосигналы, полученные с датчиков, необходимо передавать по каналам связи в центры обработки информации [8, 9]. Медицинский персонал может просматривать в режиме реального времени собранную информацию в информационном хранилище, содержащем базу данных биосигналов, и оценивать текущее функциональное состояние пациента. Для прогнозирования изменения состояния человека создаётся виртуальный физиологический образ в виде математических моделей, описывающих функционирование подсистем организма человека [10].

Одним из наиболее безопасных и удобных хранилищ медицинских данных, полученных с датчиков, является облако. Существует несколько способов передачи данных от датчика к облаку, датчики могут отправлять данные на облако напрямую или через промежуточные базовые станции. Медицинский персонал и пользователь могут просматривать собранную медицинскую информацию непосредственно из облака в режиме реального времени и принимать решения в соответствии с текущим функциональным состоянием человека (рис. 1). Анализ модели угроз (табл. 1) показал, что необходимо выбрать способ распределения криптографических ключей между датчиком и облаком для обеспечения зашифрованности и целостности передаваемых данных.

⁷⁰ Булдакова Татьяна Ивановна, д-р техн. наук, профессор, МГТУ им. Н.Э. Баумана, Москва, buldakova@bmstu.ru

⁷¹ Кривошеева Дарина Александровна, МГТУ им. Н.Э. Баумана, Москва, darinaaleks@gmail.com

⁷² Работа выполнена при финансовой поддержке РФФИ (проект 16-07-00878).

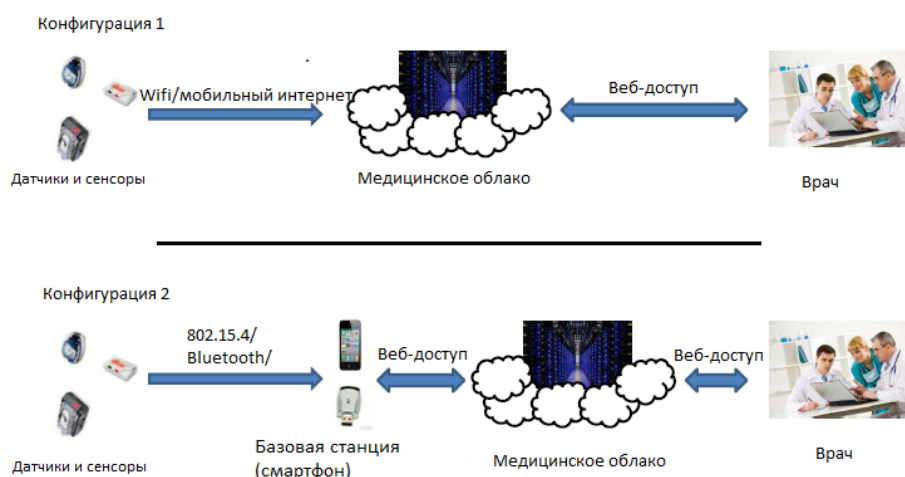


Рис. 1. Конфигурации мобильной системы дистанционного мониторинга

Таблица 1.

Возможные угрозы информационной безопасности

№	Компоненты	Угрозы	Комментарии
1	Датчики	Доступ злоумышленника к датчику	Необходимо использовать надежные датчики, ограничивающие доступ
2	Коммуникации	Злоумышленники могут подслушивать все виды разговоров, а также исказить сигналы	Коммуникационная связь в системе является надежной, поэтому необходимо шифрование сигналов
3	Смартфон	Злоумышленник может повлиять на работу смартфона	Защита приложений на смартфоне
4	Хранилище данных в облаке	Возможный доступ к данным в облаке	Только после успешной авторизации врач сможет получить доступ к информации о пациенте
5	Медицинский персонал	Передача информации злоумышленнику	Предполагается, что медицинский персонал не откроет доступ к информации под влиянием злоумышленников
6	Пациент	Передача информации злоумышленнику	Предполагается, что пациент не откроет доступ к информации под влиянием злоумышленников
7	Тело пациента	Злоумышленник может иметь физический контакт с пациентом (например, пожать ему руку), поэтому биосигналы пациента могут быть искажены сигналами злоумышленника	Надежные датчики не позволяют злоумышленнику исказить сигналы. Кроме того, вся информация о состоянии здоровья пациента в прошлом неизвестна злоумышленнику

Подходы к обеспечению безопасности систем дистанционного мониторинга состояния человека

Канал связи «датчик-облако» является наиболее уязвимым с точки зрения защиты информации. Наиболее часто используемым в подобных случаях протоколом является протокол защиты *E2E* (*end-to-end*), который работает путем задания и последующего

распределения криптографических ключей между датчиками и облаком. Созданный ключ в дальнейшем можно будет использовать для взаимной проверки подлинности сообщения. Основной проблемой является возможность конфиденциального распределения ключей для пользователя. Для пациента данная процедура не должна вызывать вопросов. В идеальном случае пациент не должен вообще заботиться о ключе.

Все традиционные подходы к обеспечению безопасности систем здравоохранения [11, 12] основываются на асимметричных криптосистемах.

Как известно, асимметричное шифрование использует два различных ключа: один для шифрования (открытый), другой для дешифрования (закрытый). Данный подход является достаточно эффективным в вопросе безопасности, но он очень затратный для регулярного обмена информацией в режиме реального времени. Кроме того, асимметричная криптография обладает некоторыми уязвимостями, из-за этого потребуются дополнительные механизмы аутентификации. В связи с вышесказанным в системах дистанционного мониторинга нецелесообразно использовать асимметричное шифрование.

В симметричных криптосистемах используется один и тот же криптографический ключ для шифрования и дешифрования, который должен сохраняться в секрете обеими сторонами. В итоге мы получаем, что алгоритмы с закрытым ключом работают на три порядка быстрее алгоритмов с открытым ключом. Однако одним из недостатков симметричных шифров является невозможность их использования для подтверждения авторства, так как ключ известен каждой стороне.

Для повышения надежности симметричных криптографических ключей в ряде работ предложено использовать регистрируемые датчиками биосигналы, которые отражают физиологические особенности пациента и могут использоваться для сокрытия информации [13, 14].

Подобный подход основывается на следующих положениях:

- 1) физиологические сигналы сложны, изменчивы, достаточно уникальны. Вместе с тем существуют характеристики, отражающие морфологию сигнала, которые относительно стабильны;
- 2) физиологические сигналы могут быть искусственно сгенерированы с помощью генератора модельного сигнала при условии, что данная модель верно построена на основе информации о состоянии человека.

Предлагаемый подход к решению поставленной задачи

Предлагается в качестве морфологических признаков использовать информацию, полученную по математической модели генератора биосигнала в форме системы дифференциальных уравнений. Морфологическими признаками в этом случае является как сама структура модели, так и ее параметры. Задача определения морфологических признаков в этом случае сводится к задаче реконструкции модели системы, которая генерирует временные ряды, диагностически эквивалентные исходным сигналам.

Реконструкция модели сложной системы по наблюдаемому временному ряду (обратная задача динамики) успешно применяется для решения различных задач. В условиях неполных данных метод реконструкции позволяет оценить состояние системы, выявить особенности поведения, прогнозировать ее развитие. Эти задачи являются крайне важными при дистанционном мониторинге состояния сложных систем. Модельный подход к анализу систем с использованием реконструкции хорошо зарекомендовал себя при обработке биосигналов человека [15].

Рассмотрим применение указанного подхода на примере использования сфигмограммы, которая регистрирует колебания артериальной стенки сосуда, обусловленные выбросом ударного объема крови в артериальное русло.

В качестве примера используем модельное уравнение пульсации стенки сосуда в форме уравнения Ван-дер-Поля – Релея:

$$\ddot{x} + [\varepsilon_1(x^2 - r^2) + \varepsilon_2(\dot{x}^2 - \omega_0^2 \cdot r^2)] \cdot \dot{x} + ax = P(\omega_0 t).$$

Здесь x – это перемещение стенки кровеносного сосуда, регистрируемое датчиком; $P(\omega_0 t)$ – воздействие сердечной активности на динамику стенки сосуда. Параметры уравнения, отражающие такие свойства сосуда, как податливость, диссипацию, свойственны любым сосудам и вместе с тем уникальны для отдельного человека. Результаты моделирования представлены на рис. 2, где приведены выходные сигналы объекта и модели.

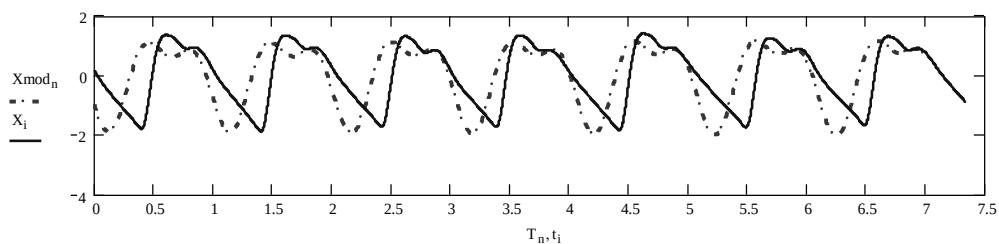


Рис. 2. Результаты моделирования

Представленные результаты, демонстрирующие сходство динамического поведения реального объекта и его модели, подтверждают хорошую адекватность модели относительно основных динамических свойств. Кроме того, преимущество представленной модели состоит в том, что параметр a имеет физический смысл: он позволяет оценивать «жесткость» сосудов за счет работы обволакивающих их гладких мышц.

Если реконструированная модель адекватно описывает регистрируемые биосигналы, то ее структура и параметры используются для формирования криптографических ключей в системе защиты информации.

Заключение

В ходе работы был предложен подход, основанный на реконструкции математической модели генератора биосигнала. Его реализация в системах мониторинга позволит не только повысить адекватность оценки состояния целостного организма человека на основе множественных неинвазивных измерений, но и сформировать морфологические признаки для формирования «физиологической» подписи. Эти признаки включают структуру модели, используемой для оценки состояния человека, и ее физиологически значимые параметры.

Литература

1. Развитие системы электронных услуг муниципальной поликлиники (на основе анализа зарубежных web-ресурсов) / А.В. Ланцберг, К. Тройч, Т.И. Булдакова // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2011. № 4. С. 1-7.
2. Prado M., Roa L., Reina-Tosina J. Virtual Center for Renal Support: Technological Approach to Patient Physiological Image // IEEE Transaction on biomedical engineering. 2002. Vol. 49, №12. Pp.1420-1430.
3. Концептуальная модель виртуального центра охраны здоровья населения / В.С. Анищенко, Т.И. Булдакова, П.Я. Довгалецкий и др. // Информационные технологии. 2009. №12. С. 59-64.
4. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2). С. 28-35.
5. Булдакова Т.И., Кривошеева Д.А. Угрозы безопасности в системах дистанционного мониторинга // Вопросы кибербезопасности. 2015. № 5(13). С. 45-50.
6. Paradiso R., Loriga G., Taccini N. A Wearable Health Care System Based on Knitted Integrated Sensors // IEEE Transactions on Information Technology in Biomedicine. 2005. Vol. 9, No. 3. Pp. 337-344.

7. Булдакова Т.И., Коблов А.В., Суятинов С.И. Информационно-измерительный комплекс совместной регистрации и обработки биосигналов // Приборы и системы. Управление, контроль, диагностика. 2008. № 6. С. 41-46.
8. Программно-аналитический комплекс модельной обработки биосигналов / Т.И. Булдакова, В.И. Гриднев, К.И. Кириллов и др. Биомедицинская радиоэлектроника. 2009. № 1. С. 71-78.
9. Баевский Р.М. Проблема оценки и прогнозирования функционального состояния организма и ее развитие в космической медицине // Успехи физиологических наук. 2006. Т. 37, № 3. С. 42-57.
10. Моделирование связей в системе «сердце-сосуды» / Н.С. Булдаков, Н.С. Самочетова, А.С. Ситников, С.И. Суятинов // Наука и образование: электронное научно-техническое издание. 2013. № 1. С. 123-134.
11. Banerjee A., Gupta S.K.S., Venkatasubramanian K.K. PEES: Physiology-based End-to-End Security for mHealth // Proceedings of the 4th Conference on Wireless Health. 2013. Article No. 2.
12. Булдакова Т.И., Суятинов С.И., Кривошеева Д.А. Обеспечение информационной безопасности в телемедицинских системах на основе модельного подхода // Вопросы кибербезопасности. 2014. № 5(8). С. 21-29.
13. Venkatasubramanian K.K., Banerjee A., Gupta S.K.S. PSKA: Usable and secure key agreement scheme for body area networks // IEEE Transactions on Information Technology in Biomedicine. 2010. Vol. 14, No 1. Pp. 60-68.
14. McSharry P.E., Clifford G.D., Tarassenko L., Smith L.A. A dynamical model for generating synthetic electrocardiogram signals // IEEE Transactions on Biomedical Engineering. 2003. Vol. 50, No 3. Pp. 289-294.
15. Методика идентификации сложных систем / А.В. Коблов, А.В. Ланцберг, Н.С. Самочетова, С.И. Суятинов // Вестник СГТУ. 2007. №4 (27). С. 31-37.

Security Threats in Systems of the Remote Monitoring **Buldakova T.I., Krivosheeva D.A.⁷³**

The article focuses on the security of data transmitted to the remote monitoring systems. Analyzed a model of potential threats to the system of remote monitoring of human health. It has been demonstrated that the previously proposed approaches to security are not effective. An alternative approach based on the reconstruction of the model of a complex system on the recorded biosignals.

Keywords: information security, telemedicine, biosignals, cryptographic keys.

⁷³ Tatiana Buldakova, Doctor of Technical Sciences, Professor, Bauman Moscow State Technical University, Moscow, buldakova@bmstu.ru; Darina Krivosheeva, Bauman Moscow State Technical University, Moscow, darinaaleks@gmail.com

Применение обучающей среды имитационного моделирования на основе технологии облачных вычислений при изучении дисциплины «Моделирование систем» для подготовки специалистов по информационной безопасности

Быков А.Ю.⁷⁴, Глинская Е.В.⁷⁵, Стручкова А.В.⁷⁶, Колинко Ф.К.⁷⁷

Аннотация. В работе представлено обучающее средство имитационного моделирования систем, основанное на технологии облачных вычислений, внедренное в учебный процесс для дистанционных исследований и обучения. Средство реализовано на языке Java в виде Web-приложения. Имитационные эксперименты выполняются на стороне сервера, на стороне клиента вводятся тексты моделей в форму Web-браузера. Для моделирования может использоваться язык Java со специальной библиотекой классов или язык, похожий на GPSS. Приведены результаты экспериментов с типовой моделью.

Ключевые слова: имитационное моделирование, облачные вычисления, дистанционное обучение

Введение

В последние десятилетия активно развиваются распределенные системы разработки, в том числе, системы ориентированные на использование сети Интернет и облачные технологии. При имитационном моделировании (ИМ) сложных систем, как правило, требуются большие вычислительные мощности, поэтому использование технологии распределенных вычислений является актуальным. При использовании облачных вычислительных технологий для ИМ эксперименты могут проводиться как на стороне клиента, так и на стороне сервера. Модель распределения заданий между клиентом и сервером в облачных вычислениях и эксперименты по распределению заданий рассмотрены в [1, 2]. Если эксперименты проводятся на стороне сервера, то клиентами могут быть средства с ограниченными вычислительными ресурсами, например, мобильные устройства, что расширяет географию нахождения исследователей. Мобильное устройство в данном случае используется как устройство ввода и редактирования исходного теста модели на заданном языке моделирования.

Реализация среды моделирования в сети Интернет и выполнение экспериментов на стороне сервера открывает пользователям дополнительные возможности, в числе которых: нулевая инсталляция (для работы достаточно стандартного браузера, нет необходимости устанавливать специальное программное обеспечение), простота обмена моделями (каждая модель может быть размещена в сети), Интернет дает возможность донести результаты своей работы до широкой аудитории за короткий срок, что является преимуществом для среды моделирования, используемой при обучении.

Приведем примеры систем моделирования, в той или иной степени, опирающиеся на использование сети Интернет: Язык SLX (Simulation Language with Extensibility), SIMUL8, RT-LAB, GridSim, Forio, WebGPSS (aGPSS), Oryx, AnyLogic, Web-среда компьютерного моделирования процессов, протекающих в стационарных линейных динамических системах (НИЯУ МИФИ) и др.

Рассмотрим обучающую систему ИМ SimJavaWeb, реализованную в виде Web-

⁷⁴Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru

⁷⁵Глинская Елена Вячеславовна, МГТУ им. Н.Э. Баумана, Москва, glinskaya-ju8@rambler.ru

⁷⁶Стручкова Александра Валентиновна, МГТУ им. Н.Э. Баумана, Москва, nissa-93@mail.ru

⁷⁷Колинко Федор Константинович, МГТУ им. Н.Э. Баумана, Москва, wolfikolinko@gmail.com

приложения, на языке Java, используемую в учебном процессе при подготовке специалистов по информационной безопасности. Основная особенность системы заключается в том, что моделирование выполняется на стороне сервера, компьютер клиента используется для ввода исходного кода модели через Web-браузер. Исходный код может вводиться как на языке Java с использованием библиотеки классов для ИМ [3], так и на языке, похожем на GPSS [4], для этого на сервере реализован специальный интерпретатор языка.

Кроме среды моделирования в Web-приложении реализованы основные функции дистанционной системы обучения с учетом особенностей учебного процесса в МГТУ им. Н.Э. Баумана и рейтинго-модульной системы.

1. Описание обучающей среды моделирования SimJavaWeb

Обучающая среда моделирования SimJavaWeb представляет собой кроссплатформенное Web-приложение, построенное на технологии Java-сервлетов. Приложение имеет модульную структуру, упрощенная структура модулей приложения (рис. 1).

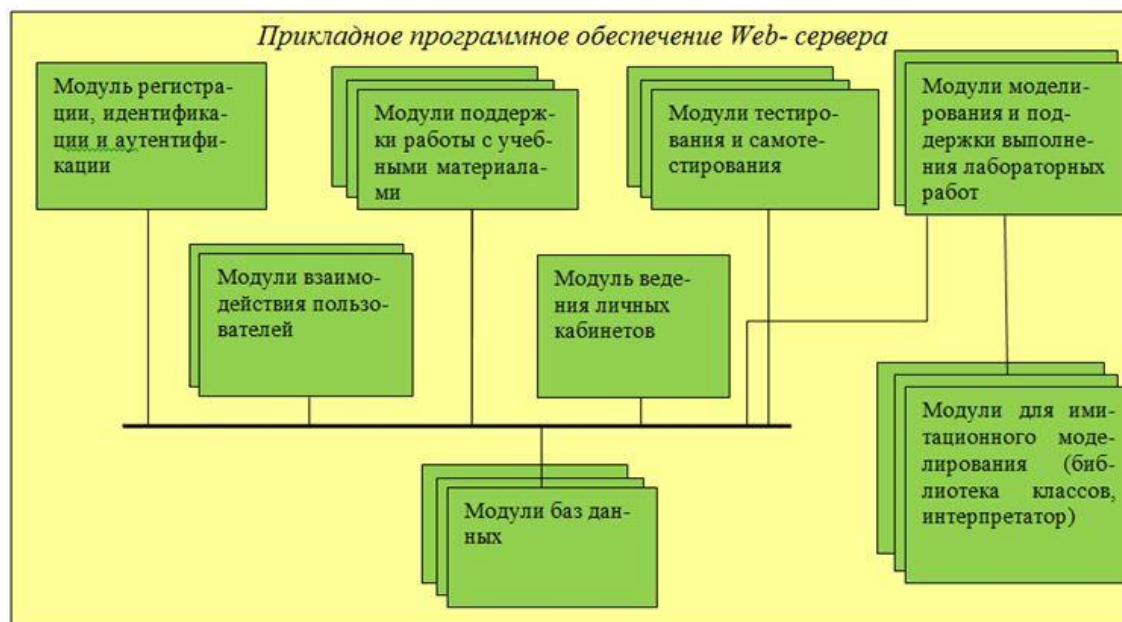


Рис.1. Назначение основных программных модулей среды моделирования и их взаимосвязи

При работе с ресурсом введены два вида пользователей: пользователь-студент и пользователь-преподаватель.

Студенту доступны следующие функции:

- ввод исходных текстов моделей как на языке программирования Java с использованием библиотеки классов для ИМ, так и на языке, похожем на GPSS, хранение моделей на сервере, их отладка и запуск на стороне сервера;
- получение доступа к учебным материалам сервера;
- знакомство с объявлениями для студентов;
- представление текстов имитационных моделей в качестве заданий лабораторных работ на проверку преподавателю, получение уведомлений от преподавателя о результатах проверки;
- представление отчетов по лабораторным работам на проверку преподавателю, получение уведомлений от преподавателя о результатах проверки;
- просмотр данных о модулях курса, с указанием контрольных мероприятий и

- выставленных за них баллах;
- проведение самотестирования по темам курса;
- автоматическое получение на сервере варианта задания для контрольной работы во время выполнения контрольной работы;
- получение статистических данных о своей успеваемости;
- получение справочной информации с примерами моделей и возможностью их запуска на стороне сервера;
- участие в форуме.

Преподавателю, кроме перечисленных, доступны функции:

- предоставление прав доступа зарегистрированным студентам;
- размещение на сервере учебных материалов (лекций, семинаров, лабораторных работ) и объявлений для студентов;
- получение уведомлений о представленных студентами текстах имитационных моделей, проверка текстов моделей с возможностью их запуска на стороне сервера, ввод данных о результатах проверки;
- получение уведомления о представленных студентами отчетов по лабораторным работам, проверка отчетов, ввод данных о результатах проверки;
- ввод данных о модулях курса, с указанием контрольных мероприятий и выставяемых за них баллах;
- ввод данных о полученных студентами баллах по контрольным мероприятиям и семинарам;
- ввод тестов в базу данных сервера для тестирования и самотестирования студентов;
- размещение на сервере вариантов заданий для контрольных работ, для последующей автоматической раздачи студентам;
- получение статистических данных об успеваемости студентов по выбранным учебным группам;
- редактирование материалов форума;
- резервное копирование и восстановление баз данных сервера.

2. Пример модели

Рассмотрим задачу. В системе электронного документооборота есть программный модуль защиты документов от несанкционированного доступа, который осуществляет обработку запросов пользователей при обращении к документам. Поток запросов пуассоновский с интенсивностью $\lambda = 1$ (запрос в секунду). Время обработки запроса есть случайная величина, распределенная по показательному закону, со средним значением $\bar{T} = 0,8$ с. Модуль в каждый момент времени может обрабатывать только 1 запрос, если модуль занят, то запрос становится в очередь, длина которой не ограничена. Необходимо провести моделирование системы при обслуживании 1000 000 запросов, найти: загрузку модуля, среднюю длину очереди и среднее время пребывания запроса в очереди.

Данная задача является примером системы массового обслуживания типа М/М/1 и имеет аналитическое решение [5], в частности, загрузка модуля – 0,8, средняя длина очереди – 3,2 запроса, среднее время пребывания в очереди – 3,2 с.

Исходный текст модели на языке Java с использованием библиотеки классов для ИМ в браузере (рис. 2).

```

import java.io.PrintWriter;
import SimJava.*;
//Одноканальная СМО с неограниченной очередью
public class MyModel extends Syst implements Runnable{
    Facility pF; // Ссылка на канал обслуживания
    Queue pQ; // Ссылка на очередь
    public MyModel()
    {
        super(1000000, null, null); // 1000000 - начальное значение счетчика завершения
        th=new Thread(this);
        out=new PrintWriter(System.out, true); // Создание потока для вывода в HTML страницу
        // Создание модельной среды
        pQ=new Queue(this, "Очередь"); // Создаем очередь
        pF=new Facility(this, "Канал"); // Создаем канал обслуживания
    }
    public void run()
    {
        initGenerate(1, 0); // Транзакт заявка направляется к первому событию
        while(tgl!=0) // Конец моделирования когда TGL (счетчик завершения равен 0)
        {
            plan();
            switch(sysEvent)
            {
                case 1: generate(v1.randExp(1, false)); break; // Генерация заявок
                case 2: pQ.queue(1); break; // Занимаем очередь
                case 3: pF.seize(); break; // Занимаем канал обслуживания
                case 4: pQ.depart(1); break; // Освобождаем очередь
                case 5: advance(v12.randExp(1/0.8, false)); break; // Задержка - время обслуживания
                case 6: pF.release(); break; // Освобождаем канал обслуживания
                case 7: terminate(1); // Транзакт уничтожается, счетчик завершения уменьшается на 1
            }
        }
        printAllHTML(); // Вывод результатов моделирования в HTML страницу
    }
    public static void main(String args []) {
        MyModel mod=new MyModel();
        mod.out.println("<br>Результаты моделирования:");
        mod.th.start();
        try { mod.th.join(); } catch(Exception e1) {} // Ждем завершения потока моделирования
    }
}

```

Рис 2. Исходный текст модели на языке Java в браузере

Результаты моделирования на языке Java (рис.3)

Системный параметр модели	Значение
СИСТЕМНОЕ ВРЕМЯ : SysTime=	1000104.2919120752
СИСТЕМНОЕ СОБЫТИЕ : SYSEVENT=	7
TRANS=	null
ВСЕГО ВЫПОЛНЕНО СОБЫТИЙ : EVENTALL=	7800848.0
ЗАТРАЧЕНО ВРЕМЯ : REALTIME=	0.8950002193450928 СЕК
СКОРОСТЬ ИСПОЛНЕНИЯ : EVESPEED=	8716029.148806456 СОБ/СЕК
СРЕДНЕЕ ВРЕМЯ ИСПОЛНЕНИЯ СОБЫТИЯ : MEANTIME=	1.1473114453006811Е-7 СЕК/СОБ

Параметры возникновения событий модели:	
Событие №	Всего
1	1000005
2	1000005
3	1000000
4	1000000
5	1000000
6	1000000
7	1000000

Параметры очередей модели:						
Очередь	Число входов	Число вх. с 0 врем.ож.	Макс.длина	Сред.длина	Текущая длина	Сред.вр.ож.
Очередь	1000005	199167	50	3.1950980384584216	5	3.195414942654946

Параметры одноканальных устройств модели:				
Прибор	число входов	Сред.вр.обработки	Загрузка	Число захватов
Канал	1000000	0.8005735848535274	0.8004901002103791	0

Рис 3. Результаты моделирования на языке Java

Исходный текст модели на языке, похожем на GPSS, с комментариями в браузере (рис. 4).

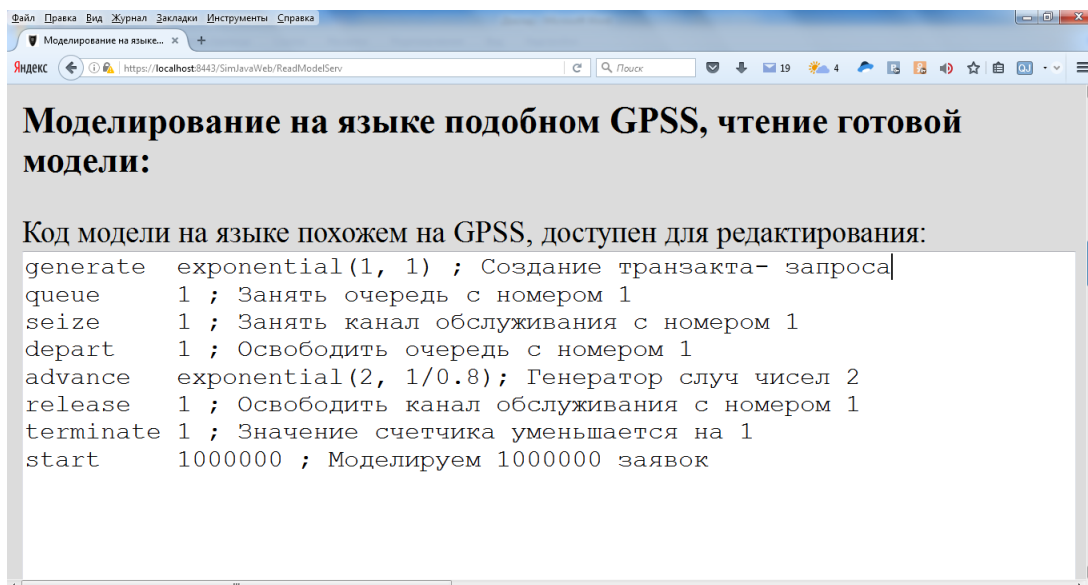


Рис 4. Исходный текст модели на языке, похожем на GPSS, в браузере

Результаты моделирования на языке, похожем на GPSS (рис.5)

6) release 1
7) terminate 1

Общие системные параметры после прогона модели:

Системный параметр модели	Значение
СИСТЕМНОЕ ВРЕМЯ : SysTime=	1000106.049008007
СИСТЕМНОЕ СОБЫТИЕ : SYSEVENT=	7
TRANS=	null
ВСЕГО ВЫПОЛНЕНО СОБЫТИЙ : EVENTALL=	7800143.0
ЗАТРАЧЕНО ВРЕМЯ : REALTIME=	17.784000158309937 СЕК
СКОРОСТЬ ИСПОЛНЕНИЯ : EVESPEED=	438604.5282593649 СОБ/СЕК
СРЕДНЕЕ ВРЕМЯ ИСПОЛНЕНИЯ СОБЫТИЯ : MEANTIME=	2.2799582210620928E-6 СЕК/СОБ

Параметры возникновения событий модели:

Событие №	Всего
1	1000006
2	1000006
3	1000000
4	1000000
5	1000000
6	1000000
7	1000000

Параметры очередей модели:

Очередь	Число входов	Число вх. с 0 врем.ож.	Макс.длина	Сред.длина	Текущая длина	Сред.вр.ож.	Сред.вр.ож.без уч.0 вх	% вх.в пуст.очер.
1	1000006	199875	52	3.2072537369027967	6	3.207575917882024	4.00883401745094	19.987380075719546

Параметры одноканальных устройств модели:

Прибор	число входов	Сред.вр.обработки	Загрузка	Число захватов	Состояние
1	1000000	0.7999949156189096	0.7999100859477999	0	FREE

Рис 5. Результаты моделирования на языке, похожем на GPSS

Выводы

В докладе представлено обучающее средство имитационного моделирования, построенное на основе технологии облачных вычислений, и рассмотрены его возможности при использовании в учебном процессе в дистанционном режиме. Результаты

представленных имитационных экспериментов с моделью, имеющей аналитическое решение, показали, что полученные результаты моделирования соответствуют результатам, полученными при расчете аналитической модели, что подтверждает их достоверность. Дополнительные возможности дистанционной системы обучения с учетом особенностей учебного процесса в МГТУ им. Н.Э. Баумана, в частности рейтинго-модульной системы, помогают студентам отслеживать данные о результатах контрольных мероприятий, что дополнительно стимулирует студентов на самообучение для повышения успеваемости.

Работа выполнена при поддержке благотворительного фонда Владимира Потанина.

Литература

1. Быков А. Ю., Медведев Н.В., Панфилов Ф.А. Тестирование клиента и сервера для выбора объекта проведения экспериментов в инструментальном программном средстве имитационного моделирование на основе технологии "облачных" вычислений // Инженерный журнал: наука и инновации. Электронное научно-техническое издание. 2013. № 11. URL: <http://engjournal.ru/catalog/it/network/989.html>
2. Быков А. Ю. Задача распределения заданий между клиентом и сервером в имитационном моделировании на основе технологии облачных вычислений и результаты экспериментов по ее решению // Инженерный вестник МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 1. URL: <http://engbul.bmstu.ru/doc/697425.html>
3. Быков А. Ю., Панфилов Ф.А., О.О. Сумарокова О.О. Имитационное моделирование с применением библиотеки классов языка Java, разработанной для «облачных» сервисов // Инженерный журнал: наука и инновации. Электронное научно-техническое издание. 2013. № 2. URL: <http://engjournal.ru/catalog/it/hidden/535.html>
4. Быков А. Ю., Кожемякина Е.В., Панфилов Ф.А. Имитационное моделирование систем массового обслуживания в клиентских приложениях при использовании технологии "облачных" вычислений // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 11. URL: <http://engjournal.ru/catalog/it/network/1001.html>
5. Вентцель Е.С. Исследование операций: задачи, принципы, методология: учебное пособие. М.: КНОРУС, 2014. 192 с.

The Use of Educational Simulation Tools Based on the Cloud Computing Technology in the Study of the Systems Simulation Discipline for Training Specialists in Information Security

Bykov A.Yu.⁷⁸, Glinskaya E.V.⁷⁹, Struchkova A.V.⁸⁰, Kolin'ko F.K.⁸¹.

Abstract. The work presents educational simulation tools based on the cloud computing technology and implemented in the educational process for the remote research and teaching. The tool is implemented in Java as a Web application. Simulation experiments are performed on the server side, client-side text models are introduced in the form of Web-browser. The Java language with the special class library for simulation or language similar to GPSS can be used for the simulation. The results of experiments with the standard model are presented.

Keywords: simulation, cloud computing, distance learning

⁷⁸Aleksandr Bykov, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, abykov@bmstu.ru

⁷⁹Elena Glinskaya, Bauman Moscow State Technical University, Moscow, glinskaya-ju8@rambler.ru

⁸⁰Aleksandra Struchkova, Bauman Moscow State Technical University, Moscow, nissa-93@mail.ru

⁸¹Fedor Kolin'ko, Bauman Moscow State Technical University, Moscow, wolfikolinko@gmail.com

Автоматизированное обнаружение уязвимостей в веб-приложениях с помощью Team Foundation Server и OWASP ZAP

Булдакова Т. И.⁸², Коршунов А.В.⁸³

Описан механизм автоматизированного обнаружения уязвимостей в веб-приложениях с помощью Team Foundation Server и OWASP ZAP. Team Foundation Server – это продукт компании Microsoft для совместной работы над проектами по разработке программного обеспечения. OWASP ZAP - это инструмент тестирования для обнаружения уязвимостей в веб-приложениях. Разработано консольное приложение, которое взаимодействует с OWASP ZAP через API и сообщает результаты тестирования TFS-серверу. Данный механизм обеспечивает безопасный цикл разработки веб-приложений и позволяет снизить затраты на обеспечение информационной безопасности веб-приложений.

Ключевые слова: безопасный цикл разработки, Team Foundation Server, OWASP ZAP

Введение

Современные тенденции в области информационной безопасности (ИБ) характеризуются устойчивым ростом количества компьютерных атак, приводящих к снижению уровня защищенности ресурсов автоматизированных систем [1, 2]. В большинстве случаев основной причиной успешности компьютерной атаки является наличие уязвимостей программного обеспечения (ПО), используемого в составе таких систем [3]. Наиболее распространенными типами уязвимостей, выявленных в программных средствах (ПС) являются: аутентификационные данные в исходном коде ПС, межсайтовый скриптинг, внедрение SQL-кода.

Одним из направлений повышения уровня безопасности ПО является внедрение в рамках жизненного цикла ПО различных процедур, касающихся снижения числа ошибок и уязвимостей [4–8]. Опыт компании Microsoft показал, что внедрение цикла разработки безопасных ПС позволило сократить число уязвимостей в ПС компании в среднем на 80% [4]. Одна из возможных процедур для уменьшения числа уязвимостей - создание сборщика приложений, который будет выполнять тестирование на проникновение для различных сайтов. В настоящий момент существуют различные инструменты для тестирования на проникновение как бесплатные, так и коммерческие. В данной статье описан способ использования бесплатного приложения OWASP ZAP, которое учитывает большинство известных уязвимостей и имеет собственный интерфейс прикладного программирования (API) для вызова встроенных функций [9].

Архитектура решения

Основная идея заключается в том, чтобы создать консольное приложение (далее – приложение), которое будет взаимодействовать с OWASP ZAP и сообщать результат взаимодействия серверу, который отвечает за сборку. Основные этапы работы при такой схеме (рис.1):

- сервер Team Foundation Server (TFS) вызывает приложение, предоставляя URL-адрес для сканирования;
- приложение подключается к OWASP ZAP через API и начинает сканирование;
- приложение запрашивает состояние процесса сканирования, пока он не закончится;
- приложение получает результаты сканирования, агрегирует их и возвращает в процесс сборки, так что TFS-сервер выводит отчет о сканировании в журнал сборки.

⁸² Булдакова Т.И., профессор, д-р техн. наук, МГТУ им. Н.Э. Баумана, Москва, Россия, buldakova@bmstu.ru

⁸³ Коршунов А.В., МГТУ им. Н.Э. Баумана, Москва, Россия, korshun3101@rambler.ru

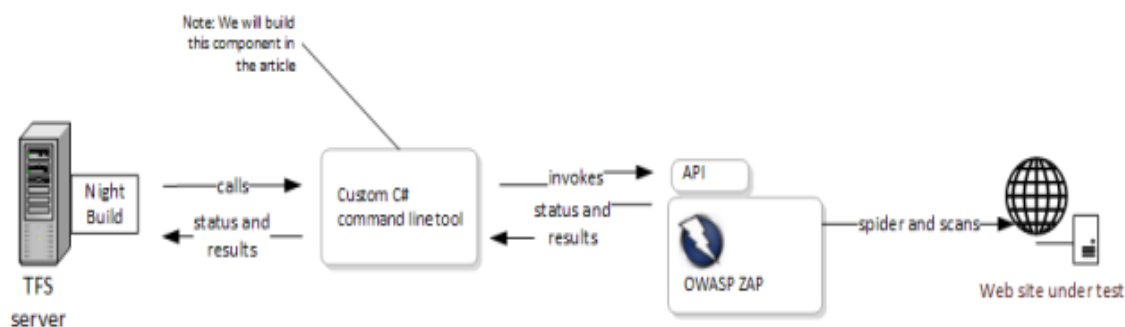


Рис. 1. Схема взаимодействия TFS-сервера и OWASP ZAP

Для реализации данной схемы необходимо выполнить несколько шагов:

- 1) скачать OWASP ZAP с официальной страницы и установить его;
- 2) разработать консольное приложение (в данной работе для этого будет использован язык программирования C#);
- 3) установить и настроить TFS-сервер. Когда он установлен и запущен, необходимо настроить правила сборки для вызова функций из командной строки.

Рассмотрим эти шаги.

Запуск OWASP Zed Attack Proxy

OWASP Zed Attack Proxy (ZAP) - это простой в применении инструмент тестирования проникновений, служащий для обнаружения уязвимостей веб-приложений. Он разработан для использования людьми с различным опытом в сфере ИБ и является эталоном для разработчиков и тестировщиков, которые не имеют опыта в тестировании на проникновение [9]. OWASP ZAP можно скачать с официального сайта проекта OWASP. После установки необходимо запустить локальный прокси-сервер. Для этого в меню Сервис->Параметры->Локальный прокси-сервер необходимо установить адрес и порт для прокси-сервера. Его можно настроить для запуска с локального хоста (OWASP ZAP и TFS-сервер будут работать на одном физическом сервере) через порт 8090 (рис. 2).

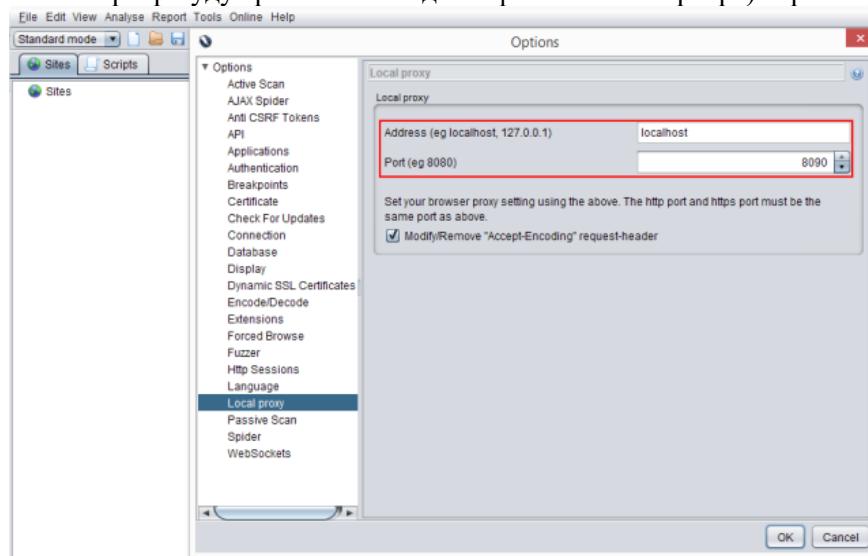


Рис. 2. Настройка OWASP ZAP

После этого можно получить доступ к OWASP ZAP через браузер с помощью запроса <http://localhost:8090>. Если прокси-сервер работает, появится стартовая страница OWASP ZAP (рис. 3).

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

Proxy Configuration

To use ZAP effectively it is recommended that you configure your browser to proxy via ZAP.

You can do that manually or by configuring your browser to use the generated [PAC file](#).

Links

- [Local API](#)
- [ZAP Homepage](#)
- [ZAP Wiki](#)
- [ZAP User Group](#)
- [ZAP Developer Group](#)
- [Report an issue](#)

Рис. 3. Стартовая страница OWASP ZAP

Теперь OWASP ZAP запущен и его API доступно для приложения.

Работа с TFS-сервером

Team Foundation Server - продукт компании Microsoft, представляющий собой комплексное решение, объединяющее в себе систему управления версиями, сбор данных, построение отчётов, отслеживание статусов и изменений по проекту и предназначенное для совместной работы над проектами по разработке ПО.

Для подключения TFS-сервера к консольному приложению создадим новую сборку (можно использовать существующую сборку) и добавим к ней определенные правила, которые будут запускать приложение для сканирования. Для этого необходимо перейти в Visual Studio Toolbox и добавить процесс InvokeProcess в алгоритм сборки. Также необходимо включить свойство WriteBuildMessage во входном параметре процесса InvokeProcess и WriteBuildError в выходном параметре (рис. 4).

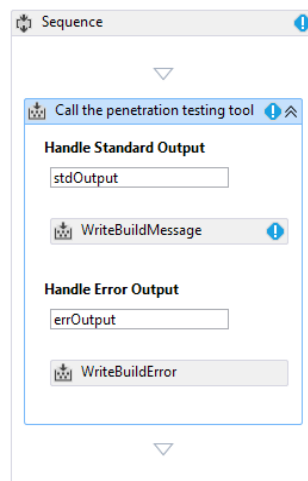


Рис. 4. Настройка правил сборки на TFS-сервере

Далее необходимо передать URL для сканирования в консольное приложение. Для этого создадим новый аргумент с именем UrlToScan типа String (рис. 5).

Name	Direction	Argument type	Default value
MSBuildPlatform	In	ToolPlatform	Microsoft.TeamFo
PerformTestImpactAnalysis	In	Boolean	True
CreateLabel	In	Boolean	True
DisableTests	In	Boolean	False
GetVersion	In	String	Enter a VB express
PrivateDropLocation	In	String	Enter a VB express
Verbosity	In	BuildVerbosity	Microsoft.TeamFo
Metadata	Property	ProcessParameterMetadataCollection	(Collection)
SupportedReasons	Property	BuildReason	All
UrlToScan	In	String	Enter a VB express

Рис. 5. Добавление аргумента UrlToScan

Теперь мы должны сообщить InvokeProcess необходимые аргументы. Для этого задаем следующие свойства (рис. 6):

- UrlToScan адрес для сканирования;
- DisplayName отображаемое имя для InvokeProcess;
- FileName путь к приложению.

Misc	
Arguments	[UrlToScan]
DisplayName	Call the penetration testing tool
EnvironmentVariables	Specify any additional environment variables and their values.
FileName	"c:\Program Files\ZAP\ZAPPenTester.exe"
OutputEncoding	System.Text.Encoding.GetEncoding(System.Globalization.CultureInfo.In
Result	Enter a VB expression
WorkingDirectory	Specify the local working directory for the process.

Рис. 6. Свойства процесса InvokeProcess

Для завершения настройки необходимо изменить свойство WriteBuildMessage на WriteBuildError. Это необходимо для вывода журнала, который генерирует консольное приложение после сканирования. После этого сохраним сборку, и настройка TFS-сервера будет завершена. Убедимся, что TFS-сервер использует новые правила сборки и правильно принимает URL для сканирования через аргумент UrlToScan. Для проверки можно запустить сборку и проверить результаты. После успешного завершения сборки мы получаем журнал, который сгенерировало консольное приложение во время сканирования (рис. 7).

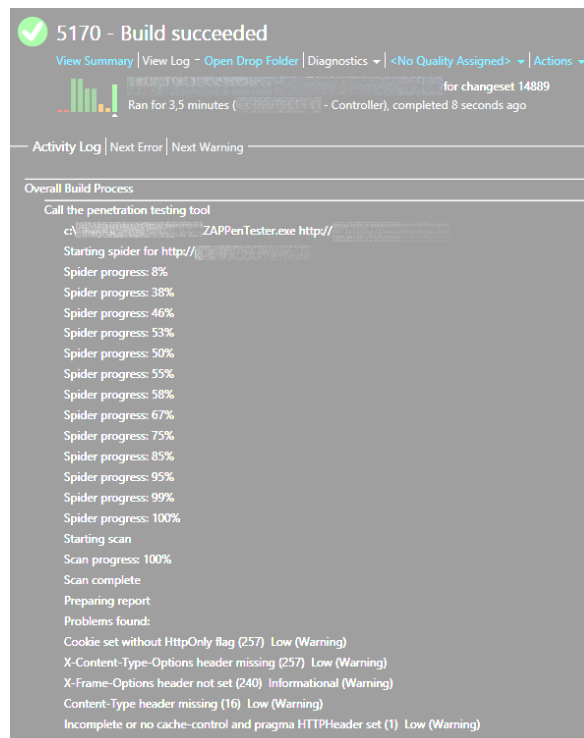


Рис. 7. Журнал сборки с результатами сканирования

Таким образом, нам удалось создать сборщик приложений, который сообщает о проблемах безопасности, обнаруженных на целевом сайте.

Консольное приложение

Приложение для подключения к API OWASP ZAP является консольным приложением на C#. При запуске OWASP ZAP становится доступным его API. Через API можно вызывать такие функции, как запуск паука (обнаружение всех доступных страниц сайта), проверка состояния паука, запуск сканера, проверка состояние сканера, получение списка обнаруженных уязвимостей. Мы можем выбрать, в каком формате получать ответы по API: Json, Xml или Html.

Основные параметры консольного приложения:

- ZapStartFile путь к exe-файлу OWASP ZAP;
- ZapWorkingDirectory папка, где находится exe-файл OWASP ZAP;
- ZapProxu адрес прокси-сервера.

Приложение должно работать в 5 этапов:

1. Открыть OWASP ZAP;
2. Передать аргументы в OWASP ZAP для сканирования целевого сайта;
3. Запросить уязвимости, найденные во время сканирования;
4. Закрыть ZAP;
5. Сбор данных и вывод журнала сканирования.

Выходные данные приложения будут отображаться в журнале сборки. Есть несколько объектов, которые составляют ядро приложения. На диаграмме ниже (рис. 8) показаны входы/выходы для каждого компонента.

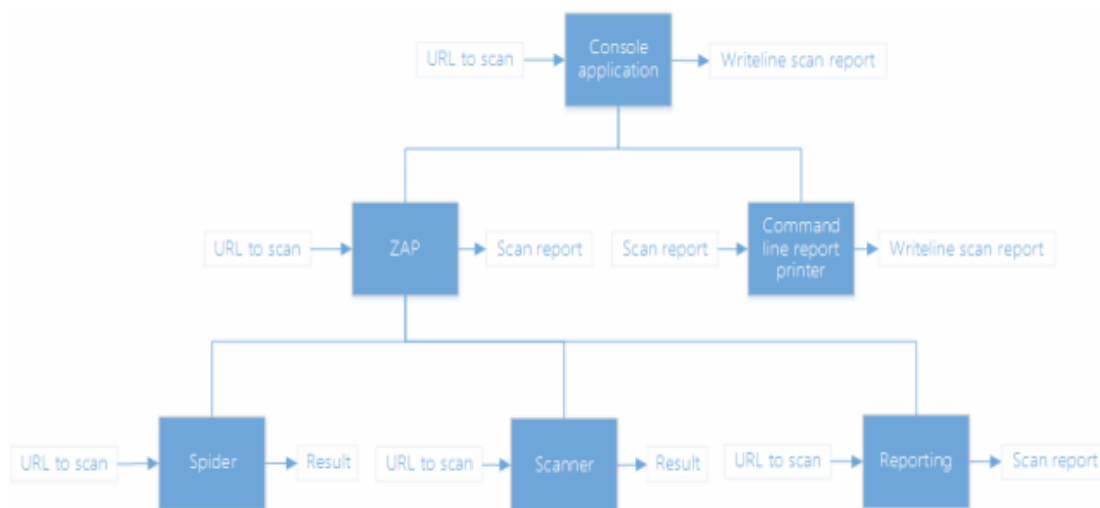


Рис. 8. Схема работы консольного приложения

API предоставляет доступ к большинству функциональных возможностей OWASP ZAP. Для достижения целей данной работы в API были доступны все необходимые функции.

Заключение

Целью описанного механизма автоматизированного обнаружения уязвимостей в веб-приложениях с помощью Team Foundation Server и OWASP ZAP является снижения числа ошибок и уязвимостей в рамках жизненного цикла разработки ПО. Данная цель достигнута путем обнаружения уязвимостей на этапе сборки приложения. Кроме обеспечения безопасного цикла разработки, описанный механизм позволяет снизить затраты на обеспечение информационной безопасности веб-приложений, т.к. затраты по устранению уязвимостей гораздо ниже на этапе разработки, чем в процессе эксплуатации приложений.

Литература

1. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5 (13). С. 2-10.
2. Булдакова Т.И., Коршунов А.В. Обеспечение информационной безопасности ERP-систем // Вопросы кибербезопасности. 2015. № 5 (13). С. 41-44.
3. Михайлов Д.М., Жуков И.Ю., Шеремет И.А. Защита автоматизированных систем от информационно-технологических воздействий. М.: НИЯУ МИФИ, 2014. 184 с.
4. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1 (1). С. 37-41.
5. Еремеев М.А., Беляков И.А. Интеллектуальные технологии при сертификации программ // Автоматика, связь, информатика. 2012. № 2. С. 23-25.
6. Жидков И.В., Шубенин А.А., Хабибуллин И.В., Поздняков С.Ю. Испытания систем защиты информации автоматизированных систем управления // Решетневские чтения. 2013. Т. 2. № 17. С. 281-282.
7. Казарин О.В., Кондаков С.Е., Троицкий И.И. Подходы к количественной оценке защищенности ресурсов автоматизированных систем // Вопросы кибербезопасности. 2015. № 2 (10). С. 31-35.
8. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1 (2). С. 36-39.
9. The Open Web Application Security Project [Электронный ресурс]. - URL: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Automated Penetration Testing of Web Applications Using Team Foundation Server and OWASP Zap

Buldakova T.I.⁸⁴, Korshunov A.V.⁸⁵

This article describes automated penetration testing of web applications using Team Foundation Server and OWASP ZAP. Team Foundation Server is Microsoft's product that was designed to joint software development. OWASP ZAP is easy to use to penetration testing of web applications. Result of this work is application that interacts with the OWASP ZAP via API and reports test results TFS-server. This mechanism provides a secure software development and reduces the cost of web application security.

Keywords: secure software development, Team Foundation Server, OWASP ZAP

УДК 003.26.004.7.004.9

Метод защиты информационной подсистемы САПР от несанкционированного доступа

Волосатова Т.М.⁸⁶

Рассмотрены вопросы информационной безопасности САПР. Предлагается метод сокрытия данных, составляющих коммерческую тайну в информационной подсистеме САПР. Метод основан на организации базы данных, являющейся виртуальным подобием голографического запоминающего устройства. Одним из достоинств технического предложения является то, что его реализация не требует реорганизации реляционных баз данных.

Ключевые слова: голография, объект проектирования, проектная документация.

Введение

Результаты анализа [1, 2] показывают, что в области информационной безопасности (ИБ) систем автоматизированного проектирования (САПР) специальных комплексных разработок не ведется. Такие системы, как САПР, рассматриваются российскими и иностранными специалистами в области ИБ без учета многих специфичных факторов. Несмотря на существование эффективных структур сертификации, обеспечивающих выявление недокументированных возможностей (НДВ) программных продуктов, защиту от программных и аппаратных закладок, а также несанкционированного доступа (НСД) к корпоративной информации, специфичные особенности ИБ САПР пока учитываются не в полной мере. Таким образом, можно полагать, что материалы публикации актуальны.

1. Существо технического предложения

Вопросы защиты от НСД проектной документации, передаваемой по открытым каналам связи, рассмотрены в [4, 5, 6]. Методы защиты основываются на сочетании стеганографических алгоритмов и цифровой голографии. Для обеспечения ИБ, собственно, САПР актуально создать средства защиты информационной компоненты, не внося кардинальных изменений в систему управления базой данных (СУБД). Для обеспечения защиты от НСД предлагается модифицировать информационную подсистему САПР путем организации хранения цифровых фурье-голограмм проектной документации. Такой подход был предложен ранее в монографии [2, с 22-26]. Структура такой базы данных (БД) дополняется дескрипторной компонентой, обеспечивающей занесение и считывание данных по ключу, однозначно определяемого пространственной частотой и фазой опорной волны, которая определяет запись и восстановление фурье-

⁸⁴ Professor, Bauman Moscow State Technical University, Moscow, buldakova@bmstu.ru

⁸⁵ Bauman Moscow State Technical University, Moscow, korshun3101@rambler.ru

⁸⁶ Волосатова Т.М., канд. техн. наук, доцент, МГТУ им. Н.Э. Баумана, г.Москва, tamaravol@gmail.com

голограммы. Как известно, цифровые голограммы Фурье моделируют классические оптические фурье-голограммы и представляют собой запись пространственного преобразования Фурье от рассеянного виртуальным предметом светового поля со сдвинутой виртуальной пространственной несущей – опорной волной. В общем случае голограмму можно представить модельно, как комплексную функцию. Комплексное преобразование Фурье изображения $W(u,v)$ в плоскости записи голограммы представим в форме: $|w(x,y)| \exp\{j\varphi\}$, где $\varphi = \Phi(x,y)$ – аргумент комплексной функции $w(x,y)$. Добавим к волновому полю $w(x,y)$ опорную когерентную волну $\exp\{2\pi j(xv_x + yv_y)\}$, где v_x и v_y – проекции пространственной частоты v и определяются углом падения опорной волны относительно нормали к плоскости регистрации голограммы. Распределение интенсивности в плоскости регистрации представляет собой квадрат модуля интерференции волнового поля $w(x,y)$ и опорной волны:

$$h(x,y) = [|w(x,y)| \exp\{j\varphi\} + \exp\{2\pi j(xv_x + yv_y)\}]^2 = |w(x,y)|^2 \cos[2\pi(xv_x + yv_y) + \varphi] + 1. \quad (1)$$

Единица в этом выражении характеризует дополнительную засветку голограммы пучком света от объекта и обычно опускается. Этот член не содержит фазовой характеристики и не несет никакой информации о восстановленном изображении. Следовательно, получаем:

$$h(x,y) = |w(x,y)|^2 \cos[2\pi(xv_x + yv_y) + \varphi] + A_0, \quad (2)$$

где постоянная составляющая A_0 – максимальное значение $w(x,y) = w(0,0)$. Таким образом, функция $h(x,y)$ является вещественной, положительной и содержит полную информацию (как амплитудную, так и фазовую) об изображении документа, заносимого в БД $W(u,v)$.

Преобразование Фурье от $h(x,y)$ будет состоять из двух слагаемых, являющихся функциями, моделирующими изображение документа $W(u,v)$ и смещенных относительно начала осей координат на величины, определяемыми проекциями несущих частот v_x и v_y :

$$\mathbf{F}\{h(x,y)\} = \tilde{W}(u,v) = W(u - u_0, v - v_0) + W(-u - u_0, -v - v_0) + A(u,v), \quad (3)$$

где $\mathbf{F}\{*\}$ – оператор Фурье-преобразования, $A(u,v)$ – автокорреляционная функция. Автокорреляция $A(u,v)$ располагается в начале координат и подавляется как в цифровой голографии, так и в оптической. Второе изображение $W(-u-M, -v-N)$ является зеркальным отображением $W(u-M, v-N)$ относительно центра осей координат. При использовании фурье-голограммы используется ее свойство избыточности, что позволяет использовать для последующего встраивания только часть массива, содержащего отсчеты цифровой голограммы. Пример процесса формирования и восстановления цифровой фурье-голограммы голограммы приведен на рисунке 1.

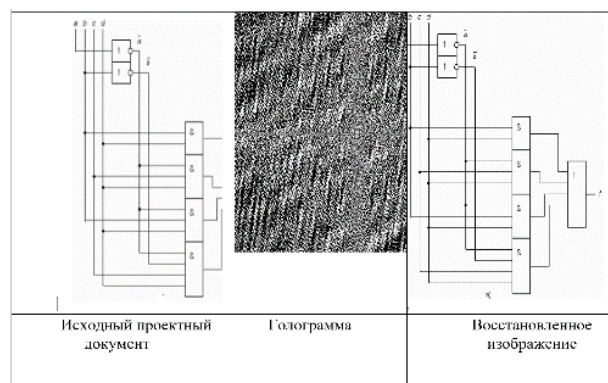


Рис. 1. Пример формирования и восстановления голограммы условного документа

Заключение

Предложенный метод модификации информационной подсистемы САПР обеспечивает: защиту конфиденциальных данных от НСД, высокую плотность записи, определенную свойством избыточности фурье-голограмм, повышенную надежность хранимой документации, поскольку даже при частичной потере голограммы, она успешно восстанавливается с некоторой потерей дифракционной эффективности [4, 5, 6].

Литература

1. Волосатова Т.М., Чичварин И.Н. Специфика информационной безопасности САПР// Известия высших учебных заведений. Машиностроение (специальный выпуск.) – 2012. С. 12 – 20.
2. Официальный сайт ОКБ САПР: www.accord.ru: Программно-аппаратные комплексы защиты информации от НСД. Последний доступ: 02.10.2016.
3. Чичварин Н.В. Экспертные компоненты САПР. – М.:Машиностроение, 1991. – 240 с.:ил.
4. Чичварин Н.В. Стеганографический метод маскирования данных с использованием цифровых голограмм. // ВНТК «Безопасные информационные технологии»: сборник тез. Докл. ВНТК (вып. 2), 2011. – с.11.
5. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Информационные технологии. Приложение. 2012, №5. С.1- 32.
6. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Защита проектной документации от несанкционированного доступа // 9 Международная конференция «Эффективные методы автоматизации подготовки и планирования производства»: труды. (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С.141-144.
7. Глинская Е.В., Чичварин Н.В. Информационная безопасность открытых каналов передачи проектной документации, производимой в САПР // Вопросы кибербезопасности. 2014. № 4 (7). С. 11-22.

A Method for Protecting an Information Subsystem of CAD System from Unauthorized Access Volosatova T. M.⁸⁷

Abstract. *This paper discusses the issues in information security of CAD systems. It proposes a method for concealing a data that constitutes a commercial secret in the information subsystem of CAD system. This method is based on the organization of a database which in turn is virtually a holographic storage device. One of the advantages of this technical proposal is the fact that it's implementation does not require reorganization of relational databases that form an essential part of every modern CAD system.*

Key words: *security, holography, protection, information, design object, design documentation.*

⁸⁷ Volosatova T. Ph. D., Associate Professor. Bauman MSTU, Moscow

О методах введения идентификаторов и перемешивания для обезличивания (анонимизации) персональных данных

Варфоломеев А.А.⁸⁸

Аннотация

Рассмотрены два метода (метод введения идентификаторов и метод перемешивания) для обезличивания персональных данных, рекомендованных Роскомнадзором России в Приказе от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных", с точки зрения криптографии. Отмечается, что, рекомендуя применение указанных методов, Роскомнадзор не выдвинул требования к качеству этих методов для защиты ПДн. Показано, что эти требования могут быть сформулированы в терминах стойкости шифров. В связи с этим могут быть подвергнуты критике некоторые реализации этих методов, встречающиеся в литературе.

Ключевые слова: стойкость, криптография, шифр перестановки, шифр замены, деобезличивание, атрибуты персональных данных.

Введение

Важными методами защиты персональных данных (ПДн) являются методы их обезличивания [1 - 3]. Применение данных методов позволяет оператору ПДн добиться ряду преимуществ [4]. Но не ясно, достаточно ли самого факта применения рекомендуемых способов обезличивания для защиты ПДн, представленных в обезличенной форме.

Методы обезличивания с точки зрения криптографии.

В документах Роскомнадзора [1-2] приводятся следующие методы обезличивания:

метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим отдельным хранением подмножеств);

метод перемешивания (перестановка отдельных записей, а так же групп записей в массиве персональных данных).

Подобные же методы предлагаются зарубежными рекомендациями [5].

Не все методы обладают свойством обратимости (то есть возможности деобезличивания). Например, этим не обладает второй из указанных методов. Метод декомпозиции требует особого рассмотрения. Остановимся на оставшихся двух.

Из описания этих методов, а также примеров их применения в [2], следует, что эти методы фактически осуществляют преобразования шифрования как в шифрах замены (метод введения идентификаторов) и в шифрах перестановки (метод перемешивания). Как известно, самого факта применения шифра недостаточно для защиты данных. Шифр должен быть стойким к атакам злоумышленника. Таким образом, для методов обезличивания ПДн можно ввести понятие стойкости через понятие стойкости шифров. Например, следуя К. Шеннону, через равенство энтропий:

$$H(\text{ПДн}) = H(\text{ПДн}/\text{ОПДн}),$$

⁸⁸ Варфоломеев Александр Алексеевич, канд. физ.-мат. н, доцент, МГТУ им. Н.Э. Баумана, a.varfolomeev@mail.ru

где слева стоит энтропия ПДн, а справа условная (средняя) энтропия ПДн при условии известных злоумышленнику обезличенных ПДн.

В связи с этим имеет смысл не придумывать какие-нибудь новые реализации методов обезличивания [6], а использовать известные проверенные методы шифрования.

Вывод.

Необходимо в нормативных документах по обработке и защите ПДн сформулировать требования к качеству методов обезличивания. Это можно сделать в терминах криптографии.

Лучшим методом обезличивания ПДн, с точки зрения невозможности их восстановления злоумышленником, является стойкое шифрование атрибутов ПДн.

Литература

1. Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных".
2. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных" (утв. Роскомнадзором 13.12.2013).
3. Шередин Р.В. Обезличивание персональных данных как универсальный способ защиты прав субъектов персональных данных: основные требования и методы. Докл. На Междунар конф. «Защита персональных данных».
4. Постановление Правительства РФ от 21.03.2012 № 211 (ред. От 06.09.2014) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".
5. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), 2010. 59 с.
6. Карпова И.П. О реализации метода обезличивания персональных данных. «Вестник компьютерных и информационных технологий» № 6, 2013.

About The Methods of Introducing IDS and Mixing for Depersonalization (Anonymization) of Personal Data

Varfolomeev A. ⁸⁹

We consider two methods (method of introducing IDs and mixing method) for the depersonalization of personal data, the recommended by Roscomnadzor (Russia) in the Order of 05.09.2013 N 996 in terms of cryptography. It is noted that by recommending the use of these methods, Roscomnadzor did not put forward demands on the quality of these methods to protect the personal data. It is shown that these requirements can be formulated in terms of security of ciphers. In this regard, it can be criticized some implementations of the methods found in the literature.

Keywords: security, cryptography, transposition cipher, substitution cipher, depersonalization, personal data attributes.

⁸⁹ Varfolomeev A.A. Ph.D. Bauman MSTU.

**Разработка защищенного протокола обмена информацией о целевых
компьютерных атаках на кредитно-финансовые организации**
Волкович Е.К.⁹⁰

Аннотация. Доход хакеров от целевых атак на кредитно-финансовые организации зачастую перекрывает суммарный заработок от остальных способов хищений, делая их самой привлекательной мишенью для атак. В связи с этим, в 2015 году на базе ГУБиЗИ Банка России было создано специализированное подразделение – Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT). Для выполнения возложенных задач, FinCERT осуществляет на постоянной основе информационный обмен индикаторами компрометации компьютерных систем (IOC, Indicators of Compromise) с кредитно-финансовыми организациями. На сегодняшний день, обмен IOC осуществляется по электронной почте, что создает сложность передачи и использования этих данных в автоматизированных аналитических системах кредитно-финансовых организаций. Следовательно, необходимо создать унифицированный протокол обмена информацией и определить формат информационного сообщения.

Ключевые слова: индикаторы компрометации, IOC, стандартизация информационного обмена, FinCERT Банка России, системы класса SIEM

Введение

13 октября 2016 года прошла ежегодная конференция Group IB «Тенденции развития преступлений в области высоких технологий», где собрались представители МВД России, ФСБ России, Европола, крупнейших банков, IT-компаний, чтобы поделиться актуальными проблемами в области кибербезопасности. Подтверждением прогнозов прошлого года стал прирост количества и средний ущерб от целевых атак на кредитно-финансовые организации, который составил 2,5 млрд. руб. По прогнозам Group-IB, данная тенденция сохранится в 2017 году, целевые атаки продолжают победное шествие по миру, при этом, делая ставку на автоматизацию хищений [1].

Организация информационного обмена

1 июня 2015 года начал работу Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России (FinCERT). Цель создания FinCERT – информационное взаимодействие Банка России, кредитных и некредитных финансовых организаций, компаний-интеграторов, разработчиков антивирусного программного обеспечения, провайдеров и операторов связи, правоохранительных и иных государственных органов, направленное на координацию работ по противодействию несанкционированного доступа к IT-инфраструктуре кредитно-финансовых организаций с целью хищения денежных средств [2].

Для достижения поставленной цели, FinCERT осуществляет обмен информацией о фактах целевых компьютерных атак, анализирует полученную информацию и на основе анализа готовит рекомендации пострадавшей стороне, а также рассылает индикаторы компрометации остальным организациям, присоединившимся к системе информационного обмена.

Согласно отчету за период с июня 2015 по май 2016 года FinCERT зафиксировал 21 атаку на инфраструктуру кредитно-финансовых организаций на общую сумму порядка 2,87 млрд рублей, при этом предотвращено хищение порядка 1,6 млрд. руб [4].

⁹⁰ Волкович Екатерина Константиновна, МГТУ им. Н.Э. Баумана, г. Москва, katvollkovich@mail.ru

Формат сообщений информационного обмена

На сегодняшний день, информационный обмен с FinCERT осуществляется посредством передачи сообщений с использованием электронной почты. «Временный регламент передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (версия 1.0)» [5] определяет формат предоставления различного типа информации участником информационного взаимодействия. Например, индикаторы компрометации должны быть представлены в форматах Yara, Open Indicators of Compromise (IOC), eXtensible Markup Language (XML) или др.

Формат уведомлений от FinCERT в рамках информационного обмена представлен на рисунке ниже (рис. 1). Для использования информации из уведомлений, аналитики кредитно-финансовых организаций должны преобразовать ее в правила выявления сценариев реализации угроз в системах информационной безопасности (ИБ), основным компонентом которых зачастую является система класса Security Information and Event Management (SIEM). Для преобразования информации необходимо определенное время, что очевидно увеличивает время обнаружения и реакции на инцидент ИБ.

ИР-20160122-003		Уязвимость повышения привилегий в ядре Linux	
Описание уязвимости		Позволяет локальному пользователю получить административный доступ и скомпрометировать систему. Эксплуатация ошибки позволяет атакующему удалять файлы, просматривать конфиденциальную информацию, устанавливать нежелательные программы и пр.	
Операционная система / аппаратная платформа		ОС Linux, ОС Android	
Версия		версии ядра Linux от 3.8	
Дата выявления / публикации		19.01.2016	
Возможные меры по устранению уязвимости		На Linux-серверах эксплойт могут предотвратить такие средства защиты, как SMEP (Supervisor Mode Execution Protection) и SMAP (Supervisor Mode Access Protection), на Android-устройствах такую же функцию выполняет SELinux.	
Статус уязвимости		Подтверждена Perception Point	
Наличие эксплойта		Есть	
Информация об устранении		Уязвимость устраняется	
Ссылки на источники		https://threatpost.ru/serious-linux-kernel-vulnerability-patched/14275/	
Идентификаторы других систем описания уязвимостей		CVE-2016-0728	
Прочая информация		Отсутствует	

Рис.1. Формат уведомлений в рамках информационного обмена

Создание унифицированного протокола обмена

На рынке представлено множество систем класса SIEM различных производителей, при этом они имеют различные формы представления журналов и нормализации событий. Наиболее общими форматами представления данных, которые могут безболезненно принять любые системы класса SIEM, являются XML и JavaScript Object Notation (JSON). Таким образом, необходимо взвесить все за и против, и выбрать единый формат единичного сообщения, которое можно будет импортировать в систему класса SIEM. Далее необходимо создать парсер, который будет разбирать установленный формат сообщения в системе класса SIEM конкретной кредитно-финансовой организации.

Также необходимо определить перечень информации, которой могут обмениваться кредитно-финансовые организации в рамках законодательства Российской Федерации. Эта информация определит наиболее значимые поля в протоколе обмена, которые необходимы системам класса SIEM для выявления инцидентов ИБ (например, вредоносный IP-адрес, хеш, имя файла). Наиболее перспективными форматами описания индикаторов

компрометации являются Structured Threat Information Expression (STIX) и Open IOC, которые и будут проанализированы при создании защищенного протокола обмена.

Вывод

Наличие унифицированного протокола обмена информацией позволит достичь высокой оперативности в выявлении и реагировании на инциденты ИБ в кредитно-финансовых организациях в целях предотвращения целевых компьютерных атак. Практическая реализация данного протокола обмена будет представлена в выпускной квалификационной работе.

Литература

1. Group-IB. Отчет о тенденциях высокотехнологичных преступлений за Q2 2015 – Q1 2016. Hi-Tech Crime Trends 2016. URL: <http://www.group-ib.ru/2016-report.html> (дата обращения: 27.10.2016)
2. «ФинЦЕРТ» Банка России. URL:
3. http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=fincert (дата обращения: 27.10.2016)
4. Банк России. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 01 июня 2015 г. по 31 мая 2016 г. 2016. URL: http://www.cbr.ru/credit/Gubzi_docs/fincert_survey.pdf (дата обращения: 28.10.2016)
5. Банк России. Временный регламент передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (версия 1.0). 2016. URL: http://www.cbr.ru/credit/Gubzi_docs/infoaregl_10.pdf (дата обращения: 28.10.2016)
6. Фролов Д.Б. FinCERT: Основные задачи и направления развития // Банковское дело. 2016. №2. С. 74-76.

Научный руководитель: Фролов Дмитрий Борисович, доктор политических наук, кандидат юридических наук, начальник Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере ГУБиЗИ Банка России, Центральный Банк Российской Федерации, fdb@cbr.ru

The Development of a Secure Protocol for the Information Exchange about the Targeted Computer Attacks on Financial Organizations Volkovich E.K.⁹¹

Abstract. The income obtained by the hackers through the implementation of targeted attacks to financial organizations covers the total income from other methods of attacks. It makes hackers consider financial organizations to be the most attractive target for attacks. In this regard, Centre for monitoring and responding to computer attacks in the credit and financial sphere (FinCERT) was founded based on the General Directorate for Security and Information Protection of the Bank of Russia. It is a specialized department to prevent attacks in the financial system of the Russian Federation. To perform assigned tasks FinCERT carries out the information exchange with indicators of compromise of computer systems (IOC, Indicators of Compromise) on a regular basis with financial organizations. Today, the exchange of indicators of compromise is done by email. It creates the complexity to transfer and use of these data in analytical systems of financial organizations. Therefore, it is necessary to create a unified protocol for the information exchange and determine the format of the informational message.

Keywords: indicators of compromise, IOC, standardization of the information exchange, FinCERT of the Bank of Russia, SIEM systems

⁹¹ Ekaterina Volkovich, Bauman Moscow State Technical University, Moscow, katvolkovich@mail.ru

Анализ защищенности бортовых вычислительных средств**Воронина П. А., Козарь А. А.⁹²**

В статье рассмотрены вопросы информационной безопасности БВС. Описывается структура системы управления ЛА. Поднимается тема вредоносных воздействий на БВС, приводятся средства борьбы с ними. Проводится анализ ЭВМ серий «Аргон» и «Багет» в качестве прототипов БВС. Одним из достоинств проведенного анализа является то, что его результаты имеют практическую ценность для дальнейших разработок.

Ключевые слова: бортовые вычислительные средства, безопасность, система автоматического управления, ЭВМ «Аргон», ЭВМ «Багет».

Введение

В настоящее время системы автоматизированного управления находят все большее применение в различных областях специального назначения, в частности, в сфере обеспечения автоматизации информационных и управляющих процессов на борту объекта в режиме реального времени. Совокупность подобных аппаратно-программных средств называется бортовыми вычислительными средствами (БВС). Одной из основных проблем при проектировании бортовых вычислительных средств является защита от несанкционированных воздействий. Таким образом, вопрос решения задачи обеспечения требуемого уровня защищенности БВС является, на данный момент, крайне актуальным.

1. Структура систем управления ЛА

Чаще всего бортовые вычислительные средства размещаются на различных летательных аппаратах (ЛА), в том числе космических кораблях, самолётах, вертолётах и беспилотных ЛА специального назначения. Для анализа решения задачи обеспечения защиты систем управления ЛА рассмотрим общую структуру системы управления (рис.1) [1].



Рис. 1. Структура системы управления ЛА

Система управления характеризуется требуемым и фактическим, то есть реальным состоянием объекта управления. Внешние воздействия на систему учитываются с помощью введения таких параметров, как возмущение объекта управления и шумов измерений.

2. Виды воздействий на бортовые вычислительные средства

При обработке поступающих сигналов системой управления существует риск возникновения помех различного характера.

⁹² Воронина Полина Александровна, МГТУ им. Н.Э. Баумана, г.Москва, voronina.p.a@yandex.ru
Козарь Анастасия Андреевна, МГТУ им. Н.Э. Баумана, г.Москва, kozar.a.a.rk6@yandex.ru

Можно выделить следующие воздействия на систему управления: случайные воздействия, такие как погодные условия, сбои аппаратного оборудования, наличие шумов в канале связи и пр., и преднамеренные, включающие в себя различные несанкционированные воздействия с целью нарушения работоспособности ЛА или искажения информации.

Описанные воздействия могут приводить к нарушениям доступности, целостности и конфиденциальности. Для решения проблем нарушения доступности и конфиденциальности необходимо построение систем защиты информации. Нарушения целостности можно избежать, обеспечив сохранность информации путем восстановительного резервирования.

3. БВС Аргон

В 1964 г. в НИЭМ впервые в СССР были развернуты работы по проектированию, производству и внедрению в системы бортовых ЭВМ (БЭВМ), получивших название "Аргон". К подобным ЭВМ, используемым в составе систем управления летательных аппаратов, предъявляется ряд специфических требований, которые значительно усложняют проектирование бортовых машин [2]. К числу важнейших требований, помимо ограничений на массо-габаритные характеристики и потребляемую мощность, относят также необходимость придания повышенной надежности функционирования, устойчивости к широкому диапазону внешних воздействий (механических, климатических, радиационных и др.).

При проектировании ЭВМ "Аргон" учитывались все возможные виды помех и применялись различные способы борьбы с ними. Однако отдельно стоит отметить методику борьбы с нарушением целостности информации.

Впервые в практике была применена схема резервирования узлов, называемая троированной структурой с мажоритированием [3]. "Аргон" представлял собой систему из трех параллельно работающих функциональных блоков. При этом на вход каждого блока от датчиков телеметрии подавалась одинаковая информация. На основе этой информации каждый блок независимо от других вырабатывал более сорока управляющих воздействий. Для формирования конечных управляющих воздействий использовался мажоритарный принцип, то есть за основу бралось значение, полученное на большинстве выходов. Входные и выходные каналы имели связи для обмена информацией в случае, если она искажалась в одном или нескольких блоках.

БВС в настоящее время применяются в составе навигационных и навигационно-пилотажных комплексов, прицельно-навигационных комплексов, бортовых систем связи, в системе дальнего радиолокационного обнаружения и др. Например, 16-разрядные БВС, разработанные НИИ «Аргон» обеспечивают выполнение широкого спектра задач по обработке информации на борту самолётов типа МиГ-29 и Су-27, в том числе управление системой вооружения и РЛС в реальном масштабе времени.

4. БВС Багет

БВС "Аргон" имели уникальную методику борьбы с нарушением целостности информации. БВС "Багет" создавались для работы в суровых условиях окружающей среды, а также превосходят обычные ЭВМ по надёжности и обеспечивают обработку конфиденциальной информации [4]. Это обеспечивается низкими уровнями электромагнитных излучений в окружающее пространство. Помимо этого, они аттестованы на соответствие требованиям нормативных документов и имеют возможность создавать защищенные локальные вычислительные сети [5]. Для подавления излучений в окружающее пространство зоны стыков панелей корпуса и планки модулей оборудованы

радиоуплотнителями. Разъёмы модулей и кабелей устройств оборудованы кабелями-поглотителями.

Большой популярностью на сегодняшний день пользуется электронно-вычислительная машина ЭВМ «Багет», предназначенная для организации взаимодействия подсистем комплекса бортового радиоэлектронного и сопрягаемого оборудования, комплексной обработки информации, решения задач навигации и управления, а также специальных задач. Используется топология — «каждый с каждым». Характеризуется большим сроком службы, небольшой массой и энергопотреблением, а также способен работать в суровых условиях.

Заключение

Случайные и преднамеренные воздействия на бортовые вычислительные средства влекут за собой нарушения доступности и целостности информации, а также нарушение конфиденциальности.

Проанализированные БВС "Аргон" и "Багет" справляются данными нарушениями. Примерами методик борьбы с нарушениями служит резервирование и снижение уровня электромагнитных излучений в окружающее пространство.

БВС "Аргон" и "Багет" имеют каждый свои собственные методы защиты от воздействий и успешно используются в реальных условиях, однако, с развитием IT технологий и приборостроения постоянно возникают новые способы взаимодействий и методы защиты, что заставляет искать новые способы анализа защищенности.

Обеспечение защищенности БВС ЛА является серьезной проблемой на сегодняшний день, в связи с этим данный анализ актуален для дальнейших разработок.

Литература

1. Басалов Ф.А., Старожук Е.А., Мамон Ю.И. Анализ защищенности бортовых информационных систем летательных аппаратов // Известия ТулГУ. Технические науки. 2015, №9. С. 58-65.
2. Моисеев В.С., Козар А.Н., Дятчин В.В. Информационная безопасность автоматизированных систем специального назначения: Монография. Казанское высшее артиллерийское командное училище (военный институт) имени маршала артиллерии М.Н. Чистякова, 2006. 384 С.
3. Официальный сайт НИИ «Аргон»: www.argon.ru: Технология построения открытых, модульных вычислительных средств. Последний доступ: 30.10.2016.
4. Багет. Семейство ЭВМ для специальных применений. Каталог. Издание 3-е. – М.: КБ «Корунд», 2004.
5. Захарова О.Л., Кирсанова Ю.А., Книга Е.В., Жаринов И.О. Алгоритмы и программные средства тестирования бортовых цифровых вычислительных систем интегрированной модульной авионики // Информационно-управляющие системы 2014, №3. С.19- 29.

Научный руководитель: Волосатова Тамара Михайловна, канд. техн. наук, доцент, МГТУ им. Н.Э. Баумана, г.Москва, [tamaravol@gmail.com](mailto:تامارавол@gmail.com)

The Security Analysis of On-Board Computing Facilities

Voronina. P.A., Kozar. A.A.

Abstract. The article examines the issues of On-board Computing Facilities information security system of the aircraft. Raised the topic of the harmful impacts on OCF and the means of combating them. Performed the analysis of a computer series called "Argon" and "Baget" as OCF prototype. One of the advantages of the analysis is that its results are of practical value for future developments.

Keywords: on-Board computing facilities, security, automatic control system, the computer "Argon", the computer "Baget".

Разработка способа управления доставкой сетевых пакетовГасанов Э.О., Медведев Н.В.⁹³

Аннотация: Разработан способ управления доставкой сетевых пакетов, при котором получатель будет контролировать информационный поток данных и регулировать скорость передачи данных в зависимости от загрузки сети по протоколу TCP. Данный способ может повысить эффективность информационных процессов, особенно в беспроводных системах и сетях связей.

Ключевые слова: окно получателя, управление перегрузкой, протокол

Введение

Основные протоколы транспортного уровня, такие как TCP, осуществляют управление перегрузкой на стороне отправителя. Скорость передачи данных по сети в этом случае будет зависеть от алгоритма управления перегрузкой (окна перегрузки, CWND), за исключением такого варианта, при котором получатель не в состоянии принять и осуществить сборку последовательности пакетов с той же скоростью, с которой её формирует отправитель (определяется окном получателя, RWIN). При этом размер скользящего окна $windows = \min(CWND, RWIN)$ будет определять скорость передачи данных от отправителя к получателю.

Для наиболее эффективного использования пропускной способности каналов передачи данных значение окна получателя $RWIN \geq RTT \cdot B$, где B – пропускная способность канала в бит/сек, RTT – время передачи сегмента данных до получателя и обратно. Однако эта величина не участвует в алгоритме управления перегрузки, так как последний основан на детектировании потерь пакетов в сети (модели Tahoe, Reno, NewReno и другие), оценки величины RTT (Vegas) или оценки скорости потока данных по получаемым ACK-пакетам (Westwood) [1, с.21-24]. В данной работе будет предложен способ управления доставкой сетевых пакетов, при котором значение окна получателя будет оказывать влияние на работу алгоритма управления перегрузкой, не давая последнему перегрузить сеть и существенно снизить скорость передачи данных.

Варианты управления окном получателя

Существует четыре варианта управления окном получателя. В первом случае используются значения окна получателя по умолчанию для каждого из сетевых интерфейсов. Эти значения пользователь может изменить либо в реестре (операционная система Windows) либо в системных настройках через утилиту sysctl в операционных системах семейства Unix.

Во втором варианте протокол прикладного уровня или приложение пользователя могут самостоятельно задавать для каждого соединения индивидуальный размер окна получателя, которое определяется размером буфера памяти, выделенного для данного соединения. Размер окна получателя может быть найден путем передачи нескольких сетевых пакетов (UDP-echo или ICMP) отправителю, прием которых получателем позволит вычислить значения B и RTT .

Третий вариант управления окном получателя отличается от второго тем, что выбор значения окна происходит на транспортном уровне автоматически и не требует от прикладного уровня никаких специальных действий. Такая технология получила название автоподстройки окна получателя [2]. Однако у данного варианта существует ряд проблем:

⁹³ Медведев Николай Викторович – МГТУ им. Баумана, кандидат технических наук, n.medvedev@bmstu.net
Гасанов Эмиль Октаевич – МГТУ им. Баумана, gasanoveo@gmail.com

- Невозможно адаптировать данный вариант управления окном к случаям, связанным с возникновением перегрузок в сетях или улучшением качества связи;

- При передаче мультимедийных данных размер окна получателя должен подстраиваться под скорость потока с данными, а не под характеристики соединения В и RTT. Из-за этого размер буфера, выделенный под эти данные, будет намного превосходить необходимый.

И, наконец, четвертый вариант состоит в том, что окно получателя меняется динамически в зависимости от окна отправителя, превосходя последнее на некоторую величину. Таким образом, пропускная способность ограничена доступной пропускной способностью сети, а не некоторым произвольно установленным постоянным значением на получателе. Примерами технологий, которые реализуют указанный принцип, являются «Dynamic Right-Sizing» [3] в операционных системах семейства Linux и «Receive window size tuning» в операционных системах семейства Windows, начиная с WindowsVista [4].

Последний вариант наиболее интересен по двум причинам. Подстройка окна получателя под окно перегрузок позволяет экономить оперативную память, что является немаловажным для мобильных пользователей и короткоживущих соединений. Вторая причина связана с реализацией атак класса hijacking типа «угадывание идентификатора», для защиты от которой необходимо минимизировать окно получателя. В работе [5] было доказано, что достижение оптимального режима функционирования TCP-соединения с учетом баланса между производительностью и безопасностью требует приближения значения RWIN к характеристикам канала В и RTT и обязано учитывать рост величины CWND на отправителе для подстройки окна получателя.

Однако данный вариант не лишен и серьезного недостатка. При росте интенсивности потока сетевых пакетов будет расти величина RTT из-за увеличения времени обслуживания пакетов маршрутизаторами и коммутаторами. Следствием этого является увеличение окна получателя, что в итоге может привести к возникновению перегрузок в сети и потерям пакетов, и существенно снизит скорость передачи данных. Для борьбы с перегрузками в этом случае следует использовать возможность управления скользящим окном путем манипуляций с окном получателя, так как отправитель при передаче данных выбирает наименьшую из двух величин: CWND или RWIN.

Способ управления скользящим окном путем определения загруженности сети на получателе

Рассмотрим типовой вариант компьютерной сети организации (рис. 1). Сеть состоит из нескольких компьютеров и серверов, соединенных между собою маршрутизаторами. Наибольшая нагрузка приходится на маршрутизатор 3, так как он соединяет пользовательские сегменты сети с серверным, а также предоставляет доступ к сети Интернет. Указанный маршрутизатор в нашей сети является узким местом и будет ограничивать скорость передачи данных по сети.

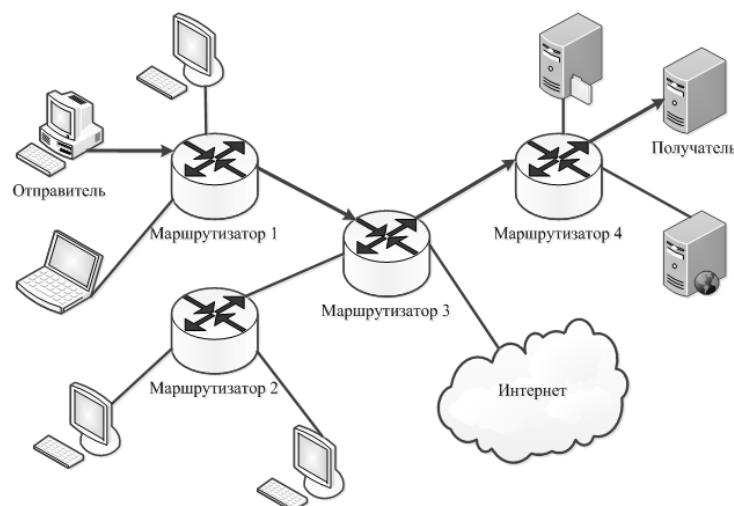


Рис. 1. Структурная схема компьютерной сети организации.

При передачи данных между отправителем и получателем данный маршрутизатор снизит скорость между нашими абонентами. Однако появление нового абонента или установление ещё одного соединения приведет к перегрузке данного узла сети и резкому возрастанию потерь пакетов, так как маршрутизатор 3 будет вынужден сократить длину очереди, используя такие алгоритмы, как RED [6], Tail Drop [7] и другие.

Метод, позволяющий определить пропускную способность канала, проходящего через маршрутизатор 3 между отправителем и получателем, показан на рис. 2. Узкое место приводит к тому, что время передачи пакета Δt увеличивается. Получатель может оценить пропускную способность канала, вычислив время Δt и определив размер пакета MTU [8].

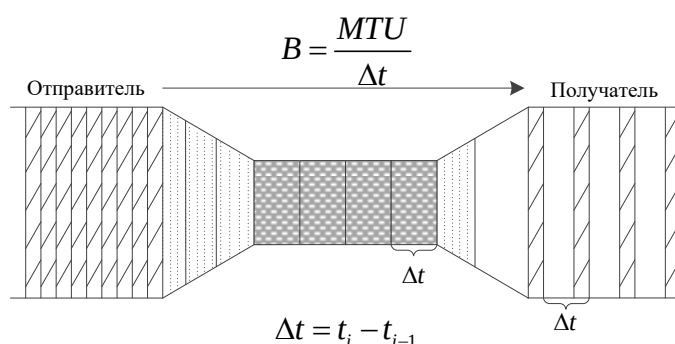


Рис. 2. Метод оценки пропускной способности канала.

Оценив пропускную способность канала и время передачи пакета от отправителя к получателю, приемная сторона выбирает такой размер окна $RWIN$, который будет на некоторую величину δ меньше, чем полученная оценка. Тем самым мы переместим узкое место к получателю и решим проблему перегруженности маршрутизатора 3.

Предложенный способ управления скользящим окном состоит из:

1. Определения пропускной способности сети по результатам мониторинга за интенсивностью поступления пакетов на получателе.
2. Корректировки окна получателя в том случае, если оно превышает необходимый для эффективной работы размер, до величины, которая на δ меньше, чем

полученная оценка пропускной способности сети, то есть

$$RWIN = \min(RWIN_{sys}, \frac{MTU \cdot RTT}{\Delta t} - \delta), (1)$$

где $RWIN_{sys}$ - размер окна получателя, определенный операционной системой.

3. Прогнозирования изменения интенсивности потока данных в сети с соответствующей коррекцией скользящего окна.

При этом стоит отметить ряд проблем, которые могут усложнить внедрение данного способа управления.

1. Необходимо выполнение предложенной процедуры управления скользящим окном на всех компьютерах нашей сети, так как те получатели, которые не модифицируют принцип определения окна получателя и не ограничат скорость передачи данных от отправителя через узкое место, будут вызывать перегрузку сети.
2. Помимо трафика, управляемого алгоритмами перегрузки, в сети существуют потоки данных, для которых управление перегрузкой нецелесообразно (речевая, мультимедийная информация) или невозможно (IPSec-туннели, служебный трафик (ICMP, UDP)).
3. Злоумышленник может использовать особенности предложенного способа управления скользящим окном для реализации атаки, снижающей скорость передачи данных.

Преодоление указанных проблем возможно в том случае, если маршрутизаторы и коммутаторы используют алгоритм «справедливая очередь», при котором они организуют независимые очереди для пакетов, поступающих от разных источников. Когда выходной канал маршрутизатора оказывается свободным, он просматривает очереди циклически и отправляет очередной пакет. В результате при n очередях по завершению такого цикла просмотров-посылок будет послано по одному пакету из каждой очереди [9].

Заключение

Предложенный в данной статье способ управления доставкой сетевых пакетов обладает целым рядом преимуществ. Первое преимущество состоит в том, что получатель может более точно оценить нагрузку сети и подобрать подходящий размер скользящего окна. Более точная оценка особенно актуальна для беспроводных систем и сетей связи, так как каналы от абонента и к абоненту могут сильно отличаться по пропускной способности, количеству искаженных пакетов, различиям в маршрутах доставки.

Во-вторых, данный способ может быть применен к существующим системам информационного взаимодействия, использующим протоколы TCP, DCCP и SCTP, без их специальной доработки. С позиции оптимизации протоколов информационного взаимодействия, данный способ следует отнести к параметрической оптимизации протокола путем динамического изменения окна получателя [10]. Это позволяет сохранить совместимость с ранними версиями протоколов и не нарушить функционирование телекоммуникационной системы, так как в указанном способе модифицируются только те поля, которые уже предусмотрены существующими стандартами. При этом данный способ не противоречит требованиям стандартов.

И наконец, незначительное уменьшение окна получателя на величину δ повышает защищенность протокольных процедур от атак класса hijacking. Исходя из указанных достоинств данного способа дальнейшие шаги по его совершенствованию и развитию должны быть направлены на:

- Выбор эффективного метода оценки загруженности сети для определения подходящего размера окна получателя. Один из методов оценки пропускной

способности канала был рассмотрен в нашей статье. Но существуют ряд дополнительных мер, позволяющих уточнять состояние маршрутизатора и линий связи в процессе передачи данных от отправителя к получателю. Кроме этого, необходимо с высокой точностью оценить величину RTT для выбора адекватного скользящего окна. Указанные параметры должны оцениваться на всем интервале времени процесса передачи данных.

- Разработку специализированных программных модулей, имитирующих процесс передачи данных по сети в зависимости от её загруженности, и позволяющих провести верификацию предложенного способа.
- Исследование влияния размера окна получателя на перегруженность сети и определение оптимального окна получателя для максимизации скорости передачи данных с учетом оценки загруженности сети. Главной целью данного исследования является выбор подходящего значения параметра δ , на которое надо уменьшить окно получателя, для каждого соединения.
- Выбор алгоритма прогнозирования загруженности сети с целью своевременного реагирования на меняющиеся условия среды передачи данных. Прогнозирование загруженности сети необходимо для быстрого и адекватного реагирования отправителем на потенциальное изменение пропускной способности каналов передачи данных, задержек, потерь пакетов и других параметров на стороне получателя. Для этой цели необходимо выявить и классифицировать признаки изменения перечисленных параметров телекоммуникационной системы, а также выбрать подходящую модель прогнозирования (регрессионную, марковскую или иную).
- Оценку эффективности метода управления доставкой информационных сообщений, заключающегося в определении загруженности сети на стороне получателя и минимизирующего повторную отправку данных. По результатам оценки будут выбраны такие конфигурации сетей, в которых данный метод может найти применение.

Литература

1. Мазепа Р.Б., Михайлов В.Ю., Большов О.А., Карпухин Е.О., Корнилов А.М. Методы обеспечения безопасности информационных процессов. М.: МАИ-ПРИНТ, 2012.
2. E. Weigle, W. Feng. A Comparison of TCP Automatic Tuning Techniques for Distributed Computing //in Proc. HPDC, 2002, pp.265-265.
3. M. Fisk, W. Feng. Dynamic Right-Sizing in TCP // Los Alamos Computer Science Institute Symposium, Oct. 2001.
4. Дэвис Д. Автоматическая настройка окна приема TCP. [Электронный ресурс]. URL: <http://technet.microsoft.com/ru-ru/magazine/2007.01.cableguy.aspx> (дата обращения: 12.11.2013).
5. Карпухин Е.О. Выбор оптимального размера окна получателя в телекоммуникационных системах, использующих протокол TCP // Известия института инженерной физики. – 2011. – №4. – С.25-27.
6. Floyd S., Jacobson V. Random Early Detection gateways for Congestion Avoidance // V.1 N.4, August 1993, p. 397-413.
7. G. Hasegawa, K. Tokuda, M. Murata. Analysis and Improvement of fairness among many TCP connections sharing Tail-Drop and RED Routers. [Электронный ресурс]. URL: <http://www.anarg.jp/achievements/web2002/pdf/proceedings/Hasegawa02INET-REDanalysis.pdf>. (дата обращения: 12.11.2013).
8. R.Carter, M.Crovella. Measuring bottleneck link speed in packet-switched networks // Tech. Rep. 1996-006, Boston University Computer Science Department, Boston, MA, USA, Mar.1996
9. Ю. Семенов. Алгоритмы телекоммуникационных сетей. В 3 частях. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных // Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2007.

Development Method for Controlling the Delivery of Network Packets

Gasanov. E.O., Medvedev N.V.⁹⁴

Abstract. The method for controlling the delivery of network packets has been developed. This method let the recipient control an information flow of data and regulate the speed of data transfer which depends on the net workload under the TCP protocol. This method can improve the efficiency of the information processes, especially in the wireless systems and communication nets.

Keywords: Receive window, congestion control, Protocol

УДК 51.74

О сохранении целостности информации в сетях с быстроменяющейся структурой Гордеев Э.Н.⁹⁵

Рассматривается сеть, узлы которой одновременно представляют источники информации, потребителей информации и структурные сетевые элементы, например, маршрутизаторы разных уровней. Сеть должна функционировать в течении ограниченного периода времени, доставляя сообщения источникам потребителям. В течении этого периода происходит исчезновение (разрушение) узлов и ребер сети, а также допускается появление новых узлов и ребер. В условиях обычной для публичных сетей доменной иерархии это весьма затруднительно. Описывается подход на основе, так называемой, «иерархии ориентиров» (Landmark hierarchy) и исследовании устойчивости решений в задачах дискретной оптимизации. Приведена схема эвристического алгоритма, параметры которого могут адаптивно настраиваться на различные сценарии разрушения сети. Результаты могут использоваться при построении специальных сетей: игры, спорт и т.д.

Ключевые слова: маршрутизация в сетях, Landmark hierarchy, устойчивость решений в задаче о кратчайшем пути.

Введение

Основным объектом модели является взвешенный ориентированный граф $G=(V,E)$ с множеством вершин V , $|V|=n$ и множеством ребер E , $|E|=m$. При этом ребрам и вершинам приписывает несколько различных типов весов.

Само множество вершин тоже может делиться на несколько типов. Например, можно считать, что любая вершина выполняет функцию источника информации, потребителя информации и маршрутизатора, а можно разграничить вершины по функциям.

⁹⁴ Medvedev Nikolay Viktorovich, Associate Professor, Candidate of Engineering Sciences, Bauman Moscow State Technical University, n.medvedev@bmstu.net; Gasanov Emil Oktaevich, Bauman Moscow State Technical University, gasanoveo@gmail.com

⁹⁵ Гордеев Эдуард Николаевич, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, tatamigor@gmail.com

В работе [1] описана система адресации на базе так называемой *Landmark hierarchy*. На ее основе можно построить адаптивную адресную систему в сети с изменяющейся структурой. Алгоритмы маршрутизации теперь будут использовать эту адресную систему. (Хотя при этом обеспечивается их максимально возможное сходство с традиционными алгоритмами маршрутизации). При этом за счет многочисленных эвристических параметризованных процедур эти алгоритмы допускают значительно большую гибкость для сохранения работоспособности сети при условии дискретности событий, приводящих к ее изменению. Такими событиями являются: уничтожение вершины, возникновение вершины, уничтожение ребра, возникновение ребра. Однако основной упор сделан на ситуацию быстро и непредсказуемо растущей сети.

Мы же применили этот метод для случая быстро меняющейся (и не обязательно растущей) сети. Но в этом случае возникает ситуация скачкообразного изменения пропускной способности существующих ребер. Поэтому мы используем гибридный алгоритм, включающий в себя проверку устойчивости решения задачи о кратчайшем пути (именно распределенный алгоритм Дейкстры для решения этой задачи наиболее распространен в алгоритмах маршрутизации). Эта проблема подробно рассмотрена в работе [2-4]. В [5] даны примеры применения теории устойчивости в задачах сохранения целостности информации.

Исключительно в качестве иллюстрации рассмотрим наглядный пример.

Пусть дан граф $G=(V_0, V_1, \dots, V_L; E \cup E')$ с двумя типами ребер. Если множество вершин – корневое L – ярусное дерево, то первый тип – это ребра между ярусами. Ребра второго типа – это ребра, образующие на каждом ярусе свой (возможно, полный) граф.

Стоимость передачи единицы информации по ребру первого типа равна w . Стоимость передачи единицы информации по ребру второго типа равна $k^s w$, где s – расстояние до ближайшего предка вершин, связанных этим ребром ($k > 1$).

Необходимо донести единицу информации от корня до всех листьев. Это будет стоить $S=(n-1)w$. Очевидно, что при разрушении некоторого подмножества вершин эта стоимость меняется. Как обеспечить некоторую пороговую стоимость при разных сценариях разрушения вершин (или добавления новых)?

Применение адресации ориентиров (*Landmark hierarchy*) и теории устойчивости.

Сначала опишем основные свойства «иерархии ориентиров». Из них станет понятен набор идей, которые будут алгоритмически реализоваться. Затем опишем состав алгоритмов модели.

1. На графе можно задавать смежность вершин, расстояние $\rho(u, v)$ между вершинами, окрестности вершины v определенного радиуса $r(v)$, числовые характеристики ребер и вершин, за счет которых задача параметризуется и т.п. Вся эта информация хранится, передается и периодически обновляется, в частности в динамических таблицах маршрутизации. Но для адресации используется понятие «ориентир» (это плохой перевод слова *landmark*, поэтому мы будем использовать оригинальный термин). Это не подграф G , а объект адресно-административный. Поэтому наравне с таблицами маршрутизации необходимы динамические *таблицы адресации*. Они используют понятия *уровень вершины* и *видимость*. Поэтому понятие *landmark* имеет два значения. Это и сама вершина, и множество вершин графа, из которых она видна. Уровни задают иерархию. В графе должен быть один или несколько *Landmark* максимального уровня. Они обладают тем свойством, что видны из всех вершин графа. Заметим, что две смежные вершины графа могут лежать в разных *Landmarks*. Получается, что каждая вершина входит обязательно в несколько *Landmark*, поэтому имеет множество адресов. Кроме того, возможна неполная адресация, если источник и адресат входят в *Landmark* небольшого уровня.

2. Инициализация алгоритма в нашем случае осуществляется вручную. Ориентиры (вместе со своими параметрами) просто назначаются. Однако, в [1] предусмотрены и другие методы: назначаются только ориентиры нулевого уровня с их радиусами, а дальше все делается автоматически на основе обмена информацией между вершинами об их свойствах и параметрах; если же в сети уже есть доменная адресация, то можно ее трансформировать. После инициализации алгоритм автоматически настраивается на изменения в сети.

3. Для этого используются параметры вершин, ребер и всей сети в целом. Примеры глобальных параметров: максимальный уровень *Landmark*, соотношения между радиусами соседних по уровню *Landmark*, максимальные времена работы этапов алгоритма, число

альтернативных путей в алгоритме маршрутизации; допуски многокритериального выбора (константы, регулирующие степень адекватности назначений *Landmark* по тому или иному критерию) и т.д. Параметры вершин: имя, степени захода и исхода, число соседей, веса смежных ребер (их может быть несколько и каждый из них имеет свой смысл); статус вершины (это важнейший параметр, который говорит о том, что эта вершина может, что хочет, что ей разрешено и т.п.); радиусы своего и всех предыдущих по уровню (так как большинство вершин имеет нулевой или первый уровень и при этом либо сами могут его поменять, либо им его изменят, то особенно тщательно регламентированы именно эти две ситуации); надежность узла. Параметры ребер: вес ребра для таблиц маршрутизации; надежность ребра; запас ресурса на ребре и пр.

Схема алгоритма использует модификацию некоторых подходов, описанных в [1], а также результаты [2]. Ее основные особенности.

1. В [1] предполагалось, что существует сеть или набор сетей с установленной доменной адресацией и неким стандартным алгоритмом маршрутизации. Далее эта структура «переводилось» на новую адресацию, а затем оптимизировалась с использованием заданных параметров. Мы пользуемся тем, что узлы типизированы (см. пример выше), поэтому построение исходной адресации для начальной структуры не привязывается к «истории» сети.

2. Максимальный уровень иерархии 4-5 (а не 8-10) в силу указанных выше соображений.

3. Мы ввели понятия *надежность ребра* и *запас прочности ребра*. Структура графа позволяет построить полиномиальную (в отличие от [2]) процедуру нахождения радиуса устойчивости задачи о кратчайшем пути (уже на подграфе графа G. Это позволяет задавать параметры ребра не вручную, а вычислять автоматически (пусть и эвристической процедурой) на основе статусов инцидентных вершин и радиуса устойчивости.

4. Важнейшими являются алгоритмы восстановления сети при изменениях. В [1] их два типа. Нас интересует тот, который отражает дискретную последовательность событий изменения: удаление(появление) ребра, удаление (появление) вершины. (Второй тип отражает ситуацию одновременного объединения нескольких автономных ранее сетей). Каждое из событий может приводить к разным уровням «бедствия»: затрагиваются таблицы маршрутизации; затрагивается корректность иерархии; затрагивается корректность адресации; разрушается сеть. Поэтому и возникают четыре последовательно вложенных уровня тонкости и сложности работы: сначала происходит формальное изменение таблиц маршрутизации и попытка восстановления работы сети; затем (если первое не удалось) происходит необходимое изменение иерархии; после этого меняются адреса и таблицы адресации; затем осуществляется попытка восстановления работы сети. Но даже при ее неудаче есть еще один шанс. Уже искусственно можно потребовать включения в сеть определенного ребра с определенными параметрами.

Объем тезисов не позволяет изложить даже малую часть описания алгоритмов. Они опробованы на тестовых примерах.

Вывод

Мы считаем, что гибридный подход с использованием теории устойчивости позволяет придать дополнительные возможности к повышению качества возможных подходов к проблеме сохранения целостности информации распределенной в сети, склонной к разрушениям.

Наш вывод, в частности, базируется на испытаниях, результаты которых приведены в [1], правда, для несколько иных сценариев, так как наши дополнения только могут их улучшить.

Очевидно, что для определения степени актуальности данной постановки (и оценки ее эффективности) необходимы испытания на конкретном сценарии.

Литература

1. Tsuchiya P.F. The Landmark Hierarchy: A new Hierarchy for Routing // Computer Communications Review. 1988. № 4 (18). P. 35-42.
2. Гордеев Э.Н. Устойчивость решения в задаче о кратчайшем пути на графе // Дискретная математика. 1989. №3 (1). С. 39-46.
3. Гордеев Э.Н. Об исследовании устойчивости математических моделей и геометрических конфигураций кода // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2015. № 5 (105). С. 61-74.

4. Гордеев Э.Н. Сравнение трёх подходов к исследованию устойчивости решений задач дискретной оптимизации и вычислительной геометрии // Дискретный анализ и исследование операций. 2015. №3 (22). С. 18-35.

5. Гордеев Э.Н. Использование радиуса устойчивости оптимизационных задач для скрытия и проверки корректности информации // Инженерный журнал: наука и инновации. 2013. №11. С. 14-19.

About Maintaining the Integrity of Information in Networks with Rapidly Changing Structure **Gordeev E.N.⁹⁶**

Abstract. We consider a network where nodes are simultaneously information sources and information consumers and structural network elements such as routers at different levels. The network must operate for a limited period of time, delivering messages to consumers sources. During this period the disappearance (destruction) of nodes and edges of the network, and also allowed the emergence of new nodes and edges. In normal conditions for the public network domain hierarchy is very difficult. The approach based on the so-called Landmark hierarchy and the investigations of the stability of solutions in discrete optimization problems. The scheme heuristic algorithm, the parameters of which can adaptively adjust to different scenarios of network failure. The results can be used in the construction of ad hoc networks: games, sports, etc.

Keywords: routing networks, Landmark hierarchy, the stability of solutions in the shortest path problem.

УДК 004.056.5

Основные положения национальной инициативы США в области кибербезопасности

Голов И.Ю.⁹⁷, Кукишев Д.А.⁹⁸

В статье рассмотрены основные положения рассекреченной президентом США Б. Обамой «Всеобъемлющей национальной инициативы по кибербезопасности», определяющей направления повышения уровня безопасности США в киберпространстве на долгосрочную перспективу. Анализ данных положений позволит лучше понять: как самая развитая в мире в технологическом плане страна намеревается защищать свою критически важную инфраструктуру и с какими угрозами и вызовами ее безопасности она сталкивается.

Ключевые слова: киберпространство, план, технология, критически важная инфраструктура

Введение

В 21 веке деятельность правительства США в информационной сфере остается направленной на достижение и удержание информационного превосходства над другими странами. Ведущая роль США в мире будет зависеть не только от того, насколько удастся сохранить преобладающий уровень состояния и темпы развития ИТ-технологий в США по сравнению с другими странами, но и, в не меньшей мере, от того: насколько США удастся защитить свое информационное и киберпространство [1-4]. В этом контексте киберинфраструктура США становится важным национальным стратегическим ресурсом, а ее защита одним из приоритетных направлений обеспечения национальной безопасности.

⁹⁶ Gordeev Eduard, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, tatmigor@gmail.com

⁹⁷ Голов Игорь Юрьевич, кандидат технических наук, ФГУП «18 ЦНИИ» МО РФ, г. Москва

⁹⁸ Кукишев Дмитрий Анатольевич, ФГУП «18 ЦНИИ» МО РФ, г. Москва

В связи с этим США стараются предпринять полный спектр организационных и научно-технических мер и действий для решения проблемы обеспечения безопасности национального сегмента киберпространства. Барак Обама, придя на пост президента США в 2009 году, значительно интенсифицировал деятельность правительственных структур в сфере защиты киберпространства страны. В годы его президентства для решения вопросов кибербезопасности стали привлекаться существенные государственные ресурсы (чего не было ранее): административные (организационные), финансовые, людские, нормативно-правовые и др. Политика администрации Б. Обамы в области кибербезопасности потребовала не только значительных объемов финансирования, но и привлечения большого количества исполнителей НИОКР, широкого привлечения частного капитала к исследованиям и разработкам, а также серьезной работы экспертного научно-технического сообщества для генерации новых инновационных идей, подходов и направлений исследований. Привлечение широкого круга людей к решению проблем и обсуждению вопросов обеспечения кибербезопасности страны, скорее всего, стало главной причиной частичного раскрытия (в октябре 2009 г.) секретной «Всеобъемлющей национальной инициативы по кибербезопасности», принятой еще администрацией Дж. Буша-мл. в начале 2008 г. Реализация основных положений этой инициативы, определяющей основные направления работы правительства, частного сектора и американского общества в сфере повышения уровня безопасности США в киберпространстве, по замыслу высшего руководства США, позволит обеспечить дальнейшее доминирование США в информационной сфере на долгосрочную перспективу (в течение 20-25 лет).

Основные положения

«Всеобъемлющая национальная инициатива по кибербезопасности» (Comprehensive National Cybersecurity Initiative – CNCI) [5] преследует следующие основные цели повышения уровня безопасности США в киберпространстве:

- **установка передний рубеж обороны от непосредственных угроз** путём расширения общей осведомлённости пользователей о реальной ситуации в сети в отношении ее уязвимости, имеющихся угроз и возможностей федерального правительства, а также правительств штатов, местных властей и партнеров из частного сектора;
- **защита от всего спектра угроз** путём расширения контрразведывательных возможностей США и укрепления безопасности сети операторов по всем ключевым информационным технологиям;
- **укрепление безопасности киберпространства** за счёт обучения пользователей, координации и переориентации усилий федерального правительства в области исследований и разработок;
- **разработка стратегии сдерживания враждебной (недружественной) деятельности в киберпространстве.**

Кроме общесистемных декларируемых принципов (целей) инициатива включает в себя в себя 12 конкретных пунктов, обязательных к исполнению органами исполнительной власти и рекомендуемых к исполнению частным сектором, обществом и отдельными людьми:

1. «Надежное соединение с сетью Интернет». Подключение правительственных сетей к внешним сетям производится через доверенные точки. Провайдерами доступа к сети Интернет предполагается ограниченное число специальных коммерческих провайдеров. Правительственные министерства и ведомства, располагающие собственными возможностями, подключаются к сети Интернет через своих провайдеров. Все другие министерства и ведомства могут заключать договоры со специальными коммерческими провайдерами, прошедшими процедуру аттестации и работающими через контактный механизм NETWORKS Администрации общих служб. Создание доверенных

точек позволит снизить число точек подключения, обеспечить общность подходов и решений в сфере обеспечения безопасности информационного обмена и информационных ресурсов, установить единые правила подключения и работы в сети, упростить верификацию трафика, информационных ресурсов и отдельных пользователей.

2. Внедрение в федеральных учреждениях сенсоров систем обнаружения и предупреждения вторжений в местах подключения правительственной сети к внешним сетям (сети Интернет). Министерство внутренней безопасности в рамках проекта «Эйнштейн-2» разворачивает сигнатурные сенсоры, которые позволяют выявлять вредоносную активность и злоумышленный контекст в недоверенном трафике.

3. Внедрение в государственных организациях систем предотвращения кибератак в рамках проекта «Эйнштейн-3». Целью установки является развертывание системы, которая сможет блокировать вредоносный трафик, до того, как он сможет нанести вред целевым системам и информационным ресурсам.

4. Координация и переориентация исследований и разработок в области технологий кибербезопасности. Целью пункта является разработка стратегии и структуры координации всех НИОКР в области разработки и совершенствования технологий кибербезопасности (как секретных, так и несекретных) с установлением единых правил, процедур и ответственных заказчиков, ответственных за разработку. Это исключительно важно для исключения избыточности федерального финансирования НИОКР по тематике кибербезопасности, а также для формирования инвестиционной стратегии в этой области.

5. Укрепление взаимодействия (осуществление обмена данными) между киберцентрами с целью повышения уровня общей ситуационной осведомленности о киберугрозах. В рамках данного пункта усилия фокусируются на ключевых технологиях практического взаимодействия различных элементов киберактивности, в том числе повсеместное внедрение организационных решений и проведение инвестиций, повышающие уровень информационной осведомленности с помощью обмена аналитическими технологиями, а также так называемыми «технологиями сотрудничества». Ключевую роль в этом деле должен сыграть национальный центр кибербезопасности министерства внутренней безопасности, который координирует и интегрирует информацию шести национальных центров с целью обеспечения перекрестной ситуационной осведомленности, анализа, подготовки сводных справок о состоянии защищенности правительственных информационных сетей и систем США, а также дальнейшего усиления их интеграции, взаимодействия и координации.

6. Разработка и внедрение общеправительственного плана противодействия иностранным разведкам в киберпространстве. Такой план необходим для координации усилий всех федеральных министерств и ведомств с целью выявления, сдерживания, атрибуции и противодействия киберугрозам из-за рубежа, направленным против правительственных и частных информационных сетей и систем США. Для достижения этих целей план предусматривает расширение программы образования по дисциплинам обеспечения контрразведывательной деятельности в киберпространстве, программы повышения уровня осведомленности о возможных внешних киберугрозах, а также проведение НИОКР, направленных на интеграцию средств, методов и процедур киберзащиты во все кибероперации, повышение ответственности должностных лиц в отношении киберугроз и усиление сотрудничества в области противодействия внешним киберугрозам между всеми правительственными министерствами и ведомствами.

7. Повышение защищённости сетей, обрабатывающих закрытую информацию. Закрытые сети содержат наиболее чувствительную и особо охраняемую информацию федерального правительства. Обеспечение безопасности, целостности и необходимой

доступности этих сетей и систем, а также циркулирующих (содержащихся) в них данных требуют непрерывных усилий и организационно-технических мероприятий по их защите.

8. Расширение образования в сфере кибербезопасности. Существующих в правительственных структурах людей, обладающих необходимыми знаниями, навыками, опытом и способностями внедрения и эксплуатации передовых технологий кибербезопасности, не достаточно. Более того, в сфере обеспечения кибербезопасности правительственных федеральных структур отсутствуют адекватные возможности для карьерного роста. Отсюда возникает проблема, что наиболее квалифицированные и образованные эксперты в данной области концентрируются в коммерческом ИТ-секторе. Существующие государственные программы подготовки персонала в области кибербезопасности ограничены по своим возможностям и целям, отстают от насущных потребностей отрасли и страдают от отсутствия унификации. Для эффективного обеспечения в перспективе технического превосходства США в сфере кибербезопасности необходимо готовить технически грамотных специалистов, мотивированных для работы правительственных структурах в сфере кибербезопасности. Решение этой задачи потребует от правительства серьезных усилий, подобных тем, которые в 60-х годах прошлого века были предприняты для достижения мирового уровня американским математически и научным образованием.

9. Разработка прорывных технологий, стратегий и программ в области кибербезопасности. Целью данного пункта является, в первую очередь, разработка технологий и систем, обеспечивающих кибербезопасность, уровень которой на порядок превышал бы показатели существующих технологий и систем за рубежом. При этом данные технологии и системы должны быть внедрены уже в ближайшие 5–10 лет. Это потребует разработки программы финансирования НИОКР, ориентированных на высокорисковые/высокоэффективные решения ключевых теоретических и научно-практических проблем кибербезопасности.

10. Разработка перспективных стратегий и программ сдерживания киберугроз. Этот пункт нацелен на формирование нового государственного подхода к построению стратегии киберзащиты, который направлен на сдерживание кибератак путем радикального совершенствования киберпотенциала их предупреждения, четкого определения в этом процессе ролей правительственных структур, частного сектора, международных партнеров США, а также разработки, правовых нормативных актов, процедур и технологий осуществления адекватно реагирующих ответных действий со стороны как государственных, так и негосударственных акторов.

11. Разработка многофакторного подхода к управлению и анализу киберрисков в глобальных экономических системах. Глобализация рынка коммерческих информационных технологий создает реальные возможности для получения к ним доступа тех структур, которые намерены нанести ущерб США путем проникновения в международные и национальные экономические системы с целью получения несанкционированного доступа к данным, их модификации или вывода из строя. Риски такого рода вмешательства в глобальные экономические системы должны всесторонне оцениваться правительственными экспертами на стратегическом уровне, учитывая при этом весь жизненный цикл продукта, системы или услуги. Анализ и управление такими рисками требует: большей осведомленности об угрозах, уязвимых местах этих систем и возможных последствиях воздействия на них, связанных с приобретением (использованием) такого продукта (системы, услуги) с обязательным внедрением и эксплуатацией систем защиты, технически и операционально учитывающих соответствующие риски в течение всего жизненного цикла (от проектирования до утилизации); разработки новой политики и практики государственных закупок, которая

отражала бы сложности существующих киберугроз; близкого партнерства с коммерческим сектором с целью разработки и внедрения систем и передового опыта эксплуатации глобальных экономических систем и передовых стандартов и лучших практик управления рисками.

12. Определение роли федерального правительства при укреплении кибербезопасности критически важных инфраструктур. Правительство США при исполнении своих государственных и общественных функций сильно зависит от множества критически важных объектов инфраструктур, находящихся в частном секторе, которые, в свою очередь, недостаточно защищены и чувствительны к злонамеренным киберугрозам. Данный пункт инициативы подразумевает организацию более тесного партнерства между федеральным правительством и частным сектором, управляющим объектами критически важной инфраструктуры. Министерство внутренней безопасности и его партнеры из частного сектора разработали поэтапный план совместных действий по киберзащите критически важной инфраструктуры. План включает краткосрочные и долгосрочные рекомендации по защите, учитывающие текущую деятельность этих структур. План предусматривает также осуществление конкретных мер обеспечения кибербезопасности, имеющие целью повысить гибкость реагирования и защитный киберпотенциал частного сектора, эксплуатирующего объекты критически важной инфраструктуры. Он также предусматривает на обмене информации между правительством, частным сектором и обществом о киберугрозах и инцидентах, имеющих место на этих объектах.

Выводы

«Всеобъемлющая национальная инициатива по кибербезопасности» определила основные магистральные направления обеспечения приемлемого уровня кибербезопасности киберпространства США на долгосрочную перспективу (40 лет и более), которые видятся правительству США.

Анализ данных положений позволяет определить основные пути и направления работ по защите киберпространства США, к которым относятся:

- обеспечение надежного и безопасного соединения с сетью Интернет всех правительственных сетей и систем через доверенные точки доступа;

- разработка и развертывание на государственном уровне всеобъемлющей системы обнаружения вторжений и противодействия компьютерным атакам «Эйнштейн-2» и «Эйнштейн-3», развертывание системы киберцентров с целью повышения уровня общей ситуационной осведомленности о киберугрозах и быстрого подавления распространения в сети новых вирусных инфекций;

- разработка технологий и аппаратно-программных средств, обеспечивающих значительное повышение сетей и систем, обрабатывающих закрытую информацию;

- расширение разведывательных и контрразведывательных возможностей в области ведения информационного противоборства спецслужб США в рамках реализации общеправительственного плана противодействия иностранным разведкам в киберпространстве;

- повышение уровня финансирования НИОКР в области защиты киберпространства, более жесткая координация и переориентация исследований и разработок, разработка прорывных технологий, методов, аппаратного и программного обеспечения в области кибербезопасности;

- разработка стратегий сдерживания противоборствующих сторон в киберпространстве, отработка и распространение лучших практик реагирования на кибератаки, имеющих в частном секторе, разработка многофакторного подхода к управлению и анализу рисков в сложных критических системах (в том числе глобальных

экономических системах, системах управления производством, транспортом, электросетями и др.);

расширение возможностей получения образования и обучения в сфере кибербезопасности;

тесное взаимодействие правительственных структур с частным сектором, эксплуатирующим объекты критической инфраструктуры страны, а также научным и экспертным сообществом в сфере киберзащиты, повышение роли правительства в их защите;

Практически схожие проблемы, цели и задачи в сфере защиты национальной инфраструктуры стоят и перед Россией. Приняты соответствующие государственные решения: законы (ФЗ №№ 374, 375 от 6 июля 2016 г.) указы, постановления, приказы и распоряжения по противодействию кибертерроризму, защите информационной инфраструктуры страны, сетей и систем банковского, энергетического, транспортного сектора, автоматизированных систем управления процессами критически важных объектов жизнеобеспечения, ядерных и вредных производств, разворачивается система обнаружения и предотвращения компьютерных атак СОПКА и др. Выделены достаточные денежные средства на финансирование НИОКР в области информационной безопасности государства, поставлены и успешно реализуются программы импортозамещения электронной компонентной базы, компьютерного и телекоммуникационного оборудования, системного и прикладного программного обеспечения. К реализации этой задачи привлечены лучшие научные и производственные коллективы страны. В ведущих технических вузах России по новым скорректированным программам осуществляется подготовка специалистов по специальности «информационная безопасность». Увеличиваются возможности спецслужб, министерств и ведомств, национальных ИТ-компаний по защите киберпространства страны и своих ведомственных сегментов. При правильной организации и реализации этой работы и имеющихся планов у России есть все шансы на базе своих ресурсов и технологий надежно обеспечить безопасность своей национальной кибернетической инфраструктуры.

Литература

1. Голов И.Ю. Стратегический план научных исследований и разработок США в области кибербезопасности // Вопросы защиты информации. 2013. № 3 (102). С. 86-91.
2. Марков А.С. Летописи кибервойн и величайшего в истории перераспределения богатства // Вопросы кибербезопасности. 2016. № 1 (14). С. 68-74.
3. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA// Вопросы кибербезопасности. 2015. №3(11). С. 2-14.
4. Петренко А.А., Петренко С.А. НИОКР агентства DARPA в области кибербезопасности // Вопросы кибербезопасности. 2015. №4 (12). С. 2-22.
5. The Comprehensive National Cybersecurity Initiative // National Security Council. 2010. URL: <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.

Basic Provisions of the Us Comprehensive National Cybersecurity Initiative

I.Golov⁹⁹ and D.Kukishev¹⁰⁰

The article contains basic provisions of «The US Comprehensive National Cybersecurity Initiative», declassified of the US President B. Obama, which determined the directions of increase the level of USA security in cyberspace on long-term perspective. The analysis of these provisions allows to understand better: how the most developed in the technological plan the

⁹⁹ IgorY. Golov, Chief Scientist, 18 Central Military R&D Institute, Moscow, Russia.

¹⁰⁰ Dmitrii A. Kukishev, Head of Department, 18 Central Military R&D Institute, Moscow, Russia.

state intends to protect own critical infrastructure and with which threats and challenges USA security is to impact.

Keywords: cyberspace, plan, technology, critical infrastructure.

УДК 51.74

Об одном подходе к оценке рисков при моделировании систем защиты информации
Гордеев Э.Н.¹⁰¹

При моделировании систем защиты информации и информационного обмена используются известные оптимизационные задачи, например, задача о покрытии при оценке качества систем защиты; задача о назначениях при минимизации риска утечки информации, различные задачи на графах при моделировании информационного обмена. Если в таких задачах вводится минимаксный функционал, то возникает задача на узкие места (bottleneck problem), которая позволяет выявить «слабое звено» в модели. Здесь в качестве параметров используются оценки рисков элементов модели. Но не все элементы модели равноправны и не для всех можно в равной степени адекватно оценить эти риски. В данных тезисах рассматривается задача, когда допускаются возможные ошибки в определенных подмножествах элементов модели и оценивается мера этих ошибок, при которых сохраняется адекватность используемой модели. Этот подход базируется на исследовании устойчивости решений дискретных экстремальных задач на узкие места при возмущении лишь части параметров задачи.

Ключевые слова: риски при математическом моделировании, задача на узкие места, устойчивость решений, радиус устойчивости.

Введение

В качестве примеров рассмотрим две типичные ситуации. Имеется множество субъектов, обменивающихся информацией, но адекватность передачи информации (риск от потери) для каждой пары субъектов разная, при этом для каких-то пар мы можем оценить ее достаточно точно, а для каких-то можем лишь приблизительно. Построить модель минимизации риска можно с использованием какой-нибудь дискретной экстремальной задачи (см., например, [1]), но насколько можно доверять полученному в результате решению? Например, в известной модели с множеством средств защиты и множеством объектов защиты в каких-то средствах мы уверены, а в каких-то просто доверяем рекламе поставщиков. Оптимизационная модель здесь сводится к известной задаче о взвешенном покрытии, но как оценить качество решения?

Рассмотрим следующую модель. Пусть $E = \{e_1, \dots, e_m\}$ - некоторое множество, $D_m = \{\square_1, \dots, \square_q \mid q > 1\}$ - система подмножеств множества E , называемых траекториями.

Элементам из E приписаны веса $w(e_1) = a_1, \dots, w(e_m) = a_m$.

И пусть вектор $A = (a_1, \dots, a_m)$, берется из некоторого пространства R^m .

На каждой траектории определяется функционал $\square(A)$ - длина траектории при взвешивании A . В нашем случае это функционал на узкие места:

$$\tau(A) = \max_{e_i \in \tau} a_i.$$

Под задачей понимается тройка (E, D_m, A) . Пара (E, D_m) определяет “комбинаторику” задачи, поэтому, если эта пара и функционал фиксированы, а варьируется лишь некоторое

¹⁰¹ Гордеев Эдуард Николаевич, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, tatamigor@gmail.com

подмножество C , $|C|=k$, элементов вектора $A=(a_1, \dots, a_m)$ в R^m (конфигурационном пространстве), то получающуюся при этом индивидуальную задачу будем обозначать через $Pr_{A(C)}$.

Решениями задачи называются траектории, доставляющие минимум функционалу (оптимальные траектории).

Множество номеров оптимальных траекторий задачи при взвешивании $\square$ обозначим через $\varphi(A)$, а длину оптимальной траектории через $m(A)$. Пусть $R_0=\{\square: \square \in R^m, |\square(A)|=q\}$ и в пространстве R^m задана норма.

Назовем задачу $Pr_{A(C)}$ ε -устойчивой, если для любого $B \in R^m$ с нулевыми компонентами на месте элементов не из множества C и такого, что $\|B\| < \varepsilon$, выполняется условие $\varphi(A+B) \subseteq \varphi(A)$.

Радиус устойчивости задачи $Pr_{A(C)}$, $\square \in R_0$, полагаем по определению равным нулю, в противном случае радиусом устойчивости назовем $\sup \varepsilon$, где $\sup$ берется по всем $\square$, для которых Pr_A является $\square$ -устойчивой.

Обозначим радиус устойчивости задачи Pr_A через $\rho(A)$.

Таким образом, радиус устойчивости задает предел возмущений элементов весового вектора задачи Pr_A , при которых не расширяется множество оптимальных решений.

Данный подход подробно аргументирован в [2]-[5].

В содержательном смысле элементы C – это те весовые параметры задачи, которые мы знаем не точно. Выбор функционала оправдан, когда риск не аддитивен (не накапливается), т.е. максимальные риск мажорирует все остальное. Радиус устойчивости показывает, насколько мы можем ошибаться в оценке риска при выборе стратегии принятия решения.

Формулы и оценки

Объем тезисов не позволяет приводить доказательства результатов, поэтому мы просто приведем некоторые формулы для радиуса устойчивости и оценки его величины в рамках поставленной выше задачи для случая чебышевской нормы в конфигурационном пространстве.

Рассмотрим траекторию $\square_i$ и через $\tau_i^s(A)$, $\tau_i^n(A)$ обозначим соответственно веса максимального стабильного (не входящего в C) элемента и максимального нестабильного (входящего в C) элемента. Пусть $V(A)$ – множество неоптимальных траекторий, в которых нет стабильных элементов веса, большего $m(A)$. Пусть $R_0(A)$ – множество оптимальных траекторий таких, что для траектории $\square_i$ из этого множества выполняется условие: $\tau_i^n(A) = \min_{\tau_k, k \in \varphi(A)} \tau_k^n(A)$. Для

любой такой траектории $\square_i$ и любой неоптимальной траектории $\square_s$ корректно определены следующие параметры:

$$\alpha_{si}(A) = \tau_s(A) - \tau_i(A), \beta_{si}(A) = \tau_s^s(A) - \tau_i^n(A), \gamma_{si}(A) = \tau_s^n(A) - \tau_i^n(A).$$

Пусть по определению

$$P_i(A) = \min_{\tau_s \in V(A), s \notin \varphi(A)} \{\alpha_{si}(A), \gamma_{si}(A)\}, \min_{\tau_s \notin V(A)} \{\max\{\beta_{si}(A), \gamma_{si}(A)\}\}.$$

$$\alpha^*(A) = \min_{\tau_i \in R_0(A), s \notin \varphi(A)} \alpha_{si}(A).$$

Формулы для радиуса устойчивости приведены в следующих трех утверждениях, которые охватывают все возможные случаи.

Теорема 1. Пусть $A \notin R_0$, $V(A) = \emptyset$ и существует оптимальная траектория, состоящая только из стабильных элементов, тогда $\rho(A) = \infty$.

Теорема 2. Пусть $A \notin R_0$, $V(A) \neq \emptyset$ и существует оптимальная траектория $\square_i$, состоящая только из стабильных элементов, тогда число $\min_{\tau_k \in V(A)} \alpha_{ki}(A)$ не зависит от i и

$$\rho(A) = \min_{\tau_k \in V(A)} \alpha_{ki}(A).$$

Теорема 3. Пусть $A \notin R_0$ и в любой оптимальной траектории $\square_i$ существует нестабильный элемент, тогда величина $P_i(A)$ не зависит от i и $\rho(A) = P_i(A)$.

Если теперь допустить следующую ситуацию: разделение элементов на стабильные и нестабильные происходит после решения задачи и нахождения оптимальной (оптимальных) траектории. То из теорем вытекают, например, такие следствия.

Пусть *норменными* называются те элементы траектории, на которых достигается ее длина.

Следствие 1. Если возмущаются только элементы, не превосходящие $m(A)$, то $\rho(A) = \alpha^*(A)$.

Следствие 2. Если возмущаются только элементы, превосходящие $m(A)$, то $\rho(A) = \alpha^*(A)$.

Пусть $S(A)$ – множество неоптимальных траекторий, длина которых меньше, чем $2 \min_{s \notin \varphi(A)} \tau_s(A) - m(A)$.

Следствие 3. Если возмущаются только *норменные* элементы траекторий, то для любой $\square_i$ из $R_0(A)$ число $\min_{\tau_s \in S(A)} \{\max\{\beta_{si}(A), \gamma_{si}(A)\}\}$ не зависит от i и $\rho(A) = \min_{\tau_s \in S(A)} \{\max\{\beta_{si}(A), \gamma_{si}(A)\}\}$.

Если построить три упорядоченные последовательности: из всех элементов A , из стабильных элементов и из нестабильных элементов, то в терминах этих последовательностей можно получить простые оценки для радиуса устойчивости снизу и сверху, вычисляемые за линейное время.

Вывод

Модели оценки риска достаточно адекватно описываются не аддитивным функционалом, в функционалом на узкие места. Добавление к традиционной оптимизационной задаче исследование ее решения на устойчивость дает дополнительные возможности при выборе стратегии принятия решения в той ситуации, моделью которой является оптимизационная задача. Приведенные здесь оценки и формулы для радиуса устойчивости могут представлять практический интерес, а имплементация алгоритмов для их вычисления, может быть осуществлена на основе модификации алгоритмов решения задачи. (См. [2], [3]).

Литература

1. Басараб М.А., Булатов В.В., Булдакова Т.И. и др. Математические основы информационной безопасности. (Под редакцией В.А.Матвеева). М.: НИИ радиоэлектроники и лазерной техники МГТУ им. Н.Э.Баумана, 2013. 244 с.
2. Гордеев Э.Н. Использование радиуса устойчивости оптимизационных задач для скрытия и проверки корректности информации // Инженерный журнал: наука и инновации. 2013. №11. С. 14-19.
3. Гордеев Э.Н. Об исследовании устойчивости математических моделей и геометрических конфигураций кода // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2015. № 5 (105). С. 61-74.
4. Гордеев Э.Н. Об устойчивости задачи на узкие места // Журнал Вычислительной Математики и Математической Физики. 1993. №9 (33). С. 1391-1402.
5. Гордеев Э.Н. Сравнение трёх подходов к исследованию устойчивости решений задач дискретной оптимизации и вычислительной геометрии // Дискретный анализ и исследование операций. 2015. №3 (22). С. 18-35.

An Approach to Risk Assessment in Modeling of Information Systems

Gordeev E.N.¹⁰²

Abstract. In the simulation, the protection of information systems and information exchange using known optimization problems, such as the coverage problem of in the evaluation of the quality of security systems; assignment problem while minimizing the risk of information leakage, a variety of problems on graphs for modeling information exchange. If such problems introduced the minimax functional, then the problem occurs at the bottleneck, which allows you to identify the "weak link" in the model. Here, as parameters used risk assessment model elements. But not all elements of the model are equally at risk and is not for everyone can be equally adequately assess these risks. In these theses we consider the problem

¹⁰² Gordeev Eduard, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, tatmigor@gmail.com

when admitted errors in certain subsets of elements of the model and measure these errors is estimated, that preserve the adequacy of the model used. This approach is based on a study of the stability of solutions of discrete extreme bottleneck problem under perturbation of only part of the parameters of the problem.

Keywords: risks in mathematical modeling, bottleneck problem, the stability of solutions, stability radius.

УДК 004.383.3

Анализ автоматических систем контроля доступа **Ефремов Е.А., Ковалевский А.Е.¹⁰³**

В данной работе рассматриваются уязвимости широко распространенных в повседневной жизни систем автоматического контроля доступа, будь то сигнализация от автомобиля, дистанционное управление шлагбаумом или воротами гаража. Также по результатам найденных уязвимостей будет составлена универсальная модель кодграббера, зная принципы работы которой, можно будет успешно противодействовать взлому.

Ключевые слова: противодействие взлому, автомобильные сигнализации, взлом автоматических систем.

Введение

В настоящее время, когда научно-технический прогресс делает семиметровые шаги вперед, электронные системы все больше и больше занимают места в нашей жизни. Многие люди хранят важные документы в телефонах, компьютерах, передают конфиденциальные данные по открытым каналам связи, доверяют безопасность своей собственности уже не механическим, а электронным системам защиты. Однако все ли задумываются о том, насколько защищены те, или иные средства?

Наша исследовательская работа посвящена поиску уязвимостей автоматической системы контроля доступа фирмы Came, а также разработке рекомендаций по противодействию несанкционированного доступа на объекты, для охраны которых используются данные системы.

Цели работы:

- Изучение информации об устройстве и принципе работы охранных систем данного класса устройств
- Конструирование испытательной модели охранной системы на основе изученной информации на базе микроконтроллера Arduino Uno
- Исследование амплитудно-частотных характеристик брелоков различных фирм-изготовителей автоматических систем контроля доступа
- Поиск возможных уязвимостей автоматической системы контроля доступа Came
- Конструирование опытного образца устройства для взлома охранной системы
- Разработка рекомендаций по противодействию взлому данных систем

Информация об устройстве и принципе работы охранных систем

Рассматриваемая нами автоматическая система контроля доступа (далее АСКД) представляет собой систему из:

- Двухканального радиоприемника команд управления, работающего на частоте 433,92 МГц

¹⁰³ МГТУ им. Н.Э. Баумана, dedelya666@gmail.ru, net_packet@mail.ru

- Брелоков-передатчиков на частоте 433,92 МГц, имеющих дальность действия порядка 20 метров

Ниже представлен снимок со сканера частот(Рис. 1):

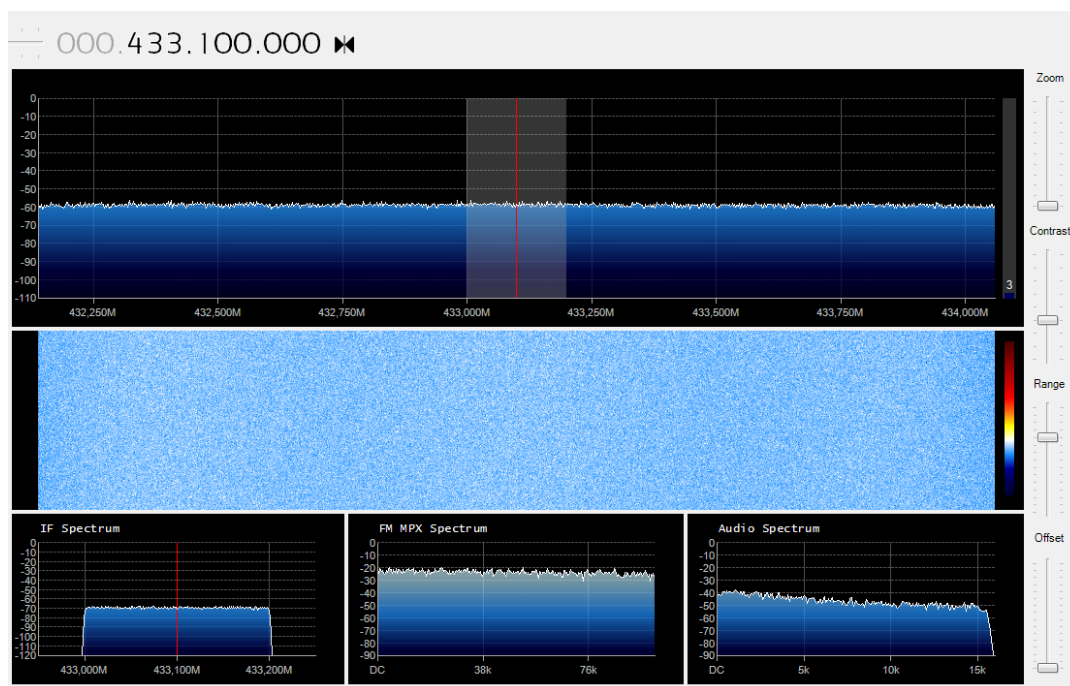


Рис. 2. Снимок со сканера частот

Как видно на картинке, прослушивается диапазон частот 432,25 434 МГц, при передаче сигнала наблюдаются соответствующие картины на спектрограмме(Рисунок 2) и сонограмме(Рисунок 3).

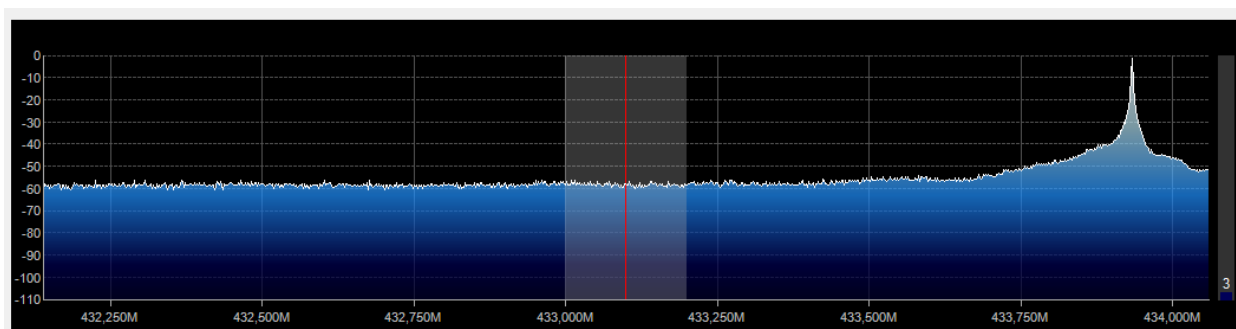


Рис. 3. Момент передачи сигнала на спектрограмме

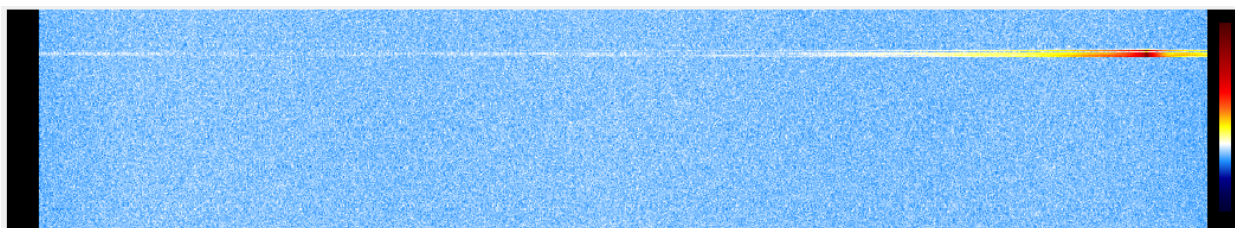


Рис. 4. Момент передачи сигнала на сонограмме

Для добавления нового передатчика в память приемника необходимо запустить операцию копирования кода с одного брелока на другой. Следовательно, нет никакой необходимости производить какие-либо манипуляции с приемником. Рассмотрим передаваемый сигнал более подробно.

До сих пор остается актуальным формат статических кодов. Форматы разных фирм отличаются друг от друга длительностями импульсов. Для реализации передатчиков используются микросхемы кодеров Holtek HT-12E – в этом случае в брелоках устанавливают микропереключатели, которыми задается номер брелока. Могут иметь одну или несколько кнопок – микросхема кодера позволяет реализовать от 1 до 4 кнопок. Длительности импульсов задаются резистором в обвязке кодера. Встречаются кодеры без наборного поля, серийный номер прошивается в микросхему производителем.

Кодовая посылка состоит из 12 бит. Перед началом кода идет пилотный период (состоящий из 36 интервалов низкого уровня) и стартовый импульс (состоящий из 1 интервала высокого уровня). Именно длительность стартового импульса указывает, какой временной интервал используется при формировании сигнала. После стартового бита начинается сама посылка, начало бита – с низкого уровня. После окончания последнего импульса кодовое слово повторяется, начиная с пилотного периода. При коротком нажатии на кнопку передаются 4 кодовых слова, при удержании кнопки посылки циклически повторяются (сериями по 4 кодовых слова). Возможное количество кодовых комбинаций – 4096. Рассмотрим импульсы различных АСКД. Длительности импульсов САМЕ:

Лог. «1» – 640 мкс низкий уровень (два интервала), 320мкс высокий (один интервал)

Лог. «0» – 320 мкс низкий уровень (один интервал), 640мкс высокий (два интервала).

Пилотный период – 11520 мкс, стартовый импульс – 320 мкс.

Длительности импульсов NICE:

Лог. «1» – 1400мкс низкий уровень (два интервала), 700мкс высокий (один интервал)

Лог. «0» – 700мкс низкий уровень (один интервал), 1400мкс высокий (два интервала).

Пилотный период – 25200 мкс, стартовый импульс – 700 мкс.

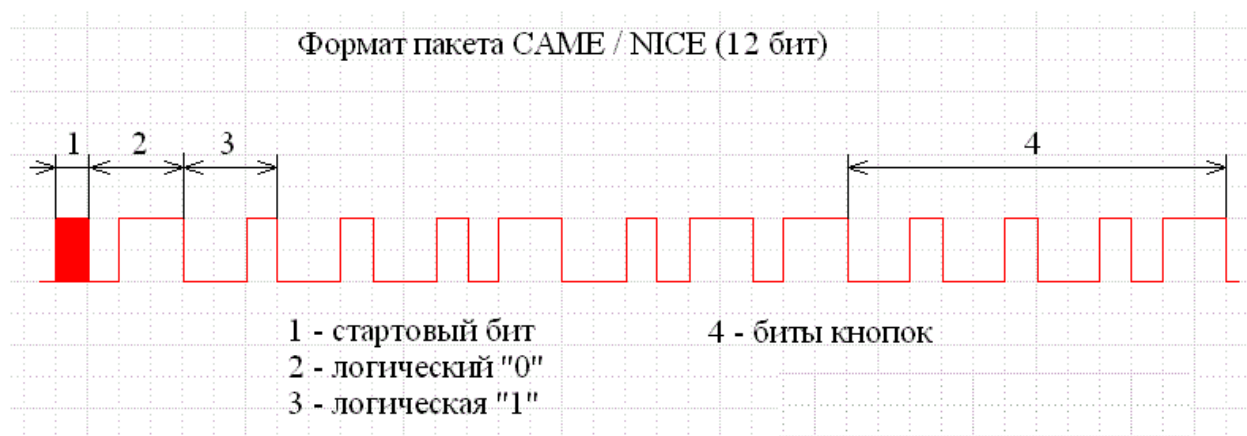


Рис. 5. Амплитудно-частотная характеристика сигнала

Возможны и другие длительности импульсов, но соотношения высоких и низких уровней, а также пилотный период и стартовый бит формируются по такому же принципу.

Из найденной информации следует, что для того, чтобы открыть шлагбаум, необходимо либо скопировать код, в момент его передачи, либо подобрать его.

Конструирование испытательной модели АСКД на базе микроконтроллера Arduino Uno.

Arduino — это открытая платформа, которая позволяет собирать всевозможные электронные устройства. Платформа состоит из аппаратной и программной частей. Для программирования используется упрощённая версия C++, известная так же как Wiring.

Помимо Arduino были использованы:

- Беспроводной передатчик на 433 МГц (WRL-10534)^[1]
- Беспроводной приёмник на 433 МГц (WRL-10532)^[2]

Результатом этого этапа исследовательской работы стало создание макета, включающего в себя модели устройств «шлагбаум – брелок» и «шлагбаум – перехватчик – брелок».

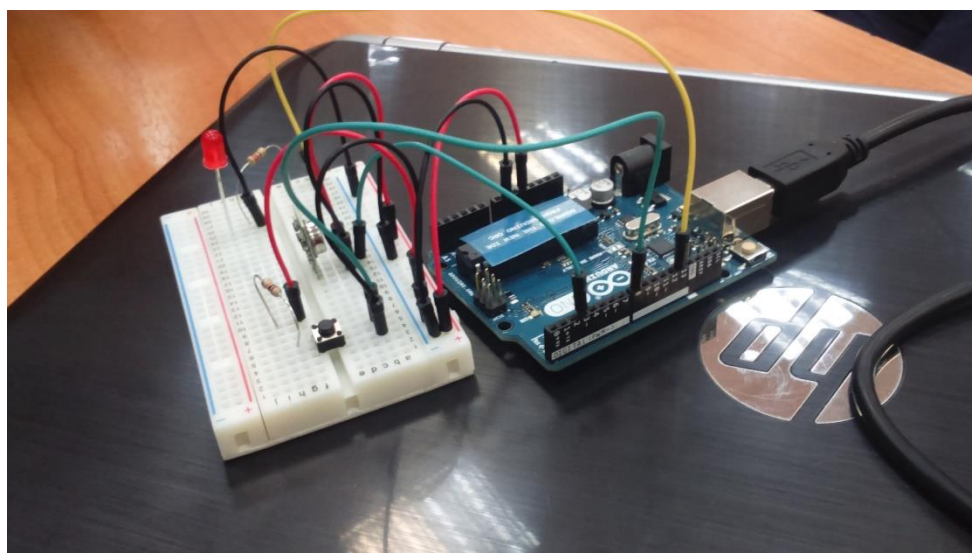


Рис. 6. Передатчик

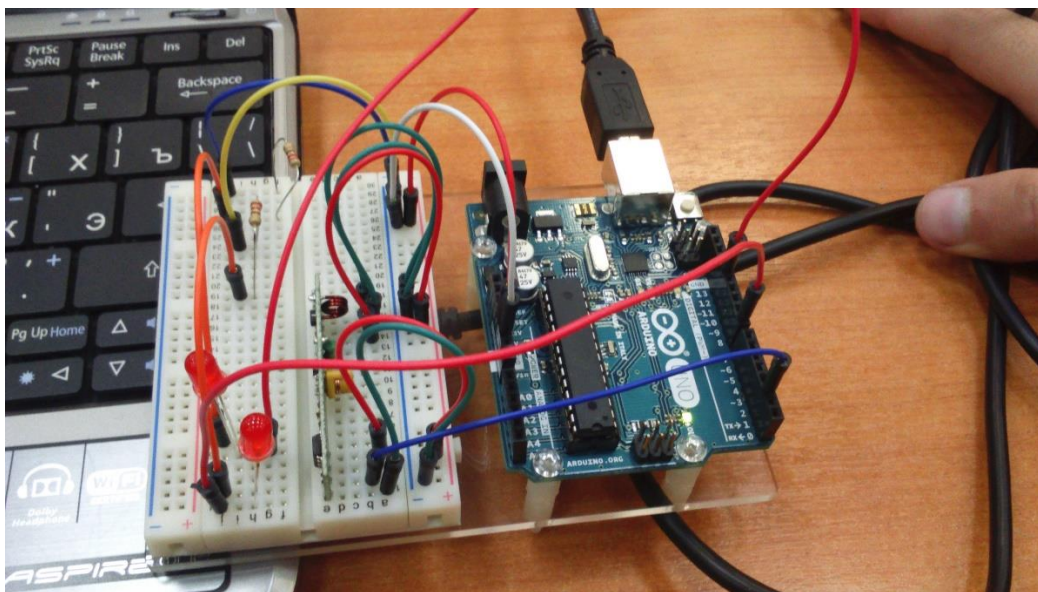


Рис. 7. Приемник

Модель «шлагбаум – брелок» представляет собой взаимодействие двух модулей: приемника, имитирующего охранное устройство, и передатчика, имитирующего работу брелока (может быть использован брелок от обычной охранной системы, работающей на частоте 433МГц).

Модель «шлагбаум – перехватчик – брелок» состоит из вышеописанных модулей и «перехватчика». «Перехватчик» представляет из себя устройство, которое в фоновом режиме сканирует и сохраняет во внутреннюю память все сигналы на частоте 433МГц.

Принцип работы модели «шлагбаум – перехватчик – брелок» описывается ниже (см. Универсальная модель кодграббера).

Исследование АЧХ брелоков различных АСКД

В ходе работы над проектом были проведены исследования амплитудно-частотных характеристик брелоков различных фирм, производящих различные АСКД, в том числе и автомобильные сигнализации. В результате стало известно, что подавляющее большинство производителей АСКД используют одинаковую частоту, а именно 433,92 МГц. Однако есть фирмы, в частности Starline, которая использует частоту 434,5 МГц, причем сигнал посылается импульсно и очень быстро. Это вызывает большие сложности при перехвате таких сигналов из-за нестандартной частоты и короткого времени передачи.

Универсальная модель кодграббера

Прежде всего стоит отметить, что данная модель подойдет как для различных автоматизированных охранных систем, так и для некоторых автомобильных сигнализаций (Рисунок 7). Подразумевается, что ключ не статичный, а постоянно изменяющийся, т.е. динамический. (Со статическим ключом, как уже говорилось ранее, все гораздо проще – достаточно его перехватить один раз.) К взлому такой системы защиты можно подойти по-разному, например, записав большое количество ключей, можно попытаться разгадать алгоритм генерации ключей, однако данный метод не сулит успеха. Наиболее интересна следующая модель взлома. Взломщик дожидается человека с брелоком от охранной системы, и ждет начала передачи сигнала. Затем, после отправки сигнала, кодграббер записывает сигнал, но при этом в направлении охраняемого объекта осуществляется глушение эфира, таким образом до объекта сигнал не дойдет. Естественно человек попытается нажать на кнопку ещё раз, чтобы повторить передачу сигнала. В этот

момент осуществляем аналогичные мероприятия, но уже с добавлением следующего: как только мы получаем второй ключ, глушение, например через 500 мс, прекращается, и со своего кодграббера мы посылаем сигнал с первым ключом. В результате у нас остается один действующий ключ. Достоинства этого метода состоят в том, что нам не важно какой длины ключ и по какому алгоритму он генерируется.

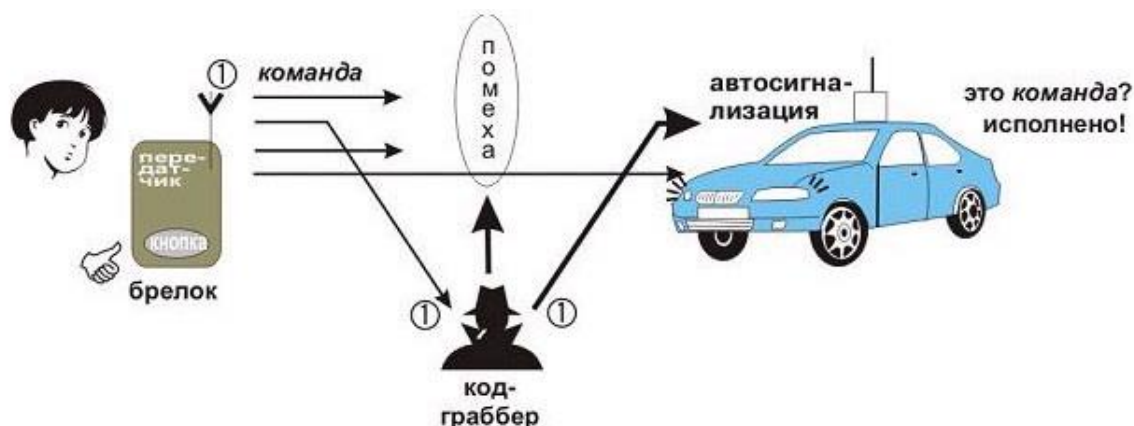


Рис. 8. Схема диалоговой системы

Из соображений противодействия таким кодграббера, можно предложить защиту по времени в совокупности с «диалогом». Её отлично описывает информационный плакат от фирмы StarLine(Рис. 8):



Рис. 9. Технология StarLine

К этому лишь стоит добавить, что если в течение определенного числа миллисекунд не будет получен ответ, то диалог считается проваленным, и начнется заново.

Стоит отметить, что в 2016 году такая система защиты становится популярной не только у производителей автомобильных сигнализаций, но и у фирм, специализирующихся по охране недвижимости.

Вывод

В настоящее время в рамках нашей исследовательской работы производится разработка устройства, способного анализировать уровни защиты конкретных АСКД путем непосредственной компрометации системы. По результатам тестирования систем АСКД можно будет выявить уязвимые места, носящие массовый характер, а также найти наиболее удачные реализации по противодействию вторжениям в работу охранных систем. Итогом проведения данных мероприятий подразумевается разработка наиболее защищенного прототипа АСКД для демонстрации устойчивости к различным типам атак на систему.

Литература

1. Техническая документация передатчика TWS-BS-3. [Электронный ресурс]. – Режим доступа: http://cdn.sparkfun.com/datasheets/Wireless/General/TWS-BS-3_433.92MHz_ASK_RF_Transmitter_Module_Data_Sheet.pdf (доступ свободный) – Загл. С экрана. – Яз. Англ.
2. Техническая документация приемника TWS-BS-3. [Электронный ресурс]. – Режим доступа: https://www.sparkfun.com/datasheets/RF/KLP_Walkthrough.pdf (доступ свободный) – Загл. С экрана. – Яз. Англ.

Рецензент: Медведев Николай Викторович, канд. техн. наук, доцент, МГТУ им. Н.Э.Баумана, medvedevnick54@yandex.ru

Analysis of Automatic Systems Access Control **Efremov E.A., Kovalevsky A.E.¹⁰⁴**

***Abstract:** We have decided to consider vulnerabilities of automatic access control systems, which widely used in everyday life. First of all this applies to car's alarms, remote control of barriers of gates. Also, there will have been made universal codegrabber's model according to the results of known vulnerabilities. The knowledge about it provide successful resistance from hacking.*

***Keywords:** counter hacking, car signaling, hacking automating systems.*

¹⁰⁴ Efremov E.A., Bauman MSTU, dedelya666@gmail.ru; Kovalevsky A.E., Bauman MSTU, net_packet@mail.ru

Новые технологии анализа и засекречивания речевых сигналов**Горшков Ю.Г.¹⁰⁵, Марков А.С.¹⁰⁶, Цирлов В.Л.¹⁰⁷**

Выполнен анализ принципов построения систем исследования речевых сигналов на основе преобразования Фурье. Изложена методология анализа и засекречивания речи на вейвлетах. Приводится структура системы исследования речевых сигналов «Фон-НІ». Проведено сравнение частотно-временных характеристик сонограмм звуков речи, полученных с использованием преобразования Фурье и многоуровневого вейвлет-преобразования. Представлены примеры построения вейвлет-сонограмм с высоким частотно-временным разрешением при анализе и засекречивании речевых сигналов.

Ключевые слова: речевой сигнал, анализ, сонограмма, засекречивание

Введение. Развитие речевых технологий в части построения систем исследования речи, комплексов идентификации диктора, а также средств засекречивания речевого сигнала во многом определяется точностью представления его частотно-временных характеристик. Системы инструментального исследования речевого сигнала находят широкое применение при решении задач криминалистической экспертизы фонограмм. Так, ежегодно, только экспертно-криминалистическими лабораториями МВД РФ выполняется несколько тысяч экспертиз. Практически все судебные фоноскопические экспертизы связаны с идентификацией дикторов по голосу и речи. В связи с этим, вопросы создания новых инструментальных средств анализа речевого сигнала и методов исследования аудиозаписей, их эффективного применения на практике, эксперты-фоноскописты относят к наиболее важным.

Безопасности конфиденциальных переговоров или засекречиванию речевой информации на телефонных каналах сети общего пользования (ТфОП) уделяется особое внимание как разработчиков, так и потребителей методов и средств речевой защиты. Специалистами кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана и ГК «Эшелон» проведены исследования по разработке новых методов, средств анализа и засекречивания речевых сигналов с использованием многоуровневого вейвлет-преобразования. В работе представлены некоторые из полученных результатов.

Системы исследования речевых сигналов. Большинство современных методов анализа звуков речи основываются на спектральной модели для стационарного сигнала. Основным недостатком этой модели является отсутствие характеристик для основных шумовых составляющих в произносимых согласных и это при том, что в большинстве языков основная речевая информация передается согласными звуками. Традиционно разрабатываемые алгоритмы идентификации личности по голосу и распознавания речи основываются, как правило, на определении характеристик гласных звуков [1]. Разработанная специалистами ООО «Центр Речевых Технологий», Санкт-Петербург, методика криминалистической идентификации дикторов с использованием комплекса исследования фонограмм «Икар Лаб» является развитием известной методики идентификации дикторов «Диалект». Включает в себя на этапе инструментального анализа

¹⁰⁰ Горшков Юрий Георгиевич, канд. техн. наук, доцент, МГТУ им. Н.Э. Баумана, Москва, y.gorshkov@pro-echelon.ru

¹⁰¹ Марков Алексей Сергеевич, д-р техн. наук, ст.науч.сотр., МГТУ им. Н.Э. Баумана, Москва, a.markov@pro-echelon.ru

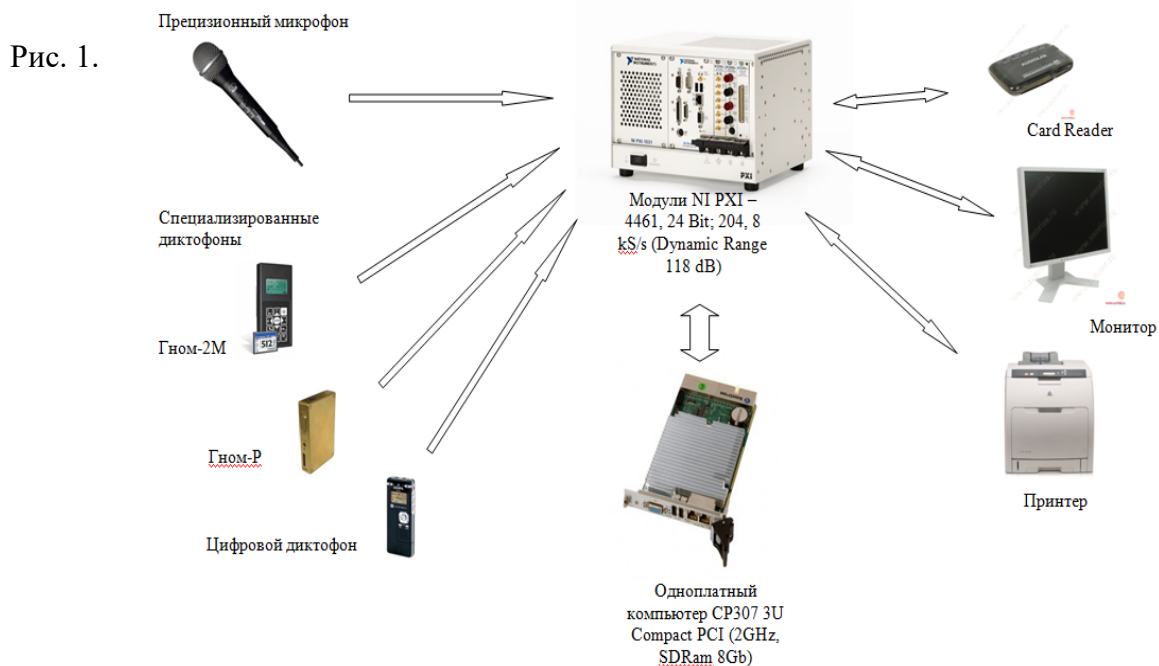
¹⁰² Цирлов Валентин Леонидович, канд. техн. наук, МГТУ им. Н.Э. Баумана, Москва, v.tsirlov@pro-echelon.ru

сравнение статистик основного тона голоса и формант, формантное «выравнивание», экспертное сравнение формант ударных гласных. В последние годы широкое применение находят комплексы «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.

Анализ и засекречивание речевых сигналов на основе вейвлетов. Все большее число специалистов по цифровой обработке сигналов убеждаются в том, что преобразования Фурье в классическом виде не обеспечивают необходимую точность представления нестационарных сигналов, в частности, к которым относятся речевые сигналы. В то же время применение на практике теории всплесков (wavelets) позволяет решать широкий круг задач при фильтрации, предварительной обработке и синтезе различных сигналов, сжатия и обработки изображений. Особенно важна принципиальная возможность вейвлетов представлять нестационарные сигналы. Значительный интерес представляет утверждения о том, что вейвлет-спектрограммы намного более информативны, чем обычные Фурье-спектрограммы и, в отличие от последних, позволяют легко выявлять тончайшие локальные особенности акустических сигналов.

В ходе исследований создавалось специальное программное обеспечение (СПО) «WaveView» высокоточного вейвлет-анализа с последующим построением изображений «видимый звук» или сонограмм. Первая версия СПО «WaveView» разработана в 2002 году. «WaveView-MWA» является последней версией СПО семейства вейвлет-анализа сигналов, в котором реализован алгоритм многоуровневой обработки.

Система исследования речевых сигналов «Фон-NI». На рис. 1 представлена структура системы исследования речевых сигналов «Фон-NI». Ввод и обработка аудиосигналов выполняется с использованием средств, выпускаемых компанией National Instruments (США): модули NI PXI – 4461, 24 Bit; 204, 8 kS/s (Dynamic Range 118 dB); одноплатный компьютер CP307 3U Compact PCI (2GHz, SDRam 8Gb). В тракт высокоточной регистрации входят: прецизионный микрофон, специализированные диктофоны «Гном-2М» «Гном-Р», цифровой диктофон. Экспериментальные исследования, проведенные с использованием системы «Фон-NI» позволили подобрать параметры программного обеспечения многоуровневого вейвлет-анализа таким образом, что высокое частотно-временное разрешение сонограмм достигалось при снижении частоты дискретизации речевого сигнала с 44,1 кГц до 8 кГц, а разрядности аналогово-цифрового преобразования с 24 бит до 16 бит.



Структура системы исследования речевых сигналов «Фон-NI»

СПО «WaveView-MWA». Обеспечивает решение задач определения подлинности фонограмм, идентификации диктора, оценки эмоциональной напряженности по голосу, получения акустической обстановки окружения [2-4].

СПО «WAVELET-FONE». Предназначено для обеспечения безопасности речевой связи на коммутируемых телефонных каналах сети общего пользования. Засекречивание передаваемой информации осуществляется многоуровневым вейвлет-преобразованием речевого сигнала по заданному ключу с последующим его восстановлением на приемном конце [5-6]. Основные характеристики: 4-х уровневое вейвлет-преобразование; общее количество ключей: $1,3 \times 10^{15}$; диапазон рабочих частот 300 – 3400 Гц; частота дискретизации 8000 Гц, разрядность 16 бит.

Выводы

Новые технологии анализа и засекречивания речевых сигналов на вейвлетах позволяют решать задачи определения подлинности фонограмм, идентификации, оценки эмоциональной напряженности диктора, получения акустической обстановки окружения и защиты речевой информации на новом уровне. Эффективное применение вейвлет-технологий обработки речевых сигналов возможно лишь при использовании на этапе регистрации фонограмм специализированных средств.

Литература

1. Горшков Ю.Г. Криминалистическое исследование фонограмм. Методические указания к лабораторным работам. МГТУ им. Н.Э. Баумана, 2016. 25 с.
2. 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.
3. Горшков Ю. Г. Исследовательский комплекс частотно-временного анализа речевого сигнала с использованием вейвлет-технологии // «Вестник Московского государственного технического университета им. Н. Э. Баумана». Серия: Приборостроение. 2011. № 4. С. 78-87.
4. Горшков Ю. Г., Каиндин А. М., Марков А. С., Цирлов В. Л. Система определения подлинности фонограмм. // Патент на полезную модель RUS 150244. 2013. 30.12.2013. Заявка № 2013158829/08. Бюл. № 4.
5. Горшков Ю. Г., Кузин А. Ю., Цирлов В. Л. Засекречивание речевой информации на основе вейвлетов // «Вестник Московского государственного технического университета им. Н. Э. Баумана». Серия: Приборостроение S-2. 2011. С. 138-145.

New Technology Analysis and Scrambling of Speech Signals

Y.G. Gorshkov¹⁰⁸, A.S. Markov¹⁰⁹, V.L. Tsirlov¹¹⁰

The principles of the construction of systems studies of speech signals based on the Fourier transform are analyzed. Methodology of the analysis and speech scrambling on the wavelets is presented. The paper provides the structure of a speech signals study system «Fon-NI». It compares the time-frequency characteristics of sonograms of speech sounds based on the Fourier transform and a multilevel wavelet transform. It provides examples to build wavelet sonograms with a high time-frequency resolution, when the analysis and scrambling of speech signals are performed.

Keywords: speech signal, analysis, sonogram, scrambling

УДК 004.056

Современные тренды в области кибербезопасности

Горшков Ю.Г.¹¹¹, Марков А.С.¹¹², Матвеев В.А.¹¹³, Цирлов В.Л.¹¹⁴

Рассмотрены основные события в области кибербезопасности в период 2015-2016 гг. Выделены основные тенденции в различных сегментах информационной и кибербезопасности.

Ключевые слова: кибербезопасность, информационная безопасность, защита информации, тенденции, тренды, прогнозы

1. Актуальность проблематики кибербезопасности

Актуальность проблематики кибербезопасности [1] можно связать с двумя феноменами информатизации общества за последние три года:

- предсказания в области компьютерных достижений и инцидентов сбываются, т.е. мировое сообщество понимает состояние вопроса;

- продолжается нарастание политического противостояния государств в киберпространстве [2, 3].

2. Основные тенденции кибербезопасности в России

Основной посыл политического противоборства нашей страны, как известно, состоит в реализации асимметричности подхода. Не является исключением и область киберпротивоборства. Опираясь на системный подход, удобно рассмотреть следующие уровни тенденций:

- политические декларации;
- законодательство;
- нормативно-правовые акты;
- технологии;
- кадровые вопросы.

¹⁰⁸ Yuri Gorshkov, Ph.D., Associate Professor, Bauman MSTU, y.gorshkov@bmstu.ru

¹⁰⁹ Alexey Markov, Dr. Sc., Associate Professor, Bauman MSTU, a.markov@bmstu.ru

¹¹⁰ Valentin Tsirlov, Ph.D., NPO Echelon, z@cnpo.ru

¹¹¹ Горшков Юрий Георгиевич, канд. техн. наук, доцент, МГТУ им.Н.Э.Баумана, y.gorshkov@bmstu.ru

¹¹² Марков Алексей Сергеевич, д-р техн. наук, ст.науч.сотр., МГТУ им.Н.Э.Баумана, a.markov@bmstu.ru

¹¹³ Матвеев Валерий Александрович, Заслуженный деятель науки РФ, д-р техн.наук, проф., МГТУ им.Н.Э.Баумана, v.a.matveev@bmstu.ru

¹¹⁴ Цирлов Валентин Леонидович, канд.техн.наук, ЗАО «НПО «Эшелон», z@cnpo.ru

2.1. Политические декларации

В плане реализации политических деклараций следует отметить:

- *документальный уровень*, касающийся текущих доктрин национальной и информационной безопасности;
- *организационный уровень*, касающийся оргштатных структур (киберкомандование);
- *технологический* - курс на импортозамещение [4].

К новым нормативным парадигмам можно отнести: Стратегию национальной безопасности РФ до 2020 г. и Доктрину ИБ (2016 г.).

2.2. Законодательство

В плане становления законодательства следует отметить следующие моменты:

- приостановление проекта «Концепции стратегии кибербезопасности РФ» [5];
- реализацию Постановления Правительства РФ 31с (ГосСОПКА) [6,7];
- ожидание ратификации проекта ФЗ «О безопасности КИИ РФ».

Нельзя не отметить ряд законодательных актов по изменениям в ФЗ-152, а также инициативы о кардинальном изменении Закона «О связи» и сопутствующих федеральных законов (ФЗ 184, 149, 152 и др.), «закон Яровой», которые касаются как обновления устаревших технологических концепций, так и повышения уровня госконтроля и национальной безопасности киберпространства.

2.3. Нормативно-правовые акты

Следует отметить актуальность обновления нормативно-правовых актов [8].

В плане формирования новых требований к мерам и средствам защиты тон задает, без преувеличения, ФСТЭК России» и Технический комитет по стандартизации ТК-362. Выделим два основных инновационных направления:

- формирование новых организационно-технических мер;
- определение критериев оценки СЗИ.

Примеры мер, соответствующих международному и национальному подходу представлены в таблице 1.

Особенность подхода, предлагаемого приказами ФСТЭК России, состоит в реализации квази риск-ориентированного подхода вместо директивного [9], а также в разработке передовых национальных мер по безопасной разработке ПО (ГОСТ Р ГОСТ Р 56939) [10].

Инновационный характер оценки соответствия СЗИ состоит в разработке НПА и пакетов профилей защиты, соответствующих международному подходу ISO 15408 [11]. Особое внимание представляет нормативный прорыв в области результативности проверок по требованиям ИБ, связанных с внедрением передовых практик выявления уязвимостей согласно ISO 20004.

Таблица 1.

Меры по ISO 27001: 2013	Меры по Приказу ФСТЭК России №17
A.5: Политики информационной безопасности A.6: Организационные аспекты информационной безопасности A.7: Вопросы безопасности, связанные с персоналом A.8: Управление активами A.9: Управление доступом A.10: Криптография A.11: Физическая безопасность и защита от угроз окружающей среды A.12: Безопасность операций A.13: Безопасность коммуникаций A.14: Приемка, разработка и поддержка систем A.15: Отношения с поставщиками услуг A.16: Управление инцидентами информационной безопасности A.17: Аспекты информационной безопасности в обеспечении непрерывности бизнеса A.18: Соответствие требованиям	1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) 2. Управление доступом субъектов доступа к объектам доступа (УПД) 3. Ограничение программной среды (ОПС) 4. Защита машинных носителей информации (ЗНИ) 5. Регистрация событий безопасности (РСБ) 6. Антивирусная защита (АВЗ) 7. Обнаружение вторжений (СОВ) 8. Контроль (анализ) защищенности информации (АНЗ) 9. Обеспечение целостности информационной системы и информации (ОЦЛ) 10. Обеспечение доступности информации (ОДТ) 11. Защита среды виртуализации (ЗСВ) 12. Защита технических средств (ЗТС) 13. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

Отметим особенности подхода ФСТЭК России:

- разрабатываемые документы «живые» (см. План разработки НПА на ftes.ru), т.е. подлежат обновлению (как известно, руководящие документы Гостехкомиссии России не претерпевали переработки с момента создания);
- разворот в сторону практической безопасности, включая тестирование на проникновение и анализ уязвимостей;
- поддержка Банка угроз и уязвимостей ФСТЭК России, имеющего, фактически, национальный характер (рис.1);
- конкретизация требований к лицензиатам, испытательным лабораториям и органам по сертификации.

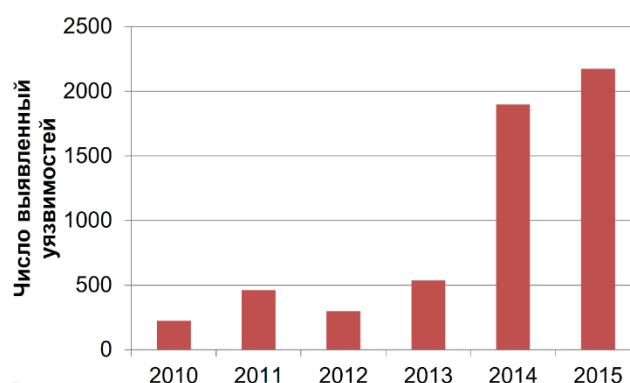


Рис.1. Динамика объема Банка данных угроз безопасности информации

2.4. Технологии

Согласно [12] выделяют три базовых направления развития механизмов безопасности:

- консолидация средств защиты информации;
- внедрение биометрических средств и методов безопасного доступа;

- исследование постквантовой криптографии.

Первый подход определяется тем, что развитие отдельных СЗИ достигло своего технологического потолка в плане результативности. Одним из направлений выхода систем информационной безопасности на новый уровень результативности является организация сбора и корреляции событий от всех СЗИ и устройств. Подобные решения получили название SIEM-систем.

Биометрические средства позволяют с одной стороны исключить недостатки, свойственные техническим средствам идентификации и аутентификации, а с другой выйти на уровень верификации субъектов защищенных информационных систем.

Постквантовая криптография – инновационное направление, основанное на эффектах квантовой физики, в первую очередь, сверхвысокой производительности квантового компьютера и невозможностью перехвата квантовой передачи данных.

2.5. Кадровые вопросы

Кадровые вопросы всегда относят к первому рубежу организации защиты информационных ресурсов в компьютерных системах. В общем плане можно констатировать что в стране продолжает функционировать ассоциация вузов в области информационной безопасности, а также идет совершенствование профессиональных стандартов в этой области. В табл. 1. указаны требования к лицензиатам в области безопасности информации [11]. С другой стороны, в стране пока национальной сертификации специалистов.

Таблица 2.

Требования по обучению

Вид и методы защиты информации	Законодательная база	Требования к лицензиатам
Защита государственной тайны	Методические рекомендации ФСБ России ФСТЭК России	ВПО ЗИ или ВТО+ переподготовка или повышение квалификации по вопросам защиты информации
Средства криптографической защиты информации	ПП 313	ВПО либо переподготовка (1000, 500, 100 час.) + стаж
Техническая защита конфиденциальной информации	ПП 79, 171 (с 15.06.2017 г.)	ВПО или переподготовка 360/500 час (руководители) 250/100 (работники)+ стаж. Переподготовка (72 час.) один раз в пять лет

Литература

1. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2). С. 28-35.
2. Марков А.С. Летописи кибервойн и величайшего в истории перераспределения богатства // Вопросы кибербезопасности. 2016. № 1 (14). С. 68-74.
3. Петренко А.А., Петренко С.А. НИОКР Агентства DARPA в области кибербезопасности // Вопросы кибербезопасности. 2015. № 4 (12). С. 2-22.
4. Муравник В.Б., Захаренков А.И., Добродеев А.Ю. Некоторые предложения по подходу и порядку реализации политики и стратегии импортозамещения в интересах национальной безопасности и укрепления обороноспособности Российской Федерации // Вопросы кибербезопасности. 2016. № 1 (14). С. 2-8.
5. Гаттаров Р.У. Концепция стратегии кибербезопасности // Вопросы кибербезопасности. 2014. № 1 (2). С. 2-4.
6. Петренко А.С., Петренко С.А. Проектирование корпоративного сегмента СОПКА // Защита информации. Инсайд. 2016. №6 (72). С. 47-52.
7. 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.
8. Плигин В.Н., Макаренко Г.И. Страна нуждается в обновлении общественных договоров в современном российском обществе // Мониторинг правоприменения. 2015. № 1 (14). С. 4-11.
9. Markov A., Rautkin Y., Luchin D., Tsirlor V. Evolution of a radio telecommunication hardware-software certification paradigm in accordance with information security requirements. // В сборнике: 2015 International

Siberian Conference on Control and Communications, SIBCON 2015 - Proceedings 2015. С. 7147139. DOI: 10.1109/SIBCON.2015.7147139.

10. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls // Journal of Theoretical and Applied Information Technology. 2016. Т. 88. № 1. С. 77-88.

11. Barabanov A., Markov A. Modern Trends in the Regulatory Framework of the Information Security Compliance Assessment in Russia Based On Common Criteria. In: ACM International Conference Proceeding Series 8. Proceedings of the 8th International Conference on Security of Information and Networks, SIN 2015. 2015. P. 30-33. DOI: 10.1145/2799979.2799980.

12. Прогноз научно-технологического развития России: 2030 / Под ред. Л.М.Гохберга и др. - М.: Минобрнауки России, ВШЭ, 2014. 244 с.

13. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности // Мониторинг правоприменения. 2017. № 1.

Modern Trends in Cybersecurity

Gorshkov Yu.¹¹⁵, Markov A.¹¹⁶, Matveev V.¹¹⁷, Tsirlov V.¹¹⁸

The main events in the field of cybersecurity the period 2014-2016 are reviewed. The basic trends in the various segments of the information and cyber security are noted.

Keywords: cybersecurity, information security, trends, forecasts

УДК 004.056

Развитие концепции безопасных социальных сетей

Зорин Е. Л.¹¹⁹, Басараб М. А.¹²⁰, Матвеев В. А.¹²¹

Аннотация. Рассматривается концепция защищенной социальной сети. Проанализированы основные незащищенности пользователей в существующих проектах социального взаимодействия и имеющиеся решения защиты пользовательской информации.

Ключевые слова: социальные сети, безопасность, криптография.

Введение

Повсеместное развитие социальных сетей приводит к необходимости выработки некоторых стандартов коммуникации между людьми в сети. Всё большее количество ранее самостоятельных технологий поглощаются и интегрируются как сервисы внутри социальных сетей. Рассмотрим очевидные проблемы безопасности подобных больших проектов, связанные с развитием функционала, а также существующие возможные пути их решения.

Незащищенность пользователей

Как правило, информация социальных сетей хранится в больших центрах обработки данных, защищенных аппаратными и программными межсетевыми экранами и имеющими самую актуальную прошивку и интеллектуальную систему предотвращения вторжения. Бесспорно, такие технологии защищают серверную инфраструктуру проекта. Вместо проникновения на сервер можно провести DDoS-атаки (отказ в обслуживании), однако современные системы защиты позволяют локализовать

¹¹⁵ Yuri Gorshkov, Ph.D., Associate Professor, Bauman MSTU, y.gorshkov@bmstu.ru

¹¹⁶ Alexey Markov, Dr. Sc., Associate Professor, Bauman MSTU, a.markov@bmstu.ru

¹¹⁷ Valerii Matveev, Honored Scientist of Russia, Dr. Sc., Professor, Bauman MSTU, v.a.matveev@bmstu.ru

¹¹⁸ Valentin Tsirlov, Ph.D., NPO Echelon, z@cnpo.ru

¹¹⁹ Зорин Егор Леонидович, МГТУ им. Н. Э. Баумана, Москва, e.zorin@bmstu.net

¹²⁰ Басараб Михаил Алексеевич, д. ф.-м. н., профессор, МГТУ им. Н. Э. Баумана, m.basarab@bmstu.net

¹²¹ Матвеев Валерий Александрович, д. т. н., профессор, МГТУ им. Н. Э. Баумана, Москва, v.matveev@bmstu.net

исходящий трафик от таких сетей. Возникает вопрос: поможет ли это получить интересующую нас информацию о пользователях? Ведь именно утечка информации из социальной сети, мессенджера, портала для хранения фотографий или поиска работы и т.д. приводит к уязвимости пользователей. Например, приложения Telegram (мессенджер) или Skype хранят всю переписку у себя на серверах.

Уровни защиты

Известно, что повышением уровня защиты можно вызвать отторжение пользователей от продукта. Например, чтобы подписать и зашифровать электронное письмо при помощи PGP (Pretty Good Privacy), требуются специализированное программное обеспечение и навыки. В том же Telegram при регистрации мы обязаны указать мобильный телефон и привязать учётную запись к SIM-карте. Таким образом мы раскрываем свой телефон компании-владельцу социальной сети. Кроме того, SIM-карта привязана к паспорту. Всё это нивелирует основную суть владения личной информацией. На каждом этапе пользователь перестаёт единолично владеть своими данными, загружая их на сервера владельца социальной сети. Это могут быть заметки на iOS, которые автоматически синхронизируются с серверами Apple или Google Drive, у которого в соглашении с пользователем право владения информацией на серверах сохраняется за корпорацией Google.

Шифрование и децентрализация

К первым попыткам можно отнести криптографический мессенджер с открытым исходным кодом Bitmessage, использующий децентрализованную P2P-сеть. Система использует шифрование с открытым ключом, гарантируя получателю единоличное расшифрование. Алгоритм устроен таким образом, что отправитель не сможет расшифровать своё сообщение, так как ключ для шифрования отключается от ключа для расшифрования. Существуют сервисы, позволяющие шифровать информацию, используя алгоритм симметричного шифрования непосредственно в браузере пользователя. Таким образом, информация на сервера сервиса поступает уже зашифрованной. Ниже приведены концепции, которые могли бы разрешить существующие проблемы социальных сетей:

1. Хранение на серверах социальной сети в зашифрованном виде;
2. Процесс шифрования и расшифрования происходит на стороне пользователя в браузере;
3. Использование алгоритма асимметричного шифрования для осуществления приватной передачи информации между пользователями.

Безопасная инфраструктура

Каждый пользователь мог бы иметь публичный и приватный ключ. Когда один пользователь посылает сообщение другому, он использует публичный ключ второго пользователя и зашифровывает им сообщение. Второй пользователь, используя свой приватный ключ, расшифрует сообщение. Конечно, все время носить с собой приватный ключ не удобно, поэтому можно генерировать оба ключа в браузере пользователя, при этом публичный ключ передавать открыто, а приватный ключ, используя симметричное шифрование, передавать в зашифрованном виде, закрытом паролем пользователя. Таким образом, вся деятельность пользователя была бы подписана его приватным ключом, и любой входящий к нему трафик был бы подписан его публичным ключом.

Веб-сервис или приложение

В настоящее время большую популярность получили облачные технологии, и уже большинство сервисов работает через браузер. Но если обратить внимание на сегмент рынка мобильных устройств в интернете, то трудно не заметить, что большинство (около 68%) всех пользователей интернета заходит с мобильных устройств. Любое веб-приложение может по желанию обновить любую свою часть, на время открыть закладку, потом убрать без следов её обратно, обновив лишь небольшой модуль. Причем все это может быть осуществлено практически незаметно. С собранными вручную приложениями это сделать сложнее. Кроме того, можно провести аудит собранного приложения без последующего обновления. Производить же аудит той же онлайн-страницы большого смысла не имеет в силу его многократной необходимости. Отсюда проистекает большая разница в уровне доверия к социальным сетям, особенно если речь идёт о мобильных устройствах. Предлагаемый комплекс сможет реально изменить подход к пользовательской информации.

Выводы

Рассмотренный подход защиты пользовательской информации позволит иначе подойти к

вопросу социального взаимодействия в сети. Его актуальность продиктована спросом на подобные системы, обеспечивающие безопасность социальных сетей. Проблемы окупаемости подобных проектов могут быть решены за счет развития рынка рекламодателей.

Литература

1. Кондратова Е. К. Социальные сети и корпоративная информационная безопасность // Безопасность информационных технологий, ISSN: 2074-7128, 2013.
2. Мехликова А. М., Новоселов М. В. Современное применение компьютерных технологий - Социальные сети. Вопросы информационной безопасности. // Достижения и проблемы современной науки. Уфа, 2015

The Development of a Safe Social Networking Concept

Zorin E.¹²², Basarab M.¹²³, Matveev V.¹²⁴

Annotation. Considered the concept of a secure social network. We analyzed the main insecurity of users in the existing projects of social communication and the available solutions to protect user's information.

Keywords: social networks, security, cryptography.

УДК 004.056

К вопросу о защищенности систем сотовой связи

Завадская Т.Е.¹²⁵

В работе рассмотрены цели, возможные сценарии несанкционированного доступа к системам сотовой связи и обеспечение защиты информации в них.

Ключевые слова: защищенность, системы сотовой связи

Несанкционированный доступ к информации, передаваемой в системах сотовой связи (ССС), имеет целью [1-6]:

- наблюдение за выполнением процессов;
- внесение изменений;
- ликвидацию информации;
- ввод ложной информации;
- задержку;
- запись;
- изменение маршрута;
- дублирование (повторную передачу ранее переданных сообщений).

Обобщенно процесс реализации угроз несанкционированного доступа характеризуется следующим:

- сбором сведений о системе в целом;
- изучением системы защиты информации в СССР и выделением ее слабых мест;
- анализом и разработкой средств воздействия на средства защиты информации на основе новых информационных технологий (преодоление средств защиты происходит там, где злоумышленник имеет более мощные (развитые) информационные технологии);

¹²² Egor Zorin, Bauman Moscow State Technical University, Moscow, e.zorin@bmstu.net

¹²³ Michael Basarab, Dr.Sc (Math), Bauman Moscow State Technical University, Moscow, m.basarab@bmstu.net

¹²⁴ Valeriy Matveev, Dr.Sc, Bauman Moscow State Technical University, Moscow, v.matveev@bmstu.net

¹²⁵ Завадская Татьяна Евгеньевна, МГТУ им.Н.Э.Баумана, t.zavadskaya@bmstu.net

- разработкой средств воздействия на информацию;
- попытками вхождения в сеть, преодолением средств защиты и осуществлением требуемого воздействия на информационный ресурс пользователей сети или общий сетевой ресурс.

Процесс НСД осуществляется в два этапа:

- сбор сведений об ССС и встроенных системах защиты;
- выполнение попыток вхождения в систему.

Сбор сведений в общем случае осуществляется следующими путями:

- подбором соучастников, подслушиванием разговоров, подключением к телефонным аппаратам, телексам;
- изучением утерянных инструкций, документов;
- анализом периодических изданий и документации;
- перехватом сообщений;
- подслушиванием разговоров по телефонам и радиосетям;
- перехватом информации и побочного электромагнитного излучения (включая перехват от дисплейных терминалов и перехват информации с систем спутниковой связи);
- перехватом паролей, ключей;
- организацией краж с целью получения информации для последующего вхождения в ССС;
- вымогательством, подкупом.

После получения необходимого объема предварительной информации осуществляется непосредственное вторжение в ССС.

Чтобы осуществить несанкционированное вхождение в ССС, необходимо иметь доступ к компьютерам (терминала), линиям связи, иметь протоколы работы, описания процедур вхождения в ССС, коды пользователей и пароли.

Целесообразно выдавать как можно меньше информации о самой ССС до момента идентификации пользователя и предоставления ему права доступа в ССС, так как, узнав основной формат вхождения в сеть, лица (субъекты), выполняющие НСД, начинают экспериментировать с различными паролями, вычислять имена и пытаться разрушить защиту.

При несанкционированном доступе идентификаторы пользователя зачастую играют роль вспомогательных средств вхождения в систему, так как их очень легко вычислить. Поэтому их в дальнейшем лучше применять как средства административного контроля и учета.

Непрерывное возрастание динамичности процессов, происходящих в обществе, и существование вызванного этим процессом непрерывного информационного конфликта, обуславливает необходимость защиты информации со стороны тех, кто этой информацией владеет.

Каждая ССС использует свой комплекс мер защиты информации, направленных на сохранение как ее целостности, так и конфиденциальности. При этом эффективность защиты информации от преднамеренных воздействий злоумышленников тем выше, чем меньше злоумышленники знают о применяемых мерах защиты и чем сложнее вскрыть их номенклатуру и параметры (ключи).

Выводы

Многолетнее развитие ССС и существование непрерывного информационного конфликта привело к появлению и совершенствованию различных мер защиты. При этом можно выделить два основных направления защиты информации: защита от ошибок и обеспечение безопасности информации.

Меры по защите от ошибок имеют целью обеспечение доставки информации от

источника сообщений к получателю сообщений в целости и без искажений в условиях воздействия на сигналы непреднамеренных и преднамеренных разрушающих воздействий различного происхождения. К таким мерам относятся:

- помехоустойчивое кодирование - для обнаружения и исправления ошибок;
- перемежение символов - для преобразования групповых ошибок в одиночные, наиболее легко обнаруживаемые и исправляемые;
- обратная связь - для исправления обнаруженных ошибок;
- адаптивная перестройка параметров сигнала - для снижения вероятности ошибки и ухода из-под помех;

Меры обеспечения безопасности информации имеют целью сокрытие содержания передаваемой информации (а по возможности и факта передачи) и недопущение навязывания ложной информации. К таким мерам относятся:

- аутентификация абонентов сети и идентификация их оборудования - для обеспечения работы только с санкционированными корреспондентами;
- шифрование — для сокрытия содержания передаваемых сообщений;
- программная перестройка рабочих параметров сигнала - для сокрытия факта передачи сообщения и его содержания.

В то же время указные специфические меры консолидируются с известными механизмами безопасности в сетевых системах [7].

Литература

1. Средства мобильной связи / Андрианов В. И., Соколов А. В.. СПб.: БХВ - Санкт-Петербург, 2011 г. 256 с.
2. Системы и сети передачи информации / Гаранин М. В., Журавлев С. В., Кунегин С. В. : Учебное пособие для вузов. М.: Радио и связь, 2015 г. 336 с.
3. Стандарты и системы подвижной радиосвязи / Громаков Ю. А.. М: ЭКО-ТРЕНЗ, 2016 г. 242 с.
4. Средства связи для последней мили, Денисьева О. М., Мирошников Д. Г.. М: ЭКО-ТРЕНЗ, 2014 г. 146 с.
5. Защита информации в мобильных системах связи: Учеб. пособие / А. В. Заряев, В. А. Минаев, С. В. Скрыль, В. Ю. Карпычев, А. Н. Обухов, Н. Т. Шевцов, А. М. Гаврилов, Н. Т. Лебедев, И.С. Воронеж: Воронежский ин-т МВД России, 2014 г. 138 с.
6. Петренко А.А., Петренко С.А. Способ повышения устойчивости LTE-сети в условиях деструктивных кибератак // Вопросы кибербезопасности. 2015. №2 (10). С. 36-42.
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.

Научный руководитель и рецензент: Медведев Николай Викторович, канд. техн. наук, доцент, МГТУ им. Н.Э.Баумана, medvedevnick54@yandex.ru

The Issue of Information Security of Systems Cellular Communication Zavadskaja T.¹²⁶

The objectives, possible scenarios of unauthorized access to cellular communication systems and the protection of the information in them are the paper discussed.

Keywords: security, mobile communication system

¹²⁶ Zavadskaja Tatiana E., Bauman MSTU, t.zavadskaya@bmstu.net

Комбинирование форматного и пространственного методов встраивания цифровых водяных знаков в изображения графических форматов JPEG и BMP

Кажемский М.А.¹²⁷

Для встраивания цифровых водяных знаков (ЦВЗ) в изображения формата JPEG был разработан комбинированный алгоритм, который объединяет возможности встраивания больших объемов данных с помощью пространственного метода в формат BMP и сжатия данных с помощью JPEG кодирования. Предложено выражение для оценки количества данных, которое можно скрыть в одном изображении. Приведены количественные оценки качества скрытия стегоданных в изображении. Приведена оценка стойкости алгоритма к атакам на стегоконтейнер.

Ключевые слова: *стеганография, пространственная область изображения, атака, NMSE, PSNR.*

Введение

В результате анализа стенографических алгоритмов на предмет наличия такого метода, который обладал бы возможностью скрывать большие объемы данных в цифровых изображениях (мегабайты), сопоставимый с LSB (Least Significant Bits – Наименее значимых бит), но при этом контейнер с данными имел бы объем меньший, чем изображение в формате BMP (без сжатия), для более удобного обмена стегосообщениями, был сделан вывод об отсутствии такого метода. Из этого был сделан вывод о необходимости разработки алгоритма, который удовлетворял бы вышеупомянутым условиям. В качестве базового формата для исследований и разработок был выбран формат JPEG как наиболее распространенный в сценариях повседневного использования цифровой графики, в частности – цифровых фотографий.

Возможности использования формата JPEG для встраивания метаданных

Анализ структуры формата файлов JPEG [1-3] показывает, что в нем находятся маркеры, определяющие сегменты, которые не влияют на декодирование изображения и поэтому игнорируются программами просмотра. Маркеры, не участвующие в JPEG декодировании представлены в (табл. 1).

Таблица 1.

Маркеры, игнорируемые редакторами

Маркер	Байты	Длина	Назначение
COM	0xFFFE	<i>переменный размер</i>	Комментарий
SOF9	0xFFC9	<i>переменный размер</i>	Начало фрейма (арифметическое кодирование, обычно не поддерживается)
SOF10	0xFFCA	<i>переменный размер</i>	Обычно не поддерживается
DNL	0xFFDC	<i>переменный размер</i>	Может быть проигнорировано
DAC	0xFFCC	<i>переменный размер</i>	Определение арифметической таблицы, обычно не поддерживается
APP15	0xFFEF	<i>переменный размер</i>	Обычно игнорируется

¹²⁷ Кажемский Михаил Андреевич, Московский Технический Университет Связи и Информатики, г. Москва, m.kazhenskiy@gmail.com

Каждый маркер имеет два байта для записи размера маркера (включая эти два байта), то есть максимальный размер маркера может быть 65 535 байт. На основании этого можно сделать вывод о том, что максимальный количество дополнительной информации, которое может быть встроено в неиспользуемые маркеры составляет $(65535 * 6) = 393\,210$ байт.

Форматная составляющая комбинированного метода встраивания ЦВЗ предполагает работу как раз с такими сегментами, а ее использование при создании комбинированного алгоритма позволит решить задачу сокрытия значительных объемов.

Разработка алгоритма внедрения ЦВЗ

Алгоритм предполагает преобразование файла из формата JPEG в формат BMP, затем запись в BMP файл данных по методу наименее значимых бит (НЗБ – LSB – Least Significant Bits) и последующее преобразование файла обратно в JPEG [4, 5]. Для работы алгоритма необходимо было решить ряд проблем, основной из которых является то, что JPEG – формат сжатия с потерями, то есть, если BMP файл преобразовать в JPEG и потом обратно, то на выходе нельзя получить не искаженное исходное сообщение, а значит невозможно достоверное извлечь информацию. Для этого был разработан алгоритм компенсации потерь при межформатных преобразованиях вида JPEG-RGB_BMP-JPEG. Последовательность процесса внедрения сообщения представлена на (рис. 1).

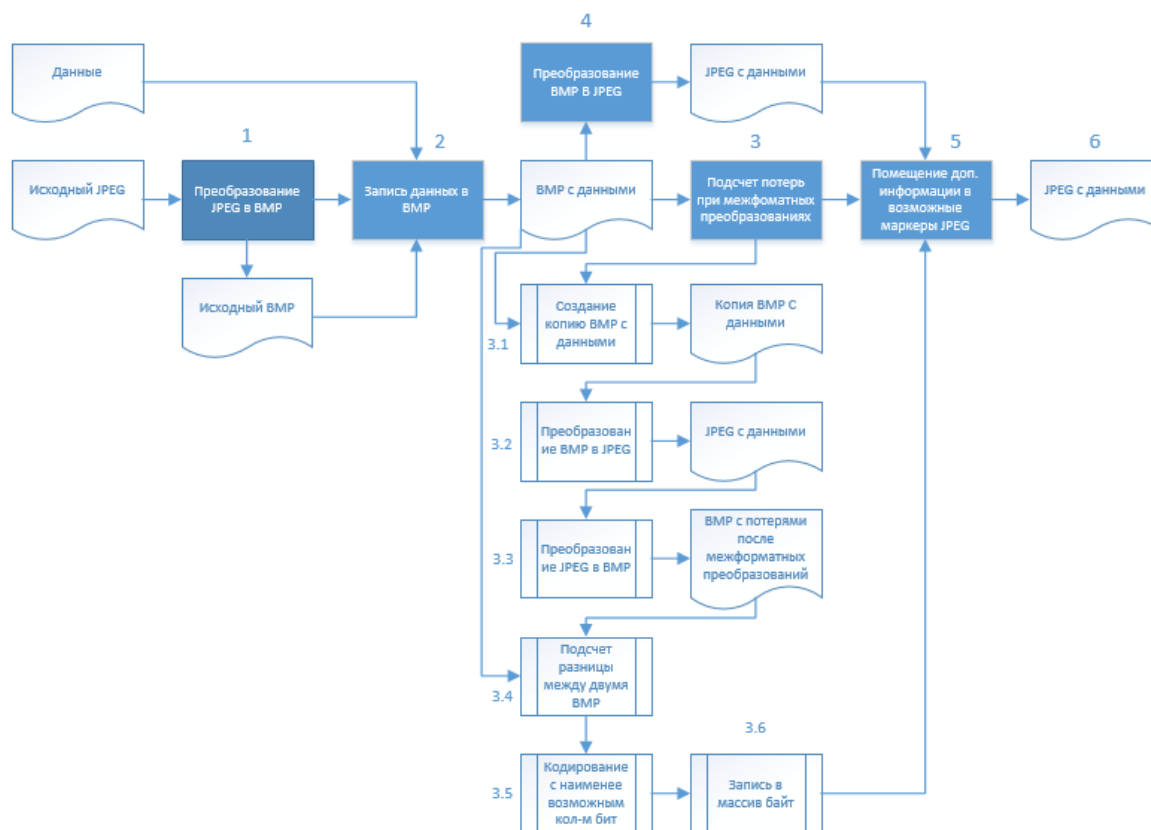


Рис. 1 Алгоритм скрытия данных поэтапно

На первом этапе, при формировании стегопосылки происходит преобразование исходного изображения формата JPEG в BMP, в котором каждый пиксель изображения кодируется с помощью трех байт. Каждый из байтов отвечает за один из трех потоков основных цветов – **R** (RED – красного), **G** (GREEN – зеленого) и **B** (BLUE – синего), формирующих RGB структуру. При этом, благодаря тому, что изображение формата BMP имеет больший размер по сравнению с JPEG, максимальный объем данных для скрытия тоже увеличивается.

На втором этапе происходит встраивание данных в синюю составляющую ВМР изображения по методу НЗБ, предполагающему замену младших бит каждого байта потока исходного изображения на биты из потока скрываемых данных как это показано на (рис.2).

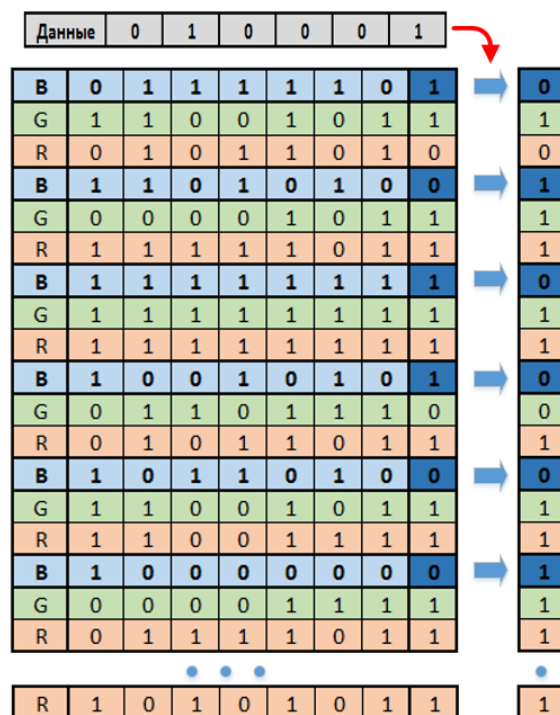


Рис. 2 Принцип работы метода НЗБ

На третьем этапе осуществляется подсчет разницы межформатных потерь при заданном качестве преобразования ВМР-JPEG (**quality**),

Вычисление минимально необходимого числа бит для кодирования каждого элемента массива осуществляется по формуле:

$$K = \text{ceil}(\log_2(\max(mas) - \min(mas))) + 1, \quad (1)$$

где: **ceil** – функция округления для ближайшего большего целого, **mas** – массив разностей.

На четвертом этапе происходит преобразование ВМР изображения в JPEG. И на пятом этапе происходит запись вспомогательной информации в игнорируемые маркеры JPEG.

Оценка эффективности алгоритма внедрения ЦВЗ

Для подсчета количества данных, которое можно скрыть в одном изображении предлагается использовать соотношение

$$N_{data} = (w \cdot h - \text{const}) \cdot \frac{n_{\text{бит}}}{i}, \quad (2)$$

где N_{data} – количество бит информации, которую можно скрыть в одном изображении; w, h – ширина и высота исходного изображения в пикселях; i – интервал скрывания (интервал, через которые берутся пиксели для записи); $n_{\text{бит}}$ – глубина скрывания (количество используемых бит в потоке для записи информации). **const = 14** – характеризует количество пикселей для записи служебной информации

Количественная оценка качества скрывания

На (рис.3) Приведены сводные количественные оценки качества скрывания стегоданных в изображении для разных параметров **quality** (качество) преобразования ВМР->JPEG. Оценка проводилась с помощью разработанного универсального комплекса для исследования алгоритмов скрывания данных.

Качество	100%			95%			85%			75%		
Глубина скрытия	2											
Плотность скрытия	1											
	ЦВЗ есть	ЦВЗ нет	Разность	ЦВЗ есть	ЦВЗ нет	Разность	ЦВЗ есть	ЦВЗ нет	Разность	ЦВЗ есть	ЦВЗ нет	Разность
Количество бит для кодирования межформатных преобразований	4 бит	-	-	7 бит	-	-	8 бит	-	-	8 бит	-	-
Размер информации в маркерах	19,54 Кбайт	-	-	34,19 Кбайт	-	-	39,07 Кбайт	-	-	39,07 Кбайт	-	-
Размер jpeg файла с информацией в маркерах	468,91 Кбайт	-	-	195,89 Кбайт	-	-	109,31 Кбайт	-	-	87,52 Кбайт	-	-
Среднеквадратичная ошибка	0,32515	0,11934	0,20581	10,39707	10,28198	0,11509	19,86811	19,82519	0,04292	25,16902	25,13227	0,03675
Норм. среднеквадратичная ошибка	0,00002	0,00001	0,00001	0,00052	0,00052	0	0,001	0,001	0	0,00126	0,00126	0
Отношение сигнал/шум	47,87276	52,22586	-4,35310	32,82443	32,87277	-0,04834	30,01197	30,02137	-0,0094	28,98488	28,99122	-0,00634
Максимальное отношение с/ш	53,01002	57,36312	-4,35310	37,9617	38,01004	-0,04834	35,14924	35,15863	-0,00939	34,12214	34,12849	-0,00635

Рис.3 Сводные данные.

Как видно из (рис.3) основные параметры оценки (MSE, NMSE, SNR, PSNR) ухудшались в большей степени из-за снижения качества полученного изображения, и лишь в малой степени зависело от встроенных данных.

Атаки на стегоалгоритм.

В работе были произведены атаки на алгоритм, направленные на преобразование стегоконтейнера [6] с помощью разработанного универсального программного [7] комплекса для исследования стегоалгоритмов (атаки проводились на промежуточное BMP изображение):

- Жpeg сжатие с разными коэффициентами сжатия.
- Поворот изображения против часовой стрелки на заданный угол
- Обрезка изображения на заданное количество пикселей справа и снизу
- Зашумление изображения разными методами:
 - Гауссов белый шум с математическим ожиданием 0 и разными значениями дисперсии
 - Мультипликативный (speckle) шум также с разными параметрами дисперсии
 - Шум «Соль и Перец» (salt&pepper) с разными значениями плотности шума
- Фильтрация изображения разными методами:
 - Фильтр «размытие по Гауссу» с разными значениями радиуса размытия
 - Медианный фильтр с различными размерами матриц

Исходные данные для атаки представлены на (рис. 4) - bmp изображение (слева), размером 512 x 512 с глубиной цвета 24 бит, содержащее в себе ЦВЗ (справа) в формате QR кода, размером 276 x 276 с глубиной цвета 1 (монохромное).

Данные внедрены с глубиной скрытия 2 и плотностью скрытия 1.



Рис. 4 Извлеченные данные без проведенных атак

Выводы

Таким образом был разработан стенографический алгоритм скрытия большого объема данных в небольших по объему изображениях (на порядок меньший, чем изображения без сжатия), с эффективностью, сравнимой с встраиванием данных по алгоритму LSB в изображения формата BMP. В результате оценки качества внедряемой информации был сделан вывод о возможности встраивания большого объема стегоданных в изображения без изменения визуальной составляющей изображения – то есть не заметной человеческому глазу. В результате анализа атак на стегоалгоритм был сделан вывод о низкой способности алгоритма противостоять атакам на стегоалгоритм.

В итоге, можно сделать вывод о том, что разработанный алгоритм подходит для скрытия и обмена данными, при условии, что пользователи будут передавать сообщения напрямую, т.е. изображение не будет изменено в период доставки сообщения от одного пользователя до другого.

Литература

1. Poonam V.B., Baisa L.G, Improved Protection In Video Steganography Using DCT & LSB // International Journal of Engineering and Innovative Technology (IJEIT), vol 1.4, 2012
2. Трегулов Т.С. , Скрытая передача данных в цифровых изображениях формата JPEG // Научные труды SWorld. 2012. Т. 4. № 2. С. 88-91.
3. Чекасин А.И., Стрельцов Е.В., Поташникова А.В., Учет особенностей формата JPEG при стеганографическом кодировании // Известия высших учебных заведений. Электроника. 2009. № 4 (78). С. 61-65.
4. Кувшинов С.С., Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии: автореферат диссертации на соискание ученой степени кандидата технических наук // Санкт-Петербургский государственный университет информационных технологий, механики и оптики. Санкт-Петербург, 2010
5. Коробейников А.Г., Кувшинов С.С., Блинов С.Ю., Лейман А.В., Нестеров С.И., Разработка стеганоалгоритма на базе форматных и пространственных принципов сокрытия данных // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 1 (77). С. 116-119.
6. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – М.: Солон-Пресс, 2009. – 272 с.

7. Шелухин О.И., Кажмский М.А., Разработка программного комплекса для исследования стеганографических алгоритмов скрытия информации // В сборнике: Телекоммуникационные и вычислительные системы Труды конференции. 2015. С. 161.

Научный руководитель: Шелухин Олег Иванович, профессор, д-р техн. наук, Заведующий Кафедрой «Информационная безопасность», Московский Технический Университет Связи и Информатики, г. Москва, ул. Авиамоторная, д. 8а, sheluhin@mail.ru

Combining of Format and Spatial Methods of Embedding Digital Watermarks in Images of JPEG & BMP graphic formats
M. Kazhenskiy¹²⁸

The combined algorithm which integrates possibilities of embedding of large volumes of data with the help of a spatial method in the BMP format and JPEG data compressions has been developed for embedding the digital watermarks in images of the JPEG format. Expression for measuring data volume which can be hidden in one image has been offered. The quality of stegodata embedding has been estimated. Algorithm resistant to attacks on stegocontainer asses has been done.

Keywords: steganography, spatial domain of the image, attack, NMSE, PSNR.

¹²⁸ Mikhail A. Kazhenskiy, Moscow Technical University of Communications and Informatics, Department of "Information Security", m.kazhenskiy@gmail.com

Рассмотрен способ разведывательного цикла, основанный на декомпозиции данных и связей между данными, касающимися конкретного человека или события. Предложена циклическая модель сбора и анализа информации, позволяющая уточнять данные и связи между данными. Разработана формальная модель, позволяющая эксперту выполнять обоснованный последовательный поиск информации.

Ключевые слова: открытые источники, структурированный анализ, разведывательный цикл, социальные сети, деловая разведка, бизнес-разведка

Введение

В настоящее время социальные медиа являются исключительным источником открытой информации о людях и происходящих событиях [1-4]. Наличие информации в открытых источниках позволяет многое узнать о конкретной персоне еще до возникновения каких-либо отношений с человеком. Однако разрозненность и динамичность данных в сети интернет, неопределенность и неустойчивость связей между объектами и событиями, усложняют получение достоверного целевого результата. Применение общесистемного подхода в некоторых случаях связано с временными издержками по причине необходимости обработки чрезвычайно большого количества информации [5]. Для исключения указанных недостатков в докладе демонстрируется структурированный поэтапный анализ информации, ориентированный на целенаправленное получение достоверных знаний о конкретном человеке или событии [6].

Понятие структурированного анализа

Под структурированным анализом (structured analysis) мы будем понимать экспертный целенаправленный пошаговый подход к сбору и обработке данных и связей между данными, позволяющий получить максимально полную и достоверную информацию о конкретном человеке или событии. В некотором смысле, в рамках структурированного анализа выполняется преобразование неясных знаний о данных и связях данных в точные, путем декомпозиции (структуризации) данных и связей между ними [6, 7]. Традиционно анализ информации включает начальный этап (определение источников, сбор и оценка априорных данных) и последующие итерационные шаги по обработке (анализ, формулировка выводов, формирование гипотез) данных в целях получения максимально объективной и полной информации.

Обеспечение полноты и непротиворечивости анализа обеспечивается соответствующей классификацией открытых источников данных.

Разведывательный цикл

С учетом целевой задачи и ее контекста первичную информацию о человеке можно условно представить кортежем:

$$D = \{Gn, Rl, Cn, Ph, Jb, Ed, Ml, Zn, Hb, Sp, Ow, Ot\},$$

который включает множества общей идентификационной информации Gn, семейных отношений Rl контактной информации Cn физических данных Ph, данных о работе Jb, образовании Ed, отношении к военной службе Ml, приятельским окружении Zn, хобби Hb, спорте Sp, частной собственности Ow, специальной информации Ot, особенно проблемной. Определение подмножеств и их допустимых значений легко детализировать, например, для случая программной реализации [6, 10].

¹²⁹ Дорофеев Александр Владимирович, CISSP, директор по развитию АО «НПО «Эшелон», Москва, mail@uc-echelon.ru

Полученная выше информация о том, где и какую информацию в принципе можно найти, по сути представляет для нас первичную карту знаний, а структурированные техники анализа создают маршрут движения по ней. Известны несколько структурных моделей сбора и анализа информации о человеке или событии¹³⁰. На наш взгляд, удобно воспользоваться предлагаемой ниже 7-ми процессной циклической моделью [6].

Предлагаемая модель включает следующие последовательные временные процессы (этапы):

1. Постановка проблемы, в рамках чего формулируется набор вопросов (задач), на которые необходимо найти ответы;
2. Планирование, в ходе которого определяются методические приемы к поиску и анализу данных;
3. Сбор данных, в ходе которого осуществляется непосредственное получение первичной информации относительно тех объектов исследования, которые были определены на предыдущем этапе;
4. Обработка данных, которая позволяет извлечь полную информацию для анализа (например, по ранее выявленным фотографиям можно определить временные и геометки);
5. Анализ информации, который нацелен на поиск ответов на поставленные вопросы (решение задач);
6. Разработка отчета, в ходе которого формулируются выводы, рекомендации, приводятся подтверждающие свидетельства;
7. Распространение информации, которая предполагает презентацию результатов заинтересованным лицам (заказчику).

Концептуальная модель цикла может быть следующей:

$$M = \{S1, S2, S3, S4, S5, S6, S7, R1, R2, R3\},$$

где: S1 – множество вопросов, S2 – упорядоченное множество источников, S3 – множество полученных данных, S4 – множество данных, извлеченных в результате декомпозиции, S5 – множество ответов на вопросы, S6 – множество выводов, S7 – множество выводов в визуальном виде, $R1: S1 \cup S2 \rightarrow S3$, $R2: S3 \rightarrow S4$, $R3: S1 \cup S3 \cup S4 \rightarrow S5$.

Данная модель предполагает дальнейшее структурирование всех указанных процессов:

Заключение

В работе предложен методический подход к проведению структурированного анализа, позволяющий путем пошаговой декомпозиции данных и связей между данным обеспечить максимальное получение значимых данных о человеке в приемлемое время. В основу метода предложено использовать так называемый разведывательный цикл сбора и анализа информации и метод тестирования альтернативных гипотез.

К достоинству структурированного анализа следует отнести то, что он не налагает ограничений на применение любых экспертных техник анализа и использования каких-либо дополнительных информационных источников.

Предложенный подход имеет непосредственное прикладное значение, в работе показаны реальные примеры получения целевой информации как о субъектах, так и объектах исследования. Данный подход может использоваться для реализации контрмеры по проверке персонала, внедряемого в рамках реализации системы менеджмента ИБ в соответствии с требованиями стандарта ISO/IEC 27001:2013 [11].

Литература

1. 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

¹³⁰ Intelligence Cycle. FBI. 2015. <https://www.fbi.gov/about-us/intelligence/intelligence-cycle>.

(обзор) // Вопросы кибербезопасности. 2016. № 4 (17). С. 11-19.

2. Лыфенко Н.Д. Виртуальные пользователи в социальных сетях: мифы и реальность // Вопросы кибербезопасности. 2014. № 5 (8). С. 17-20.

3. Ненашев С.М. Информационно-технологическая и информационно-психологическая безопасность пользователей социальных сетей // Вопросы кибербезопасности. 2016. № 5 (18). С. 65-72.

4. Сазонов М.А., Потемкин А.В. Исследование механизмов информационных воздействий на систему средств массовой информации // Вопросы кибербезопасности. 2016. № 3 (16). С. 55-59.

5. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41-53.

6. Петренко А.С., Петренко С.А. Технологии больших данных (BigData) в области информационной безопасности // Защита информации. Инсайд. 2016. №4 (70). С. 82-88.

7. Dorofeev A., Markov A., Tsirlov V. Social Media in Identifying Threats to Ensure Safe Life in a Modern City // Communications in Computer and Information Science. 2016. V. 674. P. 441- 449.

8. Пилькевич С.В., Еремеев М.А. Модель социально значимых интернет-ресурсов // Труды СПИИРАН. 2015. № 2. С. 62-83.

9. Bershadskaya L., Chugunov A., Trutnev D. Information Society development in Russia: Measuring progress and gap. In Proceedings of the 1st Conference on Electronic Governance and Open Society: Challenges in Eurasia (St Petersburg, Russia, November 18-20, 2014). EGOSE 2014. ACM New York, NY, USA, pp. 7-13 DOI=<http://dx.doi.org/10.1145/2729104.2729122>.

10. Dorofeev A., Markov A., Tsirlov V. Structured Approach to the Social Network Analysis of Information About a Certain Individual. In Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia (St Petersburg, Russia, November 24-25, 2015). EGOSE '15. ACM New York, NY, USA, 2015, pp. 174-178. DOI: 10.1145/2846012.2846017.

11. 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.

Научный руководитель: Марков Алексей Сергеевич, д-р техн. наук, ст. научн. сотр., профессор МГТУ им.Н.Э.Баумана, Москва, a.markov@bmstu.ru

Applied Questions of The Social Network Analysis **Dorofeev A.V.¹³¹**

The way of the intelligence cycle, based on data decomposition and relationships between the data relating to a specific person or event is considered. The cyclic model of the collection and analysis of information, which allows to specify data and relations between data is proposed. The formal model, which allows the expert to perform a reasonable search for the serial data is developed.

Keywords: structured analysis, intelligence cycle, social networking, business intelligence

УДК 004.056

Формально-вербальная модель противодействия угрозам информационной безопасности **Зырянов Е.А.¹³²**

В статье рассмотрена задача обеспечения информационной безопасности автоматизированных систем. Представлен обзор вербального описания модели защиты от несанкционированного доступа. Произведен анализ достаточной прочности защиты и показателей, определяющих вероятность несанкционированного доступа.

Ключевые слова: достаточная прочность преграды, автоматизированная преграда

¹³¹ Alexander Dorofeev, CISSP, NPO Echelon, Moscow, mail@uc-echelon.ru

¹³² Зырянов Евгений Алексеевич, МГТУ им. Н.Э. Баумана, г. Москва, evgenyalexeevich@gmail.com

Введение

Важнейшие этапы проектирования систем защиты информации (СЗИ) от несанкционированного доступа (НСД) основаны на модели противодействия угрозам информационной безопасности. Правильно разработанная модель является гарантией построения адекватной системы обеспечения информационной безопасности. Опираясь на построенную модель, уже можно строить адекватную систему информационной защиты. Существующие в настоящее время модели реализации угроз НСД базируются в основном на вербальном описании.

Модель противодействия угрозам информационной безопасности.

В реальных задачах обеспечения информационной безопасности автоматизированных систем очень важны вербально-формальные модели [1]. Подход к формализации отражен на рисунке 1:

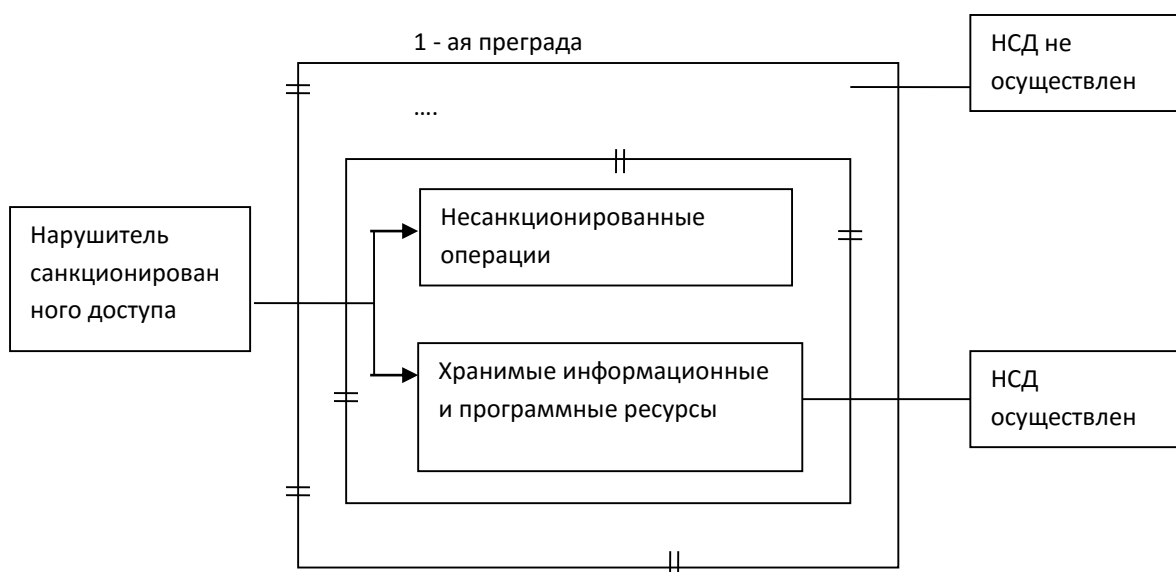


Рис 1. Схема элементарной защиты

Модель элементарной защиты представлена на рис.2. Вокруг защищаемой информации выстраивается замкнутый защитный контур [2].

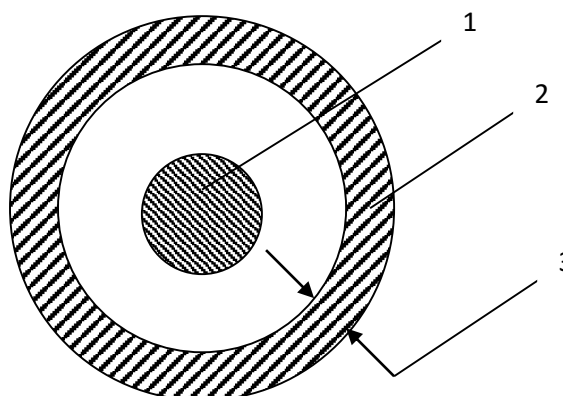


Рис 2. Модель элементарной защиты: 1- предмет защиты: 2- преграда: 3 – прочность преграды.

Оценка прочности защиты преграды.

Прочность защиты зависит от свойств преграды. Принципиальную роль играет способность преграды противостоять попыткам преодоления её нарушителем.

Для определения достаточной прочности преграды существует два подхода [2, 3]:

1. Если стоимость затрат на преодоление преграды превышает стоимость защищаемой информации, то считается, что прочность созданной преграды достаточна;
2. Если затраты времени на преодоление преграды превышают время жизни информации, то прочность созданной преграды достаточна.

Введём обозначения.

$P_{СЗИ}$ - вероятность непреодоления преграды;

$t_{жс}$ - время жизни информации;

t_n - ожидаемое время преодоления преграды нарушителем;

$P_{обх}$ - вероятность обхода преграды.

Для 2 - го случая имеем следующее:

$P_{СЗИ} = 1$ если $t_{жс} < t_n$ и $P_{обх} = 0$

$P_{обх} = 0$ отражает замыкание преграды вокруг предмета защиты.

Если $t_{жс} > t_n$ и $P_{обх} = 0$, то

$$P_{СЗИ} = (1 - P_{нр}), \quad (1)$$

где: $P_{нр}$ - вероятность преодоления преграды нарушителем за время, меньшее $t_{жс}$.

В реальных условиях $t_{жс} > t_n$ и $P_{обх} > 0$. Соответственно прочность защиты определяется по формуле:

$$P_{СЗИ} = (1 - P_{нр}) \cup (1 - P_{обх1}) \cup \dots \cup (1 - P_{обхK}), \quad (2)$$

где: $P_{нр} = 0$, если $t_{жс} < t$; $P_{нр} > 0$, если $t_{жс} \geq t$;

k - число путей обхода преграды.

Выбор и определение конкретной величины $P_{обх}$ сначала можно проводить экспертным путём на основе опыта специалистов [3]. Величина $P_{обх}$ должна принимать значения от 0 до 1. При $P_{обх} = 1$ защита теряет всякий смысл.

В ситуациях, когда информация, подлежащая защите, не устаревает или периодически обновляется, т.е. когда $t_{жс} > t_n$, применяется постоянно действующая преграда, обладающая свойствами обнаружения и блокировки доступа нарушителя к предмету или объекту защиты. В качестве такой защиты может быть применены человек или специальная автоматизированная система обнаружения под управлением человека.

Принцип работы автоматизированной преграды основан на том, что в ней блоком управления производится периодически контроль датчиков обнаружения нарушителя [4]. Результаты контроля наблюдаются человеком.

Выводы

Произведен анализ достаточной прочности защиты. Представлены формулы расчета прочности защиты и вероятности преодоления преграды. Описаны показатели, влияющие на вероятность несанкционированного доступа.

Литература

1. Клейнрок Л. Вычислительные системы с очередями. - М.: Мир, 1979. - 600 с.
2. Медведев Н.В. Исследование процесса функционирования информационных каналов мобильных робототехнических комплексов. // Электромагнитные волны и электронные системы. - 2015. - № 8. - с. 29-36.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. — М.: Гелиос АРВ, 2013. — 480 с.

Научный руководитель: Медведев Николай Викторович, к.т.н., доцент кафедры ИУ8 МГТУ им. Н.Э. Баумана

Formal-Verbal Model of Countering Threats to Information Security
Zyryanov E.A.¹³³

The article considers the problem of ensuring information security of computer systems. Presents an overview of the verbal description of a protection model against unauthorized access. The analysis of sufficient strength protection and the determinants of the probability of unauthorized access.

Keywords: Information security, Protection from unauthorized access, sufficient strength of obstacles, automated barrier.

УДК 004.056.57

Подход к построению формальной модели функционирования процесса в операционной системе
Козачок А.В.¹³⁴, **Кочетков Е.В.**¹³⁵

В статье представлена формальная модель функционирования процесса в операционной системе, построенная на основе субъектно-объектного подхода. Ее особенностью является высокоуровневая абстракция взаимодействия между процессом и ресурсами системы, что позволяет произвести описание функционирования процесса для широкого класса операционных систем. Дано определение ряда понятий, необходимых для описания модели: описание функционирования процесса, аксиома безопасного исполнения программного кода, модель безопасного исполнения программного кода, свойство безопасности исполнения программного кода.

Ключевые слова: формальная модель, процесс, Model Checking, вредоносное программное обеспечение.

Введение. В последние несколько лет особое внимание в исследованиях, посвященных защите информации, уделяется вопросу, касающемуся обеспечения информационной безопасности корпоративных информационно-вычислительных сетей (КИВС). Эти исследования касаются, главным образом, формальной верификации свойств безопасности. Основной целью при этом является разработка формальной математической модели свойств безопасности системы, а также верификация этой модели с помощью математических доказательств.

В настоящее время основным средством обнаружения вредоносного программного обеспечения (ВПО) в информационной инфраструктуре организации являются антивирусные средства (АВС). Исследования показывают, что реализованные в них механизмы обнаружения ВПО позволяют достичь вероятностей ошибок первого и второго

¹³³ Zyryanov Evgeniy Alekseevich, Bauman Moscow State Technical University, Moscow, evgenyalekseevich@gmail.com

¹³⁴ Козачок Александр Васильевич, к.т.н., Академия ФСО России, г. Орёл, alex.totrin@gmail.com

¹³⁵ Кочетков Евгений Викторович, Академия ФСО России, г. Орёл, mr.koch91@mail.ru

рода, близких к нулю. Однако даже при вероятности обнаружения равной 0,974 (Avast Internet Sefurity) остаются необнаруженными 467 образцов ВПО, что создает непосредственную угрозу информационной безопасности всей организации в целом, так как проникновение даже одной программы с вредоносным содержимым в КИВС может нанести ей существенный ущерб [1].

Применяемые в большинстве современных АВС способы обнаружения ВПО обладают рядом принципиальных ограничений, которые значительно снижают эффективность обнаружения вредоносных программ, использующих техники защиты от обнаружения: полиморфизм, метаморфизм, шифрование и упаковка кода [2, 3]. В связи с этим фактом рядом исследователей в области защиты от ВПО (Trilling S., Nachenberg C., Morales J.A., Clarke P.J., Deng Y. и др.) было сделано предположение, суть которого заключается в том, что достаточно легко изменить бинарное представление исполняемого файла, но намного сложнее изменить поведение вредоносной программы в целом. Взяв за основу данное предположение, ими был предложен новый подход к обнаружению ВПО на основе анализа поведения программы в операционной системе (ОС). Данный подход, по мнению авторов настоящей статьи, является наиболее перспективным, так как позволяет преодолеть ряд ограничений существующих методов обнаружения ВПО и повысить защищенность КИВС в целом.

Формальная модель функционирования процесса в ОС. Суть предлагаемого метода заключается в извлечении информации о поведении исследуемой программы, как на этапе хранения, так и на этапе исполнения. Полученная информация сравнивается со спецификацией описания поведения в соответствии с заданными функциональными требованиями. В случае их соответствия исследуемая программа признается безопасной [4, 5].

Из описания данного подхода следует, что для его реализации на практике необходимо решение следующих частных задач:

- анализ (извлечение и преобразование информации из исследуемой программы в вид, пригодный для дальнейшей обработки – спецификации);
- синтез (построение модели безопасного исполнения программного кода в соответствии с заданными функциональными требованиями);
- верификация (алгоритм, получающий на вход спецификацию анализируемой программы и принимающий решение о ее соответствии модели безопасного исполнения программного кода).

Для решения задачи верификации предлагается применять метод автоматической формальной верификации "Model Checking" [6, 7]. Для решения двух первых задач необходимо построение модели, позволяющей произвести формальное описание функционирования процесса в ОС.

Базовыми понятиями при рассмотрении работы ОС являются процесс и ресурс. Согласно [8, с. 22] процесс это контейнер для набора ресурсов, используемых при выполнении экземпляра программы. К основным видам ресурсов ОС относятся следующие элементы [9, с. 42-46]:

- процессорное время;
- оперативная память;
- внешняя память;
- устройства ввода-вывода.

Прикладные программы не имеют прямого доступа к ресурсам ОС, а получают к ним доступ только с помощью интерфейса прикладного программирования (Application Programming Interface) или системных вызовов.

В основе построения предложенной модели функционирования процесса лежит

принцип разделения всех взаимодействующих элементов ОС на субъекты и объекты. К субъектам относятся процессы, совершающие действия по отношению к объектам. Объектами являются ресурсы ОС и процессы в отношении которых совершаются действия другими субъектами:

- "Процесс" (P);
- "Оперативная память" (M);
- "Внешняя память" (E);
- "Периферийные устройства" (D);
- "Сетевая подсистема" (N).

Определение 1. Под описанием процесса в ОС S_i будем понимать последовательность действий $\{S_i\}_{i \in \mathbb{N}}$ выполняемых субъектом $p_i^{k_p}$. Каждое действие описывается тройкой элементов:

$$s_i = \langle p_i^{k_p}; a_o; o_y^{k_o} \rangle, \quad (1)$$

где: $p_i^{k_p}$ – субъект категории k_p с идентификатором i ; $a_o \in A_o$ – некоторое действие субъекта по отношению к объекту; $o_y^{k_o}$ – некоторый объект категории k_o с идентификатором y .

Операторное представление выражения 1 имеет следящий вид:

$$s_i = p_i^{k_p} \xrightarrow{a_o} o_y^{k_o}, \quad (2)$$

Определение 2. Под аксиомой безопасного исполнения программного кода AX будем понимать описание параметров разрешенных действий $\{S_k\}_{k \in \mathbb{Q}}$ для процесса $p_i^{k_p}$ во время его функционирования S_i , позволяющее исключить потенциальную возможность выполнения программой вредоносных действий:

$$AX_j = \bigcup_k S_k, k \in \mathbb{Q}_j, \quad (3)$$

где: $\mathbb{Q}_j$ – множество индексов безопасных действий для процесса $p_i^{k_p}$ при заданных функциональных требованиях FR_j .

Пример задания аксиомы "Запрет на создание пользовательским процессом привилегированного или системного процесса" представлен в выражении 4:

$$AX_j = \neg EF \left[p^3 \xrightarrow{c} p^2 \right] \vee \neg EF \left[p^3 \xrightarrow{c} p^1 \right]. \quad (4)$$

Определение 3. Моделью безопасного исполнения программного кода SM будем называть совокупность аксиом безопасного исполнения программного кода AX_j для процесса $p_i^{k_p}$ при заданных функциональных требованиях FR :

$$SM = \bigcup_{j \in M} AX_j |_{FR = \bigcup_{j \in M} FR_j}, \quad (5)$$

где: M – множество индексов аксиом безопасного исполнения программного кода, выбранных с учетом функциональных требований FR .

Схематичное представление модели функционирования процесса в ОС представлено на рисунке 1.

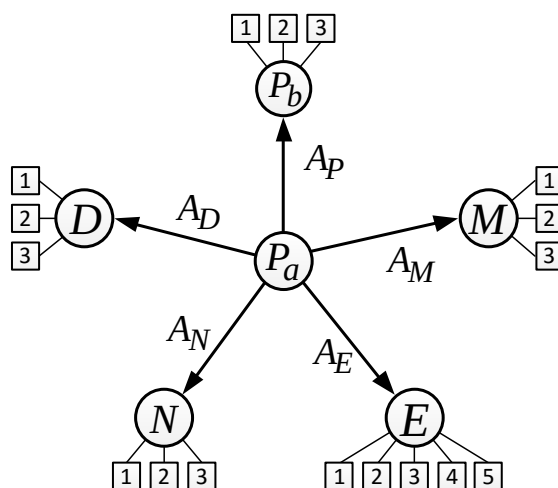


Рис. 1. Модель взаимодействия процесса с ресурсами ОС

Главным достоинством описываемой модели функционирования процесса в ОС является возможность описания функционирования процесса на высоком уровне абстракции, что позволяет применять полученные на ее основе выводы к широкому классу операционных систем.

Представление событий функционирования процесса в ОС в рамках предложенной модели позволяет описать его поведение на языке формальной логики и в дальнейшем применить метод автоматической формальной верификации "Model Checking" для доказательства соответствия спецификации заданным требованиям. Подробно данный процесс описан в [10].

Выводы. В настоящей статье предложена формальная модель функционирования процесса в ОС, построенная на основе применения субъектно-объектного подхода. Она позволяет описать поведение процесса в ОС без конкретизации операций или элементарных действий, на высоком уровне абстракции. Направлением дальнейших исследований является практическая реализация и экспериментальная проверка качества предложенной модели с применением метода "Model Checking".

Литература

1. Бекбосынова А.А. Тестирование и анализ эффективности и производительности антивирусов // Теория и практика современной науки. 2015. № 5 (5). С. 53-56.
2. Козачок А.В. Распознавание вредоносного программного обеспечения на основе скрытых марковских моделей: диссертация ... кандидата технических наук: 05.13.19. — Воронеж, 2012. — 209 с.
3. Sharma P., Kaur S., Arora J. An Advanced Approach to Polymorphic/Metamorphic Malware Detection using Hybrid Clustering Approach. — 2016.
4. Morales J. A., Clarke P. J., Deng Y. Identification of file infecting viruses through detection of self-reference replication // Journal in computer virology. — 2010. — Т. 6. — №. 2. — С. 161-180.
5. Liang G., Pang J., Dai C. A Behavior-Based Malware Variant Classification Technique // International Journal of Information and Education Technology. — 2016. — Т. 6. — №. 4. — С. 291.
6. Battista P. et al. Identification of android malware families with model checking // International Conference on Information Systems Security and Privacy. SCITEPRESS. — 2016.
7. Garcia-Ferreira I. et al. A survey on static analysis and model checking // International Joint Conference SOCO. — 2014. — С. 443.
8. Русинович М., Соломон Д. Внутреннее устройство Microsoft Windows. 6-е изд. — СПб.: Питер, 2013. — 800 с.
9. Гордеев А. В. Операционные системы:[по направлению подгот."Информатика и вычисл. техника"]. — Издательский дом "Питер", 2009.
10. Козачок А.В., Кочетков Е.В. Обоснование возможности применения верификации программ для обнаружения вредоносного кода // Вопросы кибербезопасности. 2016. № 3 (16). С. 25-32.

Formal Model of Functioning Process in the Operating System

A.V. Kozachok¹³⁶, E.V. Kochetkov¹³⁷

The article presents new process functioning formal model in operating systems, based on subject-object approach. Its main advantage is in high-level abstraction of interaction between operating system processes and resources. The paper provides definitions of some concepts: process functioning description, secure code execution axiom, secure code execution model, code execution security property.

Keywords formal model, process, Model Checking, malware.

УДК 004.056.55

Обобщённые клеточные автоматы, как основа для построения функций формирования ключа

Ключарёв П.Г.¹³⁸

Работа выполнена при поддержке РФФИ (проект №16-07-00542).

Работа посвящена рассмотрению некоторых особенностей использования обобщенных клеточных автоматов для построения функций формирования ключа. Предложена концепция построения таких функций на основе обобщенных клеточных автоматов большого размера, что существенно затрудняет их обращение путем перебора на параллельных вычислительных архитектурах¹³⁹.

Ключевые слова: обобщенный клеточный автомат, функция формирования ключа, хэш-функция

Введение

Среди хэш-функций особое место занимают так называемые функции формирования ключа (Key Derivation Function, KDF), предназначенные, в первую очередь, для формирования ключевой информации из паролей. Они представляют собой криптографические хэш-функции, обладающие дополнительными свойствами, затрудняющими восстановление паролей методом грубой силы, такими как низкая способность к распараллеливанию и относительно высокая вычислительная сложность. Одной из наиболее известных таких функций является функция `scrypt` [5], в которой распараллеливание существенно затрудняется высокой пространственной сложностью алгоритма.

Функции формирования ключа находят большое применение не только в задачах выработки криптографических ключей, но и в системах парольной аутентификации, в различных криптографических протоколах [4; 6], в алгоритмах `proof-of-work` систем электронной валюты (например, `LiteCoin`) и т.п.

Обобщенные клеточные автоматы

Получить хорошую KDF можно с помощью разработанных автором методов построения криптоалгоритмов на основе обобщенных клеточных автоматов [1; 2]. В

¹³⁶ Kozachok Alexander Vasilevich, Ph.D., The Academy of Federal Security Guard Service of the Russian Federation, Orel, alex.totrin@gmail.com

¹³⁷ Kochetkov Evgeniy Victorovich, The Academy of Federal Security Guard Service of the Russian Federation, Orel, mr.koch91@mail.ru

¹³⁸ Ключарёв Петр Георгиевич, к.т.н., доцент МГТУ им. Н.Э. Баумана, pk.iu8@yandex.ru

¹³⁹ Работа выполнена при поддержке РФФИ (проект №16-07-00542)

частности, способ построения хэш-функций был предложен автором в работе [3]. Такие хэш-функции основаны на обобщенных клеточных автоматах, представляющих собой ориентированный мультиграф $A = (V, E)$ (здесь $V = \{v_1, \dots, v_N\}$ – множество вершин, E – мультимножество ребер). Каждой его вершине v_i соответствует булева переменная m_i (будем называть ее ячейкой). С графом ассоциирована булева функция $f(x_1, \dots, x_d)$, называемая локальной функцией связи. При этом для вершины v_i , входящие в неё ребра пронумерованы числами $1 \dots d$. Такой автомат работает по шагам. На шаге с номером t с помощью локальной функции связи вычисляются новые значения ячеек

$$m_i(t) = f(m_{\eta(i,1)}(t-1), m_{\eta(i,2)}(t-1), \dots, m_{\eta(i,d_i)}(t-1)),$$

где $\eta(i, j)$ – номер вершины, из которой исходит ребро, входящее в вершину i и имеющее номер j . Заполнением клеточного автомата $M(t)$ на шаге t будем называть набор значений ячеек $(m_1(t), m_2(t), \dots, m_N(t))$.

Построению хэш-функций на основе таких автоматов посвящена, в частности, работа [3]. Они основаны на итерациях обобщенного клеточного автомата. Для подробного изложения их конструкции здесь недостаточно места, но для данной работы важен сам факт использования клеточных автоматов.

Обобщенные клеточные автоматы и вычисления на графических процессорах

Здесь же мы остановимся на одном важном свойстве криптографических алгоритмов, основанных на обобщенных клеточных автоматах. Свойство это заключается в том, что количество ячеек обобщенного клеточного автомата принципиально ничем не ограничено и, следовательно, может быть выбрано достаточно большим с тем, чтобы сделать невозможным эффективное распараллеливание вычислений.

В частности, для того, чтобы сделать невозможным эффективное вычисление выходных значений клеточных автоматов с помощью графических процессоров (технологий OpenCL и CUDA), необходимо выбрать число ячеек большим, чем количество потоков в рабочей группе графического процессора, которое составляет от нескольких сотен до нескольких тысяч, в зависимости от конкретного графического процессора.

Обобщенные клеточные автоматы и ПЛИС

Несколько сложнее обстоит дело с противодействием параллельной обработке на программируемых логических интегральных схемах (ПЛИС). Заметим, что для реализации одного клеточного автомата необходимо количество логических элементов, примерно равное количеству ячеек (в случае, если конкретной ПЛИС поддерживаются d -местные логические элементы). У современных ПЛИС количество логических элементов достигает нескольких миллионов. В любом случае, использование клеточных автоматов, состоящих из десятков и сотен тысяч ячеек, существенно ограничивает возможность распараллеливания с использованием ПЛИС, поскольку одновременно на такой ПЛИС можно будет реализовать не более $\lfloor a/n \rfloor$ клеточных автоматов, где a – количество логических элементов ПЛИС, а n – число ячеек клеточного автомата.

При этом, ничто не мешает сделать клеточные автоматы сколь угодно большими. Это приведет к некоторому снижению производительности при реализации на ПЛИС, как за счет увеличения сложности схемы, так и за счет увеличения числа шагов клеточного автомата, которое следует выбирать пропорциональным диаметру графа клеточного автомата. Однако при правильном выборе графа обобщенного клеточного автомата, в частности, при использовании того или иного графа Рамануджана, необходимое число шагов оценивается как $\Omega(\log n)$. Таким образом, с ростом размера (числа ячеек)

обобщенного клеточного автомата, необходимое число растет медленно, что позволяет использовать клеточные автоматы достаточно большого размера.

Заключение

Итак, обобщенные клеточные автоматы – весьма гибкий криптографический примитив. Использование клеточных автоматов большого размера (более 100 тыс. – 1 млн. ячеек) в таких функциях позволяет существенно затруднить применение параллельных архитектур для выполнения атаки методом грубой силы за счет увеличения количества ресурсов, необходимых для вычисления. При этом использование графических процессоров становится невозможным, либо нерациональным, а эффективность использования ПЛИС существенно уменьшается. По-видимому, такие функции могут найти широкое применение в программно-аппаратных средствах защиты информации (например, упомянутых в работах).

Литература

1. Ключарев П.Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. Электронное научно-техническое издание. 2012. № 12.
2. Ключарев П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. Электронное научно-техническое издание. 2011. № 10.
3. Ключарев П.Г. Криптографические хэш-функции, основанные на обобщённых клеточных автоматах // Наука и образование. Электронное научно-техническое издание. 2013. № 1.
4. Лебедев А.Н. Способ рассылки защищенных данных с регулированием доступа к отдельным их разделам // Вопросы кибербезопасности. 2015. № 5. С. 70-72.
5. Percival C., Josefsson S. The scrypt Password-Based Key Derivation Function, IETF, January 26, 2015. 2015.
6. Лебедев А.Н. Электронная подпись: новый этап // Вестник Московского городского педагогического университета. Серия: Экономика. 2013. № 1. — С. 43-51.

Generalized cellular automata as the base for key derivation functions construction Klyucharev P.G.¹⁴⁰

This paper is devoted to the possibility of using generalized cellular automata for the construction of the key derivation functions. We propose a concept of using the giant cellular automata for resist to the cracking by means GPU and FPGA based computations.

Keywords: Cellular automata, Key derivation function, hash function

УДК [004.773:004.023:004.031.42:[316.4+316.6]]:004.056

Социальные сети: перспективные направления исследований Ключарёв П.Г.¹⁴¹

Работа посвящена краткому обзору основных задач, связанных с анализом социальных сетей. В ней рассматриваются задачи деанонимизации пользователей, определения виртуальных пользователей, определения реакции пользователей на события, изучения закономерностей распространения информации, выявления сфер влияния, предсказания событий, определения трендов, определения событий в реальном времени, предсказания действий пользователей,

¹⁴⁰ Peter Klyucharev, Ph.D., Associate Professor, Bauman Moscow State Technical University, pk.iu8@yandex.ru

¹⁴¹ Ключарёв Петр Георгиевич, к.т.н., МГТУ им. Н.Э. Баумана, pk.iu8@yandex.ru

Введение

В настоящее время социальные сети используются большинством граждан Российской Федерации, которые публикуют в них более миллиарда записей в день. Многие пользователи доверяют информации, полученной через социальные сети больше, чем информации из традиционных СМИ. Фактически, социальные сети являются отличной средой для распространения дезинформации, пропаганды и применения различных методов воздействия на массовое сознание. Все это делает социальные сети одной из основных арен информационного противоборства. Это приводит к необходимости разработки систем мониторинга социальных сетей. Направление это является новым и требует проведения большого объема научных исследований, обзор некоторых направлений которых можно найти, например, в работах [1; 7].

В настоящей работе мы кратко очертим основные научные задачи, связанные с анализом социальных сетей.

Методы и уровни анализа социальных сетей

Для анализа социальных сетей используются различные методы, в том числе, методы машинного обучения, теории графов (в том числе, спектральной [2]), теории игр, математической статистики, социологии, социальной психологии, лингвистики и др. Таким образом, в данной области одновременно используются методы, относящиеся как к техническим, так и к гуманитарным наукам.

Анализировать ту или иную социальную сеть можно на различных уровнях. В частности, можно выделить уровень анализа топологии сети (социального графа), уровень анализа динамики сети (изменения социального графа во времени) и уровень анализа поведения пользователей (сообщений, публикуемых пользователями, а также различных меток, таких, как так называемые лайки, которые ставят пользователи). По-видимому, наиболее перспективно сочетать анализ на разных уровнях.

Некоторые задачи, связанные с анализом социальных сетей

Не претендуя на полноту, выделим следующие задачи анализа социальных сетей.

1. Деанонимизация пользователей. Сюда входит получение информации, такой как пол, возраст, образование, место жительства, место работы, место учебы и др., которую пользователь не счел нужным указать, либо указал неправильно. Эту задачу можно решать на разных уровнях: на уровне топологии сети – анализируя граф ближайшего окружения пользователя [3], а также, на уровне поведения пользователей – анализируя выкладываемые пользователем сообщения, фотографии и другие материалы (они могут содержать, например, те или иные указания на конкретное место, в том числе геотеги).

2. Выявление виртуальных пользователей (ботов). В настоящее время, боты широко используются для распространения рекламы, пропаганды и дезинформации. Выявление ботов может производиться как путем исследования графов их ближайшего окружения, так и путем анализа сообщений.

3. Определение реакции пользователей на то или иное событие, явление и т.д. Здесь анализ производится на уровне поведения пользователей. В частности, публикуемые ими сообщения, содержащие определенные ключевые слова, могут носить различную эмоциональную окраску [8]. Для определения таковой окраски служит так называемый сентимент-анализ текста – эмоциональная окраска текста определяется с помощью методов

¹⁴² Работа выполнена при поддержке РФФИ (проект №16-29-09517).

машинного обучения.

4. Изучение закономерностей распространения информации. Известно, что некоторая информация быстро распространяется в социальных сетях (например, в социальной сети Twitter, большинство сообщений не вызывает никакой реакции пользователей, либо реакция мала и быстро затухает во времени, но иногда встречаются сообщения, которые порождают целую волну ретвитов). Это весьма важное явление все еще недостаточно хорошо исследовано.

5. Выявление сфер влияния. При решении целого ряда задач очень важным является определение того, какие пользователи и группы пользователей влияют на конкретного пользователя, представляют для него авторитет.

6. Предсказание событий. Интереснейшей задачей является предсказание результатов различных событий по информации, содержащейся в социальных сетях. Так, по сообщениям в социальных сетях удастся предсказывать итоги выборов [9], показатели фондового рынка [4] и т.д. Обычно такие предсказания делаются на основании анализа сообщений, публикуемых пользователями, для чего используются методы машинного обучения.

7. Определение трендов. Большое значение имеет определение трендов, т.е. основных тем, которые занимают умы некоторой группы, выделенной по территориальному, социальному, либо какому-нибудь другому признаку. Определение трендов [6] может происходить как на поведенческом уровне, так и на уровне топологии социальной сети.

8. Определение событий в реальном времени. Получать данные о том, что и где происходит в реальном времени может быть очень важно. В социальных сетях многие пользователи публикуют данные о тех или иных событиях. Причем эти данные включают в себя геотеги, что делает возможным их сбор и анализ.

9. Предсказание действий конкретных пользователей. Большинство пользователей ведут себя стереотипно (например, ежедневно едут на работу по определенному маршруту). При этом они публикуют ту или иную информацию в социальных сетях, в том числе, фотографии, и эта информация может содержать геотеги. Все это позволяет предсказывать поведение пользователей [5].

10. Построение рекомендательных системы. По поведению пользователей в социальных сетях, а также по социальному графу возможно прогнозировать, какой именно товар необходим данному пользователю. Такие системы имеют большое применение в маркетинге и для таргетирования рекламы [10].

Заключение

Таким образом, социальные сети являются весьма важным объектом для исследования. Связанные с ними задачи чрезвычайно актуальны и, вместе с тем, все еще недостаточно хорошо исследованы.

Литература

1. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства. — Москва : Физматлит, 2010. — 225, [1] с.
2. Ключарёв П.Г., Чесноков В.О. Исследование спектральных свойств социального графа сети LiveJournal // Наука и образование. Электронное научно-техническое издание. 2013. № 9.
3. Чесноков В.О., Ключарёв П.Г. Выделение сообществ в социальных графах по множеству признаков с частичной информацией // Наука и образование. Электронное научно-техническое издание. 2015. № 9. — С. 188-199.
4. Bollen J., Mao H., Zeng X. Twitter mood predicts the stock market // Journal of Computational Science. 2011. T. 2. № 1. — С. 1-8.
5. Cho E., Myers S.A., Leskovec J. Friendship and mobility: user movement in location-based social networks. : ACM, 2011. — 1082-1090.
6. Guille A., Hacid H., Favre C., Zighed D.A. Information diffusion in online social networks: A survey // ACM SIGMOD Record. 2013. T. 42. № 2. — С. 17-28.
7. Kurka D.B., Godoy A., Von Zuben F.J. Online Social Network Analysis: A Survey of Research Applications in Computer Science // arXiv preprint arXiv:1504.05655. 2015.
8. Pak A., Paroubek P. Twitter as a Corpus for Sentiment Analysis and Opinion Mining. 2010. — 1320-1326.
9. Tumasjan A., Sprenger T.O., Sandner P.G., Welp I.M. Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment // ICWSM. 2010. T. 10. — С. 178-185.
10. Walter F.E., Battiston S., Schweitzer F. A model of a trust-based recommendation system on a social network // Autonomous Agents and Multi-Agent Systems. 2008. T. 16. № 1. — С. 57-74.

Social Networks: Perspective research fields

Klyucharev P.G.¹⁴³

Abstract. The paper is devoted to a brief survey of the problems associated with the analysis of social networks. It addresses a user deanonymization problem, a virtual users determine problem, a problem of determine users response to the events, the study of information diffusing and some other problems in this field. This work was supported by RFBR (project 16-29-09517).

Keywords: Social network, information war, machine learning

УДК 004.023

Способ выбора сканера отпечатков пальцев

Куренкова П.Ю.¹⁴⁴

В докладе рассмотрена проблема выбора сканера отпечатков пальцев для системы биометрической идентификации. Выделены основные параметры для выбора сканера отпечатков пальцев. Предложена формула, оптимизирующая выбор сканера отпечатков пальцев. Предложенный способ позволяет упростить выбор сканера отпечатков пальцев и существенно сократить время выбора.

Ключевые слова: биометрические системы, идентификация, сканер отпечатков пальцев, FAR

Введение

В настоящее время многие компании начинают использовать биометрические параметры для идентификации или аутентификации [1], в том числе для подтверждения личности человека, для защиты от несанкционированного доступа, для предотвращения краж и мошенничества при совершении финансовых сделок [2, 3]. Биометрические параметры делятся на две группы –

¹⁴³ Peter Klyucharev, Ph.D., Associate Professor, Bauman Moscow State Technical University, pk.iu8@yandex.ru

¹⁴⁴ Куренкова Полина Юрьевна, ЗАО «НПО «Эшелон», Москва, kurenkova.p@gmail.com

физиологические и поведенческие. Наибольшей популярностью среди биометрических систем пользуются физиологические параметры из-за более высокой надежности по сравнению с поведенческими параметрами при сравнительно несложных алгоритмах экстракции и вычисления сходства [4]. Один из самых распространенных примеров использования физиологического параметра в биометрических системах является использование сканеров отпечатков пальцев, например в [5]. Это обусловлено следующими причинами:

- удобство сканирования отпечатка пальца для пользователя [6];
- простота и надежность технологии сканирования;
- стоимость сканера отпечатка пальцев.

Существующие на сегодняшний день сканеры отпечатков пальцев можно условно выделить в три группы [7]:

- оптические;
- кремниевые (полупроводниковые);
- ультразвуковые.

Так же сканеры отпечатков пальцев представлены в различных форм-факторах [2]:

- компактные сканеры отпечатков пальцев для офиса;
- мобильные терминалы идентификации;
- терминалы контроля доступа и учета рабочего времени, включающего сканеры отпечатков пальцев;
- встраиваемые сканеры.

Из вышеизложенного становится понятно, что при наличии столь широкого ассортимента сканеров отпечатков пальцев задача выбора оптимального сканера для организации становится достаточно трудоемкой.

Параметры выбора сканера отпечатка пальца

Компании выбирают сканер отпечатков пальцев, руководствуясь следующими параметрами [8]:

- совместимость ПО;
- цена сканера;
- разрешение сканера;
- скорость сканирования;
- FAR, необходимая для корректной идентификации N сотрудников в день с вероятностью ошибки одна за день;
- FAR сканера.

Для оптимизации выбора сканера из нескольких вариантов, обозначим каждый параметр как некий коэффициент со значением от 0 до 1, показывающий, насколько конкретный сканер является оптимальным по данному параметру. При умножении всех коэффициентов конкретного сканера будет получено значение, меньше или равное 1. Далее операция умножения коэффициентов производится для всех остальных сканеров, полученные значения сравниваются, а сканер, чье итоговое значение будет наибольшим, будет являться оптимальным.

Стоит заметить, что перечисленные параметры являются приблизительными и могут отличаться для конкретной компании. Также каждый параметр был принят равнозначным.

Оптимизация выбора сканера для системы биометрической идентификации

С учетом вышесказанного оптимальность сканера отпечатков пальцев Q рассчитывается по формуле:

$$Q_i = c_i \cdot p_i \cdot s_i \cdot r_i \cdot FAR_i, \quad (1)$$

где: c_i — коэффициент совместимости ПО,

p_i — коэффициент цены,

s_i — коэффициент скорости сканирования,

r_i — коэффициент разрешения,

FAR_i — коэффициент соотношения FAR сканера и FAR, необходимого для корректной работы при N сотрудников с одной ошибкой в день.

Распишем каждый коэффициент подробнее.

Коэффициент совместимости ПО c_i считается по формуле:

$$c_i = \frac{c_w \cdot k_w + c_a \cdot k_a + c_l \cdot k_l}{100\%}, \quad (2)$$

где: c_w, c_a, c_l — проценты ОС Windows, Apple и Linux соответственно среди всех ОС для компьютеров, а k_w, k_a, k_l — коэффициенты наличия или отсутствия поддержки данной ОС у ПО сканера.

Рекомендуется брать статистику того года, в котором будет производиться закупка сканера.

Коэффициент p_i считается по формуле:

$$p_i = \frac{p_{\text{сканера}} - p_{\text{max}}}{p_{\text{max}} - p_{\text{min}}}, \quad (3)$$

где: $p_{\text{сканера}}$ — цена сканера, а p_{max} и p_{min} — максимальная и минимальная цена среди выборки сканеров соответственно.

Коэффициенты скорости сканирования s_i и разрешения r_i рассчитываются аналогично формуле (3).

Коэффициент FAR_i определяется по формуле:

$$FAR_i = \begin{cases} \frac{2FAR_{\text{сканера}}}{(FAR_{\text{сканера}} + FAR_N)} & \text{при } FAR_{\text{сканера}} < FAR_N \\ 1 & \text{при } FAR_{\text{сканера}} \geq FAR_N \end{cases}, \quad (4)$$

где $FAR_{\text{сканера}}$ — значение FAR (False Acceptance rate) сканера, а FAR_N — значение FAR, необходимое для корректной идентификации N сотрудников с базой отпечатков количеством N с одной ошибкой в день. Значение FAR_N рассчитывается по формуле:

$$FAR_N = \frac{1}{N^2} \quad (5)$$

Подставив формулы (2) - (5) в формулу (1), получим:

$$Q_i = \begin{cases} \left(\frac{c_w \cdot k_w + c_a \cdot k_a + c_l \cdot k_l}{100\%} \right) \cdot \left(\frac{p_{\text{сканера}} - p_{\text{max}}}{p_{\text{max}} - p_{\text{min}}} \right) \cdot \left(\frac{s_{\text{сканера}} - s_{\text{max}}}{s_{\text{max}} - s_{\text{min}}} \right) \cdot \left(\frac{r_{\text{сканера}} - r_{\text{max}}}{r_{\text{max}} - r_{\text{min}}} \right) \cdot \frac{2FAR_{\text{сканера}}}{(FAR_{\text{сканера}} + \frac{1}{N^2})} & \text{при } FAR_{\text{сканера}} < \frac{1}{N^2}; \\ \left(\frac{c_w \cdot k_w + c_a \cdot k_a + c_l \cdot k_l}{100\%} \right) \cdot \left(\frac{p_{\text{сканера}} - p_{\text{max}}}{p_{\text{max}} - p_{\text{min}}} \right) \cdot \left(\frac{s_{\text{сканера}} - s_{\text{max}}}{s_{\text{max}} - s_{\text{min}}} \right) \cdot \left(\frac{r_{\text{сканера}} - r_{\text{max}}}{r_{\text{max}} - r_{\text{min}}} \right) & \text{при } FAR_{\text{сканера}} \geq \frac{1}{N^2}; \end{cases}, \quad (6)$$

Вывод

В данной работе разработан способ для оптимизации выбора сканера отпечатков пальцев из нескольких вариантов для системы биометрической идентификации. Предложенные соотношения позволяют упростить и унифицировать процесс выбора сканера, а также существенно сократить время выбора.

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. Талецкий Н. С. Фальсификация отпечатков папиллярных узоров пальцев рук как основной способ преодоления идентификационных биометрических систем защиты / Н. С. Талецкий // Вісник Південного регіонального центру Національної академії правових наук України. - 2015. - № 5. - С. 228-234.
3. Булдакова Т.И., Суятинов С.И., Кривошеева Д.А. Обеспечение информационной безопасности в телемедицинских системах на основе модельного подхода // Вопросы кибербезопасности. 2014. № 5(8). С. 21-29.
4. Лысак А. Б. Идентификация и аутентификация личности: обзор основных биометрических методов проверки подлинности пользователя компьютерных систем // Математические структуры и моделирование. - 2012. - №. 26. - С. 124-134.
5. Максимов Р.Л., Рафиков А.Г. Разработка автоматической СКУД повышенной безопасности на базе типового решения СКУД Biosmart с использованием автоматного подхода // Вопросы кибербезопасности. 2015. № 5 (13). С. 73-80.
6. Тхай Ф. 3. Некоторые вопросы применения методов сравнения отпечатков пальцев для биометрических систем идентификации личности // Международный научно-исследовательский журнал. - 2015. - №. 7-1 (38).
7. Bilinsky Y., Yukish M., Pavliuk O. Fingerprint scanners // Scientific Works of Vinnytsia National Technical

Научный руководитель: Булдакова Татьяна Ивановна, профессор, доктор технических наук, МГТУ им. Н.Э. Баумана, buldakova.bmstu@ru.

The Method of Fingerprint Scanner Selection Kurenkova P.

The report considers the problem of choosing a fingerprint scanner for biometric identification system. The basic parameters for selecting the fingerprint scanner were highlighted. The formula that optimizes the choice of fingerprint scanner was proposed. The proposed method allows to simplify the choice of fingerprint scanner and significantly reduce the time of choice.

Keywords: biometric system, identification, fingerprint scanner, FAR

УДК 004.056

Сравнение линейных и разностных свойств операций сложения по модулю 2^n и AND

Козлов А.А.¹⁴⁵

В последние годы отмечается стремительный рост числа низкоресурсных алгоритмов шифрования. В первую очередь это обусловлено развитием «интернета вещей». При построении подобных алгоритмов часто используются сравнительно простые в реализации операции сложения по модулю 2^n или AND. В работе рассмотрены линейные и разностные свойства этих операций, приводится их сравнительный анализ. Полученные результаты могут использоваться при построении новых и оценки стойкости существующих низкоресурсных алгоритмов шифрования.

Ключевые слова: сложение по модулю 2^n , AND, блочное шифрование, низкоресурсная криптография

Введение

В последние годы стали появляться устройства бытовой техники, транспорта, а также различные датчики, имеющие выход в Интернет. Это явление получило название «Интернет вещей» (IoT). IoT характеризуется низким уровнем доступных вычислительных ресурсов устройств, входящих в его состав. В соответствии с этим, накладываются ограничения на криптографические алгоритмы, применяемые в IoT.

Раздел криптографии, изучающий алгоритмы криптографии, разрабатываемые специально для устройств с ограниченными вычислительными ресурсами, называется легковесной криптографией [1]. В последние годы наблюдается стремительный рост числа работ посвященных легковесной криптографии. Среди первых работ в этой области стоит выделить работы [2-4], которые помимо прочего были посвящены выработке требований, предъявляемых к средствам легковесной криптографии.

¹⁴⁵ Козлов Александр Александрович, МГТУ им. Н.Э.Баумана, Москва. badptr@xaker.ru

Согласно [5] наиболее активная и продуктивная деятельность в области легковесной криптографии приходится на разработку низкоресурсных алгоритмов блочного шифрования. В области разработки низкоресурсных алгоритмов блочного шифрования часто в качестве криптографических примитивов раундовых операций используются операции сложения по модулю 2^n или AND . Здесь и далее под операцией AND будем понимать операцию побитового логического «И» двух двоичных наборов равной длины. В алгоритмах шифрования, например в таких как Simon и Speck [6], эти операции являются единственным источником нелинейности.

В настоящее время не существует универсального метода криптоанализа для всех блочных алгоритмов шифрования. В то же время существуют методы, которые с некоторыми изменениями могут быть применены к любому алгоритму шифрования. В первую очередь речь идет о линейном и разностном криптоанализе. При построении нового алгоритма шифрования, разработчику необходимо убедиться в достаточной стойкости разрабатываемого алгоритма по отношению к подобным методам.

Цель данной работы – провести сравнительный анализ линейных и разностных свойств операций AND и сложения по модулю 2^n .

1. Линейные свойства операций AND и сложения по модулю 2^n

Для операции сложения по модулю 2^n в работе [7] было получено, что наилучшая линейная аппроксимация для этой операции имеет преобладание не более чем $\frac{1}{4}$. Докажем аналогичное утверждение для операции AND .

Утверждение 1. Обозначим через A и B , входы операции AND , $A = (a_{n-1}, a_{n-2}, \dots, a_0)$, $B = (b_{n-1}, b_{n-2}, \dots, b_0)$ и через Q ее выход, $Q = (q_{n-1}, q_{n-2}, \dots, q_0)$. Тогда:

$$\forall i > 0, \text{Prob}(a_i \oplus b_i = q_i) = \text{Prob}(a_i = q_i) = \text{Prob}(b_i = q_i) = 0.75.$$

Доказательство. Утверждение следует из сравнения таблиц истинности операций AND и XOR .

2. Разностный криптоанализ

В работе [8] была доказана теорема о распространении усеченных разностных характеристик через операцию сложения по модулю 2^n . Сравним результаты, полученные в [8] для операции сложения по модулю 2^n , с результатами для операции AND .

Утверждение 2. Обозначим через $andp^+$ вероятность распространения разности по модулю 2 через операцию AND . Пусть заданы входные разности A и B , и выходная разность Q , для операции AND , с операцией XOR в качестве операции разности. Тогда, если известно, что $andp^+(A_{i-1}, B_{i-1} \rightarrow Q_{i-1}) = \text{Prob}_{Q_{i-1}}$, то:

если

$$a_{i-1} = b_{i-1} = q_{i-1} = 0, \text{ то } \text{Prob}_{Q_i^0} = \text{Prob}_{Q_{i-1}}, \text{Prob}_{Q_i^1} = 0,$$

если

$$a_{i-1} \neq 0 \text{ или } b_{i-1} \neq 0 \text{ или } q_{i-1} \neq 0, \text{ то } \text{Prob}_{Q_i} = \frac{1}{2} \text{Prob}_{Q_{i-1}},$$

где

$$Q_i^0 = (0, q_{i-1}, q_{i-2}, \dots, q_0),$$

$$Q_i^1 = (1, q_{i-1}, q_{i-2}, \dots, q_0),$$

$$Q_i = (q_i, q_{i-1}, q_{i-2}, \dots, q_0), q_i \in \{0, 1\}.$$

Доказательство. Для доказательства утверждения построим таблицу истинности для следующих булевых функций. Обозначим без ограничения общности через x_1 и x_2 k -е биты входа операции *AND* слева, так что

$$x_1 \oplus x_2 = a_k \quad (1)$$

Аналогично, обозначим через x_3 и x_4 k -е биты входа операции *AND* справа,

$$x_3 \oplus x_4 = b_k \quad (2)$$

Тогда выходная разность выражается как

$$x_1 x_3 \oplus x_2 x_4 = q_k \quad (3)$$

Таблица истинности для (1), (2) и (3) представлена в таблице 1.

Таблица 5.

Таблица истинности выражений

x_1	x_2	x_3	x_4	$x_1 \oplus x_2$	$x_3 \oplus x_4$	$x_1 x_3 \oplus x_2 x_4$
0	0	0	0	0	0	0
0	0	0	1	0	1	0
0	0	1	0	0	1	0
0	0	1	1	0	0	0
0	1	0	0	1	0	0
0	1	0	1	1	1	1
0	1	1	0	1	1	0
0	1	1	1	1	0	1
1	0	0	0	1	0	0
1	0	0	1	1	1	0
1	0	1	0	1	1	1
1	0	1	1	1	0	1
1	1	0	0	0	0	0
1	1	0	1	0	1	1
1	1	1	0	0	1	1
1	1	1	1	0	0	0

Из представленной таблицы следует доказываемое утверждение.

3. Сравнение операций

Полученные выше результаты позволяют доказать следующую теорему.

Теорема 1. Если в некоторый *ARX* алгоритм шифрования была заложена стойкость к линейному и разностному методам криптоанализа, то алгоритм останется по-прежнему стойким по отношению к этим методам при замене в нем операции сложения по модулю 2^n на операцию *AND*.

Доказательство. В предыдущих разделах было получено, что операция *AND* обладает такими же предельными характеристиками по отношению к статистическим методам линейного и разностного криптоанализа как и операция сложения по модулю 2^n . Отсюда следует доказываемое.

Выводы

В работе были рассмотрены линейные и разностные свойства операций сложения по модулю 2^n и *AND*. Для каждой из этих операций были получены оценки для их линейных и разностных свойств. На основе полученных оценок была сформулирована теорема о взаимосвязи между двумя исследованными операциями. Полученные результаты могут служить важным оценочным инструментом при конструировании новых

или проведении анализа уже существующих **низкоресурсных** алгоритмов блочного шифрования.

Литература

1. Paar C. Light-Weight Cryptography for Ubiquitous Computing. Securing Cyberspace Workshop IV: Special purpose hardware for cryptography –Attacks and Applications. University of California at Los Angeles, December 4, 2006.
2. Sarma S. E., Weis S. A., Engels D. W. Radio-frequency identification: Security risks and challenges. CryptoBytes 6, 1, pp. 2–9, 2003.
3. Sarma S. E., Weis S. A., Engels D. W. RFID systems and security and privacy implications. In CHES 2002, Lecture Notes in Computer Science v. 2523, pp. 454–469, 2003.
4. Weis S. A., Sarma S. E., Rivest R. L., Engels D. W. Security and privacy aspects of low-cost radio frequency identification systems. In Security in Pervasive Computing 2003, Lecture Notes in Computer Science v. 2802, pp. 201–212, 2004.
5. Жуков А.Е. Легковесная криптография. Часть 2. // Вопросы кибербезопасности. 2015. № 2 (10). С 2-10.
6. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013)
7. Козлов А.А., Карондеев А.М., Силков А.А. Сложение по модулю 2^n в блочном шифровании // Вопросы кибербезопасности. 2015. №3(11). С 32-44.
8. Козлов А.А. Криптографический анализ ARX шифров на основе усеченных разностей. Электронный журнал «Молодежный научно-технический вестник». //http://sntbul.bmstu.ru/doc/833658.html

Научный руководитель: Жуков Алексей Евгеньевич, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э.Баумана, канд. физ.-мат. наук, доцент

Comparison of linear and differential properties of addition modulo 2^n and AND

Kozlov A.A.¹⁴⁶

In recent years there has been rapid growth in the number of lightweight encryption algorithms. This is primarily due to the development of the "Internet of Things". In the construction of such algorithms are often used relatively simple operations of addition modulo 2^n or AND. The paper deals with linear and differential properties of these operations, their comparative analysis are given. The results can be used in the construction of new and cryptanalysis of existing lightweight encryption algorithms. The author is grateful to Ph.D, Associate Professor A.E. Zhukov for the participation in the preparation of this paper.

Keywords: addition modulo 2^n , AND, block ciphers, lightweight cryptograph

¹⁴⁶ Kozlov Alexander Alexandrovich, Bauman Moscow State Technical University, Moscow, badptr@xaker.ru

Биометрические методы в симметричном шифровании**Комаров А.И., Комаров Н.И.¹⁴⁷**

В статье представлен способ совмещения методов биометрической идентификации и симметричного шифрования, как наиболее эффективного. В качестве метода симметричного шифрования выбран наиболее распространенный метод DES. В качестве биометрических показателей выбраны отпечатки пальцев отправителя и получателя. Дана схема шифрования и описаны ее основные этапы.

Ключевые слова: симметричное шифрование, DES, биометрия, отпечатки пальцев

Введение

Симметричное шифрование еще называется шифрованием с симметричным ключом (мастер-ключом), так как для шифрования и дешифрования используется один ключ. Процесс симметричного шифрования показан на рис. 1.

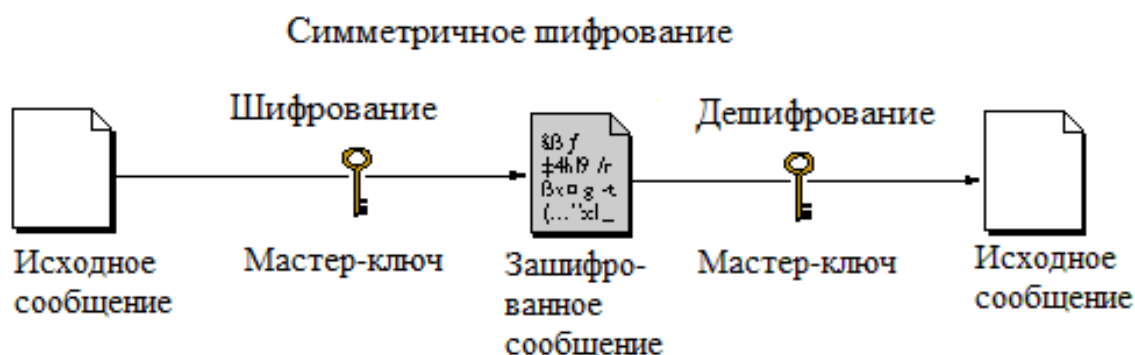


Рис. 1. Процесс симметричного шифрования

Симметричное шифрование является востребованным, поскольку:

- можно относительно недорого создать мастер-ключ;
- ключи, как правило, не имеют большого размера;
- алгоритмы являются относительно недорогими для обработки.

Таким образом, реализация симметричной криптографии (в частности, с оборудованием) может быть весьма эффективной, потому что вы не испытываете каких-либо значительных задержек по времени в результате шифрования и дешифрования [1]. Это удобно для систем реального времени [2, 3]. Симметричная криптография также обеспечивает степень проверки подлинности, поскольку данные, зашифрованные одним симметричным ключом, не могут быть расшифрованы любым другим симметричным ключом. Поэтому, до тех пор, пока симметричный ключ держится в секрете, обе стороны могут быть уверены в конфиденциальности, передаваемых данных.

Как правило, каждая пара создает свой уникальный мастер-ключ. Поэтому человек может быть уверен в том, что, пока мастер-ключ будет держаться в тайне, сообщение может быть расшифровано только его оппонентом, которому известен мастер-ключ. Человек, незаконно получивший мастер-ключ, может не только расшифровать сообщения, отправленные с помощью этого ключа, но и шифровать новые сообщения и отправлять их,

¹⁴⁷ МГТУ им. Н.Э. Баумана, г. Москва, komarov.05.16@mail.ru

как если бы они пришли от тех пользователей сети, которые первоначально использовали оригинальный мастер-ключ [4].

Из симметричных алгоритмов шифрования наиболее распространенным является алгоритм DES.

Применение отпечатков пальцев и криптографии для защиты сетей

Опишем процедуру шифрования и дешифрования. Получатель первый предоставляет его отпечатки, согласно запросу от отправителя. Затем изображения отпечатков пальцев получателя и отправителя соединяются. В зависимости от размера изображения берется часть изображения на формирование 128-битного мастер-ключа с помощью алгоритма хеширования MD5. Случайная последовательность генерируется в зависимости от длины сообщения. Передаваемое сообщение шифруется при помощи алгоритма DES. Мастер-ключ вместе со случайной последовательностью подвергается ватермаркировке [5] и помещается в изображение отпечатка пальца отправителя. Ватермаркированное сообщение и зашифрованное сообщение отправляются получателю.

Зашифрованное сообщение теперь расшифровывается с помощью мастер-ключа и случайной последовательности с помощью алгоритма DES.

Выделим основные этапы работы предложенной схемы (рис. 2).

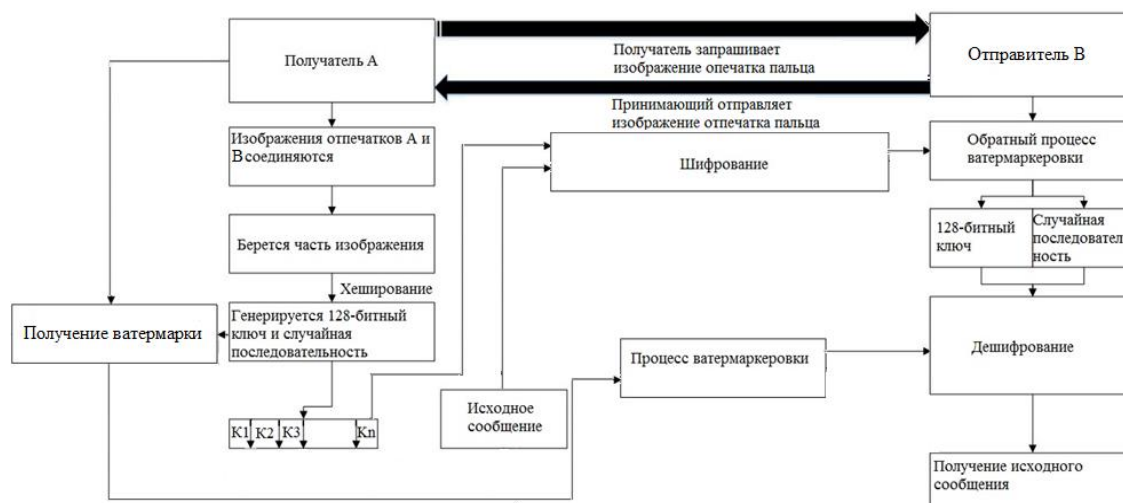


Рис. 2. Схема шифрования

1. Для отправителя:

- сначала по запросу отправителя получатель должен предоставить свой отпечаток;
- далее генерируется изображение отпечатка пальца с помощью комбинаций отпечатков пальцев получателя и отправителя. Часть с изображением пальца необходима для генерации 128-битного ключа с помощью алгоритма хеширования MD5;
- сообщение, которое предназначено для передачи на приемник, будет шифроваться при помощи стандартного алгоритма DES. В предложенном алгоритме из 128-битного ключа генерируется случайная последовательность в зависимости от длины сообщения. Для каждого 64-битового сообщения используется отдельный 64-битный ключ для шифрования;
- отпечаток пальцев теперь помечается ватермаркой с помощью последовательности, полученной на предыдущем шаге, и 128-битного ключа, полученного на основе использования вейвлет-преобразования, основанного на методе

ватермаркирования [5], в котором первое изображение отпечатка пальца разложено на n поддиапазонов с использованием преобразования DWT2 Хаара. Двоичные значения встраиваются в поддиапазоны после умножения их на коэффициент усиления.

Далее изображение отпечатка пальца вместе с ватермаркой посылается требуемому получателю.

Для получателя:

- получив сообщение, принимающий начинает процедуру расшифровки ватермарки, которая происходит с помощью метода DWT2 и корреляции вектора, тем самым извлекая случайную последовательность и 128-битный ключ;
- зашифрованное сообщение будет расшифровано с использованием стандартного алгоритма DES и извлеченного мастер-ключа. При этом выполняются те же действия, что и для шифрования, т.е. каждое 64-битное сообщение с отдельным 64-битным ключом использует ту же случайную последовательность.

Выводы

Таким образом, в представленном методе ключ шифрования и дешифрования формируется из отпечатков отправителя и получателя, что дает ему множество преимуществ с существующими методами аутентификации, поскольку ключ не может быть забыт или случайно сообщен кому-либо. Метод ватермаркировки помогает в подтверждении принадлежности ключа. Предложенный метод позволит обеспечить безопасность и целостность биометрических данных.

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. Булдакова Т.И., Суятинов С.И., Кривошеева Д.А. Обеспечение информационной безопасности в телемедицинских системах на основе модельного подхода // Вопросы кибербезопасности. 2014. № 5(8). С. 21-29.
3. Булдакова Т.И., Суятинов С.И. Применение биосигналов к защите данных в телемедицинских системах // Математические методы в технике и технологиях: в 12 т. Т.6. Санкт-Петербург: СПбГТИ(ТУ), 2016. С. 87-88.
4. Бельфер Р.А., Петрухин И.С., Тепикин А.П. Анализ угроз информационной безопасности виртуальных частных сетей VPLS на базе сети MPLS // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2015. № 1 (100). С. 47-57.
5. Goi, B.M., Phan, R.C.W., Yang, Y., Bao, F., Deng, R.H., Siddiqi, M.U. Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity. In: Jakobsson, M., Yung, M., Zhou, J. (eds.) Proc. Applied Cryptography and Network Security 2004, LNCS 3089, pp. 369–382.

Научный руководитель: Булдакова Татьяна Ивановна, профессор, д.т.н, профессор кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана, buldakova@bmstu.ru.

Biometric Methods in Symmetric Encryption

Komarov A.I., Komarov N.I.¹⁴⁸

Abstract: in this article we shows the possibility of combining the methods of biometric identification and symmetric encryption techniques as the perfect one. DES was chosen as the most common method of symmetric encryption. As biometric data were selected sender and receiver fingers` prints. The scheme of encryption and the main stages were shown here.

Keywords: symmetric encryption, DES, biometrics, finger prints

¹⁴⁸ Komarov A.I. and Komarov N.I., Bauman Moscow State Technical University, Moscow, komarov.05.16@mail.ru

**Безопасное распределение конфиденциальной информации при
инициализации приложения****Лебедев А. Н., Островский Д.Е.¹⁴⁹**

Решается задача безопасного конфигурирования приложения для работы с конфиденциальной информацией, такой как ключи и пароли для доступа пользователя к сторонним сервисам. В работе рассмотрены различные подходы к безопасному созданию и хранению такой конфигурации, проведён анализ возможных угроз. На основе новой технологии аппаратной защиты данных Intel SGX предложен способ безопасного создания цифрового сертификата для приложения, обоснована его способность противостоять угрозам определенного класса.

Ключевые слова: чувствительная (конфиденциальная) информация, конфигурация приложения, цифровой сертификат, технология Intel SGX, виртуализация.

Введение. При развертывании прикладной программы, как некоторого сервиса, требуется произвести ее начальное конфигурирование и инициализацию. Конфигурация приложения представляет собой отдельный статический компонент, который обрабатывается при запуске программы и задаёт её параметры. Приложение не работает автономно, оно интегрировано со сторонними платформами и сервисами, для соединения с которыми необходима авторизация. Чтобы пройти авторизацию для использования сервисов, программа должна иметь технический аккаунт и пройти аутентификацию при установлении соединения [1-2].

Для успешной аутентификации программе необходимо обладать некоторым секретом, который позволит удалённому сервису убедиться в подлинности программы. Любой секрет имеет определенное время жизни, по истечении которого его следует изменить на новый, однако в течение времени жизни секрет является статической конфиденциальной информацией, и в большинстве случаев задаётся через конфигурацию программы. В этом подходе есть два существенных недостатка [1-3]: секрет хранится в незашифрованном виде и доступен в операционной системе из-под аккаунта приложения (секрет можно зашифровать, но возникает новая задача – где хранить ключ шифрования?); секрет создаётся и разворачивается человеком, имеющим доступ к системе из аккаунта приложения. Такой подход небезопасен, вследствие человеческого фактора (секрет преднамеренно или непреднамеренно попасть к злоумышленнику).

Рассмотрим принципы, которые используются для защиты чувствительной конфигурации.

Способы защиты секретов конфигурации. Во-первых, следует отметить известные способы [1-4], которые используются для защиты чувствительной информации приложения: аппаратное хранение ключа (например, на USB-токене или смарт-карте), либо обфускация. Однако эффективная и стойкая обфускация недостижима на практике, а аппаратные способы хранения чувствительной информации на отдельном устройстве неудобны для масштабирования и удалённого администрирования, что противоречит тенденциям развёртывания сервисов в облаке.

Для повышения надежности защиты секрета от доступа в операционной системе можно использовать два подхода.

¹⁴⁹ 1 Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lan@lancrypto.com, 2 Островский Дмитрий Евгеньевич, МГТУ им. Н.Э.Баумана, Москва, crypto-expert@yandex.ru

Первый подход – *виртуализация*, секреты приложения разворачиваются в некоторой доверенной ОС, доступ к которым из недоверенной ОС ограничивается гипервизором путём проверки электронной подписи приложения, запущенного в недоверенной ОС, и определения, имеет ли это приложение доступ к тем или иным секретам. Однако у такого подхода остаются практически те же самые недостатки: секреты хранятся в открытом виде на диске доверенной ОС, следовательно, они не защищены физически; секреты создаются и разворачиваются в доверенной ОС человеком. Преимущество подхода состоит в том, что секреты защищены от компрометации из недоверенной ОС. Доступ к ОС даже администратора не поможет завладеть секретами приложений.

Второй подход базируется на *аппаратной поддержке* хранения и обработки чувствительной информации, встроенной в центральный процессор. Такая поддержка появилась в 2015 году в шестом поколении микропроцессоров Интел на архитектуре Skylake и носит название Software Guardian Extensions (SGX) [3-5]. Технология SGX позволяет “упаковывать” секреты приложения так, что они хранятся зашифрованными как на диске, так и в оперативной памяти во время обработки. Доступ к секретам имеет только приложение, они не доступны операционной системе даже в режиме гипервизора [5].

Технология SGX поддерживает протокол удалённой аттестации платформы, на которой запущено приложение. Он служит для того, чтобы пользователь мог убедиться, что приложение запущено на подлинном процессоре

Интел с технологией SGX. Протокол удалённой аттестации служит для проверки целостности участка кода приложения, отвечающего за работу с чувствительной информацией. Этот участок кода называется *анклав*.

Используя SGX, можно защитить секреты приложения, однако их необходимо создать и передать приложению на этапе инициализации. Разработчики SGX предложили использовать для этой цели отдельный сервис SP, который после аттестации приложения, передаст ему секреты по зашифрованному каналу. Остается человеческий фактор, секреты будет создавать и передавать в SP человек при развёртывании приложений.

Для защиты предлагается разделить роли: техническая – секреты генерируются внутри анклава приложения и не покидают его; административная - администратор верифицирует анклав и подписывает его ключом разработчика. Таким образом, имея протокол, по которому можно проводить удалённую аттестацию анклава с проверкой подписи разработчика, можно убедиться в его целостности и аутентичности.

Безопасная инициализация приложения. Развёртывание и инициализация приложения, в котором осуществляется безопасное получение сертификата изображены на рис.1.

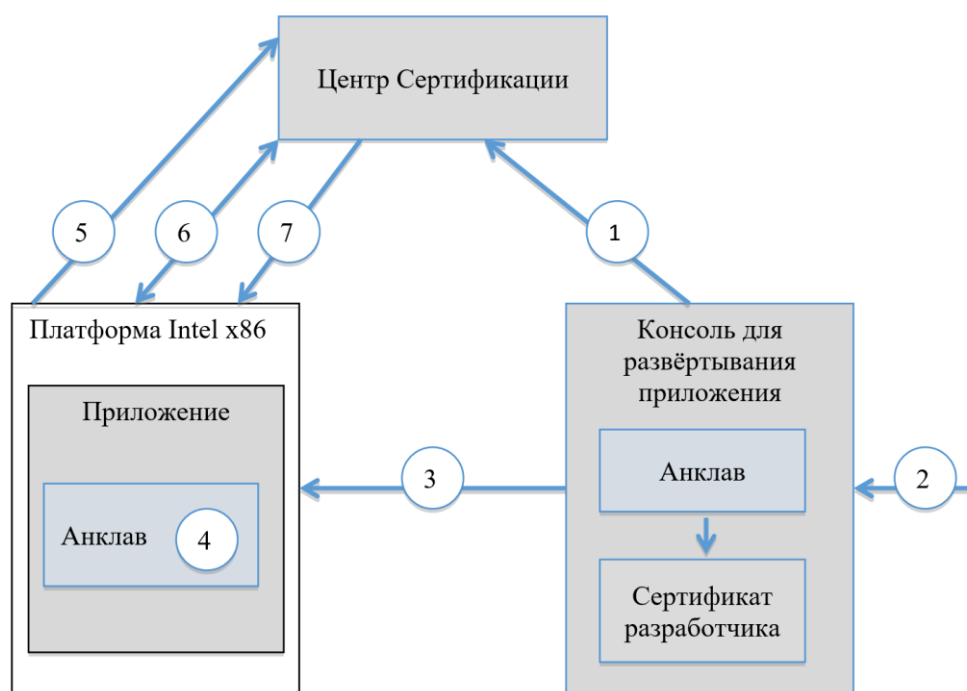


Рис.1. Схема безопасного получения приложением цифрового сертификата

Развёртывание приложения и получение сертификата состоит из следующих фаз:

1. Администратор проходит аутентификацию в ЦС чтобы получить доступ к сертификату разработчика.
2. Администратор, имея исполняемый код приложения, верифицирует анклав, работающий с чувствительной информацией, затем подписывает анклав ключом разработчика.
3. Администратор устанавливает приложение на целевую платформу и запускает его.
4. Приложение (анклав) производит начальную инициализацию своего секрета: генерирует ключевую пару закрытый ключ – открытый ключ.
- 5 Приложение отправляет запрос на подпись сертификата в ЦС.
6. ЦС производит удалённую аттестацию приложения: проверяет подлинность платформы и подпись разработчика анклава.
7. ЦС, доверяя разработчику и платформе, на которой запущено приложение, выдает сертификат.

Вывод. Предложенная авторами схема позволяет защитить секретный ключ приложения как от непосредственной компрометации, при условии полного доступа к платформе, так и от возможного влияния человеческого фактора. В рамках предложенного способа аутентификации даже администратор приложения не будет обладать секретным ключом сертификата. Базируясь на этих принципах, можно разработать протоколы для безопасной инициализации приложения чувствительной информацией и оценить их защищённость в предложенной модели угроз.

Литература

1. Brickell E., Li J. Enhanced privacy ID from bilinear pairing for hardware authentication and attestation. International Journal of Information Privacy, Security and Integrity, Vol. 1, No. 1, 2011, pp. 3-33. DOI: 10.1504/IJIPSI.2011.043729 URL: <http://dx.doi.org/10.1504/IJIPSI.2011.043729>
2. Johnson S. Intel® Software Guard Extensions // EPID Provisioning and Attestation Services. 2016, pp. 1-10. URL: <https://software.intel.com/en-us/blogs/2016/03/09/intel-sgx-epid-provisioning-and-attestation-services>
3. Garg S., Gentry C. Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits. In 54th Annual Symposium On Foundations of Computer Science, FOCS 2013, pp. 40-49, 26-29. URL: <https://eprint.iacr.org/2013/451.pdf>
4. Китайские закладки: непридуманная история о виртуализации, безопасности и шпионах. - Журнал «Хакер» 26.12.2011. URL: <https://xakep.ru/2011/12/26/58104/>
5. Ярыженко Р. Обзор фреймворка для создания ОС Genode. - Журнал «Хакер» 20.05.2015. URL: <https://xakep.ru/2015/05/20/genode-os-build-review/>

Secure Distribution of a Sensitive Information During Software Initialization

Lebedev A.N., Ostrovsky D.E.¹⁵⁰

Abstract. The problem of secure initialization of application software is analyzed for that works with sensitive or confidential information. Some new methods and algorithms have been offered. Analysis of some probable attacks is made. A method based upon digital certificates use is offered in combination with the Intel SGX techniques. Its security with respect to the set of all known attacks is analyzed.

Keywords: sensitive (confidential) information, software application configuration, digital certificate, Intel SGX techniques, virtualization.

УДК 004.056.55

Анализ надежности защиты баз данных методами современной криптографии

Лебедев А. Н., Барсукова А. С.¹⁵¹

В работе приведены результаты сравнительного анализа надежности, технологичности и удобства пользователей при различных методах реализации криптографической защиты баз данных в зависимости от целей и задач такой защиты. Показано, что при естественных предположениях о возможностях потенциального злоумышленника (противника) криптографическая защита данных в основных распространенных типах баз данных может обеспечить наибольшую надежность защиты при минимальных затратах по сравнению с любым другим способом защиты данных, не внося значительного неудобства в работу пользователей.

Ключевые слова: база данных, криптографические преобразования, стойкость, ключи шифрования, гомоморфное шифрование способы распределения ключей, управление ключами.

Введение. Современная криптография позволяет наиболее эффективно решать многие практические задачи в области защиты информации, которые возникают перед организацией, использующей компьютеры. В частности, задачу защиты баз данных, которая в силу требований действующего законодательства и в силу практической необходимости на сегодняшний день стоит практически перед каждой реально работающей организацией [1-2].

¹⁵⁰ Lebedev A., Ostrovsky D. Bauman Moscow State Technical University, Moscow

¹⁵¹ ¹ Лебедев А.Н., к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lan@lancrypto.com, ² Барсукова А. С., МГТУ им. Н.Э. Баумана, Москва, barsukova.94@mail.ru

Во многих случаях для решения задачи надежной защиты базы данных чисто организационных мер и встроенных в систему управления базами данных средств защиты оказывается недостаточно [4, 7]. Например, немаловажной особенностью защиты информации в базах данных является наличие файлов-триггеров, с помощью которых выполняются запросы. В таких файлах данные для запросов хранятся в открытом виде. При наличии у злоумышленника физического доступа к месту установки системы управления базой данных, просмотр информации, содержащейся в триггерах, не составляет труда [4-6].

Доводы в пользу криптографии. Криптографические методы защиты данных, хранимых и обрабатываемых как записи базы данных можно грубо разделить на два основных класса: методы защиты от несанкционированного просмотра данных при помощи их шифрования как в процессе хранения, так и процессе передачи по каналам связи на компьютеры пользователей; методы авторизации доступа пользователей к различным разделам базы данных, а также аутентификации блоков данных (записей базы данных) [1-7].

Шифрование непосредственно записей базы данных (или даже отдельных их частей) на различных ключах при использовании современных стойких алгоритмов позволяет радикально решить проблему надежного разграничения доступа к различным разделам базы данных и не нуждается в больших затратах на физическую защиту непосредственно самих носителей данных [1-2, 6].

Аутентификация отдельных разделов базы данных, отдельных записей или даже отдельных их наиболее важных частей с помощью технологии электронной подписи позволяет гарантировать защиту от несанкционированных изменений в базе данных с любой наперед заданной степенью детализации и документирования [3, 5-7]. Следует отметить тот факт, что на сегодня ни один способ защиты баз данных, кроме криптографического, не может обеспечить того уровня надежности защиты данных и удобства пользователей, которые обеспечиваются криптографическими технологиями.

Возможные ограничения. Однако, как показывает практика, в опоре исключительно на криптографические методы защиты баз данных есть и заметные недостатки. Так, достаточно сложная для понимания средним пользователем техника применения криптографических методов, в частности, методов управления ключами шифрования, аутентификации и паролями доступа к данным и ресурсам приводит к тому, что обычный пользователь невольно «перепоручает» большинство своих обязанностей по работе с ключами системным администраторам. А это, в свою очередь, приводит к таким явлениям как несанкционированный доступ администраторов баз данных даже к тем их разделам, к которым они доступ заведомо иметь не должны.

Наиболее показательный пример – явление Эдварда Сноудена [8], который смог получить доступ к очень важным данным с самыми высокими грифами секретности, к которым он заведомо не мог иметь легального доступа. Поэтому при использовании криптографических методов защиты базы данных на первый план выходят задачи управления ключами. Как непосредственно ключами шифрования данных и создания электронной подписи, так и ключами и паролями доступа к криптографическим ключам для работы с данными.

Идеальный вариант. Наиболее надежным и удобным, как для пользователей, так и для администраторов базы данных, представляется такой, при котором шифруются отдельные записи на индивидуальных ключах, причем сам процесс шифрования и расшифрования блока данных происходит на компьютере пользователя, а его индивидуальный пользовательский ключ для шифрования данных позволяет сформировать только ключи шифрования/расшифрования тех записей базы данных, доступ к которым ему

разрешен. При этом пользовательские криптографические ключи могут генерироваться и храниться в защищенной памяти аппаратного токена пользователя [1-2]. Такого рода схема управления ключами может быть построена по принципу, описанному в работе [3].

Кроме того, представляется заманчивым использовать гомоморфные шифры, которые позволяют осуществлять управление базой данных непосредственно с зашифрованными записями и не требуют предоставления прав доступа к данным администраторам базы.

Для этого должны быть разработаны достаточно эффективные гомоморфные шифры, которые бы не замедляли работу базы данных на порядок. Это – предмет дальнейших исследований и разработок.

Выводы. Современные криптографические методы защиты данных не имеют альтернативы ни по надежности защиты, ни по эффективности и удобству пользователей. Однако, неправильное или неаккуратное их применение, в частности, нерешенные проблемы управления ключами пользователей могут свести на нет все эти преимущества.

Важным фактором при выборе криптографических методов защиты в базах данных является структура хранения информации в базах данных и необходимость ее удаленной обработки. Существуют два основных принципа защиты данных на удаленном сервере. Первый предполагает выполнение операций с данными через систему управления базой данных на компьютерах пользователей или промежуточных серверах (прокси-серверах) [1]. При такой схеме защиты применяется один тип шифрования ко всей базе данных.

Второй принцип защиты предполагает применение разных типов шифрования для различных полей таблицы, при этом на прокси-серверах кодируются сами данные. При таком применении криптографических методов защиты производить операции над данными и устанавливать систему управления базой данных можно на удаленном сервере (или в облачной инфраструктуре) [2].

Для каждого из этих принципов авторами предложены конкретные способы, их воплощающие, которые обеспечивают реализацию всех преимуществ каждого из принципов в полном объеме [1-3].

Литература

1. Назначение Secret Disk Server NG // URL: [http:// www.aladdin-rd.ru/catalog/secret_disk/server /](http://www.aladdin-rd.ru/catalog/secret_disk/server/) 2016 /.
2. Назначение решения "Крипто БД". URL: // [www.aladdin-rd.ru/catalog/cryptobd /](http://www.aladdin-rd.ru/catalog/cryptobd/) 2016 / ноябрь / cryptobd_KCI.pdf
3. Лебедев А.Н. Способ рассылки защищенных данных с регулированием доступа к отдельным их разделам // Вопросы кибербезопасности. 2015. № 5 (13). С. 70-72.
4. Popa R.A, Redfield C.M.S, Zeldovich N., Balakrishnan H CryptDB: Protecting Confidentiality with Encrypted Query Processing In: SOSP, 2011, pp. 85-100. URL: // [https:// people.csail.mit.edu /nickolai/papers/popa-cryptdb.pdf](https://people.csail.mit.edu/nickolai/papers/popa-cryptdb.pdf)
5. Popa R.A, Redfield C.M.S, Zeldovich N., Balakrishnan H. CryptODB: Processing Queries on an Encrypted Database. Communications ACM, 55(9), 2012, pp. 103-11. URL: // [https:// people.csail.mit.edu /nickolai/popa-cryptdb-cacm.pdf](https://people.csail.mit.edu/nickolai/popa-cryptdb-cacm.pdf)
6. Popa R.A, Zeldovich N., Guidelines for Using the CryptDB System Securely In: Cryptology ePrint Archive, Report. 2015. URL: // <https://eprint.iacr.org/2015/979>
7. Curino C., Jones E.P.C., Popa R.A., Malviya N., Wu, E., Madden S., Balakrishnan H., Zeldovich N. Relational Cloud: A Database-as-a-Service for the Cloud. In: CIDR. 2011. URL: // [https:// people.csail.mit.edu /nickolai/curino-relcloud.pdf](https://people.csail.mit.edu/nickolai/curino-relcloud.pdf)
8. Сырков Б.Ю. Сноуден: самый опасный человек в мире. М.: Алгоритм, 2016. 432с.

A Strong Multifactor Authentication Method **Lebedev A.N.¹, Barsukova A.S.²**

Abstract. We analyze and compare several different approaches to secure data base by cryptographic means of the contemporary cryptography. It is clearly demonstrated that cryptographic methods are the most secure, effective and user friendly among all of the known methods and even principles to make data secure. On the other hand it is shown that key management problem may reduce security down to nothing, if it is not solved correctly. Some algorithms to solve the key management problem have been proposed.

Keywords: data base, cryptographic transformation, ciphers, homomorphic ciphers, digital signature, key management, access regulation.

УДК 004.056.55

Новый алгоритм блочного шифрования «NASH» **Лебедев А. Н., Карондеев А.М., Козлов А.А.¹⁵²**

Предложен оригинальный алгоритм блочного шифрования, предназначенный для реализации на широко распространенных микроконтроллерах общего назначения. Алгоритм «NASH» основан на принципах современной «легковесной криптографии», но использует управляемые сдвиги, что позволяет для достижения стойкости ограничиваться меньшим числом раундов, повышая скорость обработки данных. Алгоритм «NASH» может быть использован для защиты обмена данными между устройствами в сетях «интернет вещей», а также для защиты данных, записываемых на компактные персональные носители (флэш-память и т.д.).

Ключевые слова: шифрование, блочный алгоритм шифрования, легковесная криптография, раундовая функция, управляемые сдвиги, развертка ключа.

Введение. В связи с широким распространением в современных промышленных системах, системах управления и массовых бытовых устройствах потребительского рынка микроконтроллеров общего назначения они стали относительно дешевы. В то же время их возможности изменились настолько сильно, что стало возможно говорить о реальном их использовании для реализации таких сложных криптографических преобразований информации, как шифрование [1-2].

Однако реализация на таких микроконтроллерах принятых национальных стандартов шифрования не может обеспечить приемлемой скорости шифрования данных [1-2]. Поэтому для достижения высокой скорости при реализации на подобных микроконтроллерах было предложено несколько специальных алгоритмов шифрования, получивших название «легковесных» [3-7]. Наиболее эффективными среди них следует признать алгоритмы SPECK и SIMON, разработанные криптографами АНБ США [6-7].

В каждом из них наиболее явно выражена идея построения алгоритма шифрования, состоящего в большом количестве простых преобразований, которая впервые высказывалась в работе К. Шеннона [8] и письмах 50-х годов в АНБ известного лауреата нобелевской премии по экономике Джона Нэша [9].

Поэтому мы поставили своей целью разработать легковесный алгоритм блочного

¹⁵² Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lan@lancrypto.com
Карондеев Андрей Михайлович, МГТУ им. Н.Э. Баумана, Москва, karondeev@ya.ru
Козлов Александр Александрович, МГТУ им. Н.Э. Баумана, Москва, badptr@xaker.ru

шифрования, который не уступал бы по стойкости упомянутым алгоритмам АНБ, но позволял бы несколько сократить количество раундов, что должно сделать его еще более быстрым. В честь Джона Нэша (John Nash) мы назвали алгоритм NASH.

Схема алгоритма NASH выглядит следующим образом. Текст разбивается на полублоки по 2^n бит и каждый блок шифруется в течение r раундов на последовательности раундовых ключей k_i , которые в свою очередь получаются из главного ключа шифрования по определенному алгоритму «расширения ключа».

Блок данных разбивается на левый и правый полублоки (L_i , R_i) по 2^n бит каждый, с которыми на $(i+1)$ -м раунде производятся следующие преобразования

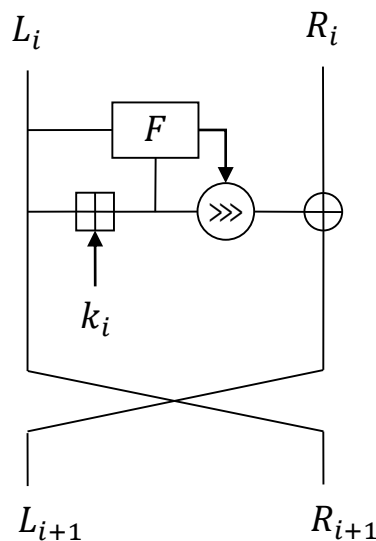


Рис. 1. Схема раунда шифрования

Уравнения шифрования блока данных на $(i+1)$ -м раунде выглядят так:

$$R_{i+1} = L_i$$

$$L_{i+1} = (L_i \boxplus k_i \ggg F(L_i, L_i \boxplus k_i)) \oplus R_i$$

В последнем раунде шифрования блока не меняем местами L_{i+1} , R_{i+1}

Детали раундового преобразования. Размер полублока равен 2^n , где $n = 5$ или 6 , соответственно 32, 64 бита. Соответственно предлагается размер блока 64 или 128 бит.

Смешивание с раундовым ключом k_i : $\boxplus$ – функция сложение двух целых чисел по модулю 2^n .

Управляемый циклический сдвиг:

для размера блока 64 бита (полублока – 32 бита) - циклический сдвиг вправо на одно из 4 значений (11, 14, 10, 19).

для размера блока 128 бит (размер полублока – 64 бита) - циклический сдвиг вправо на одно из 4 значений (37, 34, 38, 29)

Функция управления сдвигами: интерпретируем L_i как вектор значений булевой функции от n переменных, и первый выходной бит F получаем как значение данной функции на наборе битов из $L_i \boxplus k_i$ вида $2^i - 1$, где $i = 1 \dots n$, то есть как значение

$$L_i((L_i \boxplus k_i)[2^1 - 1, \dots, 2^n - 1])$$

нумерация битов полублока от 0 до $2^n - 1$;

интерпретируем $L_i \boxplus k_i$ как вектор значений булевой функции от n переменных, и второй выходной бит F получаем как значение данной функции на наборе битов из L_i вида $2^i - 1$, где $i = 1 \dots n$, то есть как

$$(L_i \boxplus k_i)(L_i[2^1 - 1, \dots, 2^n - 1])$$

нумерация битов полублока от 0 до $2^n - 1$.

Для размера блока 64 бита (полублока – 32 бита) размеры сдвигов таковы: 00 соответствует циклическому сдвигу на 11; 01 соответствует циклическому сдвигу на 14; 10 соответствует циклическому сдвигу на 10; 11 соответствует циклическому сдвигу на 19.

Число раундов r : для размера блока 64 (полублока 32): $r = 24$; для размера блока 128 (полублока 64): $r = 28$. Размер ключа 128, 192 или 256.

Функция выработки раундовых ключей

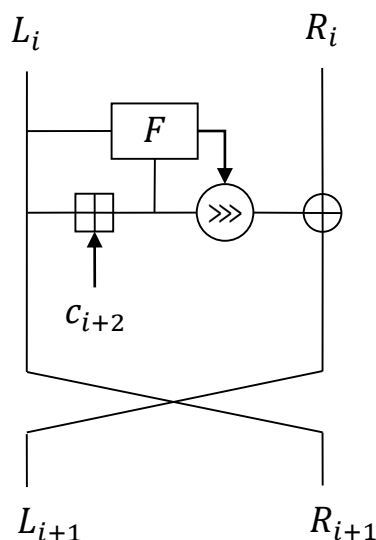


Рис. 2 Схема раунда формирования ключей

$L_0 = c_0, R_0 = c_1$, где значение константы c_i получается следующим образом.

Ключ разбивается на l блоков длины 2^n , еще $8 - l$ блоков получаем как значения квадратного корня из первых простых чисел ($\sqrt{2}, \sqrt{3}, \sqrt{5}$ и т.д., оставляем только мантиссу – дробную часть без порядка. C99 / C11 80-бит long double берем биты из последних 64 бит).

Данные блоки соответствуют $c_0, c_1 \dots c_7$. Далее при вычислении c_i берем индекс $(i \bmod 6) + 2$ и складываем его по модулю 2 с номером раунда

$$c_i = i \oplus c_{(i \bmod 6) + 2}$$

В качестве раундового ключа берем $k_i = L_{i+1}$.

Вывод. Разработанный авторами алгоритм шифрования был представлен на международной конференции EUROCRYPT 2016. Он показывает лучшие результаты по скорости реализации на массовых микроконтроллерах общего назначения, не снижая стойкости шифрования, что подтверждается результатами как отечественных, так и зарубежных (Технический университет, Цюрих, Швейцария) криптографов.

Литература

1. Microcontrollers-and-Processors. 2016. URL: http://www.nxp.com/products/microcontrollers-and-processors/arm-processors/i.mx-applications-processors:IMX_HOME
2. Internet of Things. 2016. Meudon, Cedex, France URL: <http://www.gemalto.com/iot/iot-security>
3. McKay K., Bassham L., Turan M., Mouha N. DRAFT NISTIR 8114 // Report on Lightweight Cryptography // Computer Security Division, NIST, Gaithersburg, MD, USA, 2016, pp. 1-23. URL: http://csrc.nist.gov/drafts/nistir-8114/nistir_8114_draft.pdf
4. D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, A. Biryukov. Triathlon of Lightweight Block Ciphers for the Internet of Things // Report on Lightweight Cryptography // Lightweight Cryptography Workshop 2015. Computer Security Division, NIST, Gaithersburg, MD, USA, 2015, pp. 1-18. URL: <https://eprint.iacr.org/2015/209.pdf>
5. N. Mouha, B. Mennink, A. Van Herrewege, D. Watanabe, B. Preneel, I. Verbauwhede. Chaskey: a Lightweight MAC Algorithm for Microcontrollers. Lightweight Cryptography Workshop 2015. Cryptography Computer Security Division, NIST, Gaithersburg, MD, USA, 2015, pp. 21-35. URL: <http://www.nist.gov/document/accepted-papers-lwc2015pdf>
6. H. Tschofenig, M. Pegourie-Gonnard. Performance of State-of-the-Art Cryptography on ARM-based Microprocessors // NIST Lightweight Cryptography Workshop 2015. Gaithersburg, MD, USA, 2015. pp. 54-67. URL: <http://csrc.nist.gov/groups/workshop2015/session7-vincent.pdf>
7. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers. Simon and Speck: Block Ciphers for the Internet of Things. National Security Agency, Fort Meade, MD, USA, 2015, pp. 1-15. URL: <http://csrc.nist.gov/groups/ST/lwc/session1-shors-paper.pdf>
8. C. Shannon. Communication theory of secret systems. Bell Systems Technical Journal, NY, USA, 1949, pp. 656-715.
9. J. Nash. Letter to NSA, Fort Mead, MD, USA, 1955, URL: http://www.nsa.gov/public_info/press_room/2012/nash_exhibit_shtm

A New Lightweight Block Cipher NASH

Lebedev A.N., Karondeev A.M., Kozlov A.A.¹⁵³

Abstract. An original new lightweight block cipher has been invented. The algorithm called NASH after the famous Nobel Prize winner John Nash, who had proposed some new encryption algorithms and ideas in his letter to NSA in 1955. The algorithm NASH could be effectively implemented by any of the wide range of mass contemporary general purpose microcontrollers. The algorithm is very convenient for the Internet-of-Things and many other applications of the same kind.

Keywords: general purpose microcontrollers, data encryption, lightweight cryptography, block cipher, different rotations, key schedule.

¹⁵³ Bauman Moscow State Technical University, Moscow

Правовые аспекты защиты информации в лабораторных информационных системах

Левиев Д.О.¹⁵⁴, Герасимчук С.Н.¹⁵⁵

АННОТАЦИЯ: Рассматриваются правовые аспекты защиты информации в лабораторных и медицинских информационных системах, а также в телемедицине. Рассмотрение примера реализации защиты западными компаниями

КЛЮЧЕВЫЕ СЛОВА: информационная система, ЛИС, МИС, телемедицина, врачебная тайна, персональные данные.

Введение

Из-за развития информационных технологий в области здравоохранения стала особенно актуальна проблема защиты медицинской информации. Благодаря распространению Интернета и развитию различных услуг связи расширили круг субъектов, имеющих доступ к личной информации медицинского характера, что делает возможным злоупотребление данными сведениями [1,2].

Правовые принципы ЛИС

В лабораторных информационных системах необходимо жесткое правовое регулирование. На сегодняшний день, довольно слабо законодательством регулируется защита информации в лабораторных информационных системах. В России принят ряд законодательных актов для защиты пациента, ограничивающий доступ к медицинской информации или ее использование. основополагающими в этой сфере являются Федеральные законы от 27.07.2006 № 152-ФЗ “О персональных данных” и от 27.07.2006 №149-ФЗ “Об информации, информационных технологиях и о защите информации”. Оба закона предъявляют жесткие требования к порядку получения, хранения, использования, уничтожения информации, содержащей данные о конкретных лицах, защите данных и предусматривают ответственность за нарушение этого порядка.

Так же необходимо упомянуть статьи Основ законодательства Российской Федерации об охране здоровья граждан (утв. 22.07.1993 № 5487-1; далее – Основы), устанавливающие права пациента в области информации. Это статьи 31 “Право граждан на информацию о своем здоровье”, 32 “Информированное согласие”, 61 “Врачебная тайна”. Право на сохранение тайны трансформируется в право пациента на конфиденциальность сведений о его обращении за медицинской помощью и о состоянии его здоровья, а также иной информации, которую он сообщает врачу о себе при осмотре и в ходе лечения, т. е. право на врачебную тайну.

Администрация учреждения здравоохранения несет ответственность за обеспечение конфиденциальности и защиты медицинской информации о пациенте.

Не допускается включение и использование в автоматизированных базах данных без разрешения пациента информации персонифицированного характера, касающейся его частной жизни. Не допускается подключение автоматизированных баз данных, имеющих персонифицированный характер, к сетям, связывающим их с другими базами данных.

Разглашение без разрешения пациента в устной или письменной форме информации о состоянии его здоровья и иных данных о нем, ставших известными другим лицам при оказании ему медицинской помощи, является посягательством на личную жизнь пациента независимо от того, была ли разглашенная информация достоверной или ложной.

Пример реализации защищенных систем

¹⁵⁴ Левиев Д.О., МГТУ им. Н.Э. Баумана. Leviev@bmstu.ru

¹⁵⁵ Герасимчук Сергей Николаевич, МГТУ им. Н.Э. Баумана. s.gerasimchuk@galen.ru

Личные медицинские данные наиболее уязвимы при передаче через Интернет. Ненадежное хранение данных о здоровье человека может восприниматься как серьезное посягательство на тайну его личной жизни. Американские компании RADGUARD и MediLinks совместно разработали cPro – технологию защиты медицинской информации, основанную на принципе виртуальных частных сетей. Идея заключается в использовании Интернета как транспортной среды для передачи информационных пакетов. При этом имитируется работа локальной сети, объединяющей медицинские учреждения. Таким образом, хакеры, желающие получить доступ к медицинской информации извне, не смогут этого сделать.

Технология учитывает специфику медицинских учреждений – частую передачу ЭКГ и рентгеновских снимков с большим разрешением. Широкое внедрение МИС в практику работы лечебно-профилактических учреждений поставило перед организаторами здравоохранения ряд сложнейших правовых вопросов. Наиболее актуален вопрос об обеспечении врачебной тайны при использовании сетевых информационных технологий в медицине. Отдельная проблема – правовое сопровождение сеансов телемедицины.

Доверие лечащего врача, пациента и специалиста-консультанта к телемедицинской системе должно обеспечиваться:

- качеством и надежностью, регистрируемой в системе и передаваемой по каналам связи медицинской диагностической информации. Лечащий врач и специалист-консультант должны быть уверены в том, что, находясь на разных концах линии связи, они имеют и обсуждают идентичные медицинские данные;
- юридическим обоснованием законности проводимой консультации;
- предоставлением возможности получить консультацию у лучших специалистов страны и мира по конкретному заболеванию (таким образом решается проблема общедоступности медицинского обслуживания и обеспечения единого высокого стандарта качества медицинской помощи).

Безопасность внутри телемедицинской системы обеспечивается:

- защитой медицинской информации каждого пациента при передаче ее по каналам связи. Согласно закону, эта информация относится к персональной, поэтому должна быть защищена;
- защитой медицинской информации на этапе подготовки телемедицинской консультации, поскольку доступ к ней имеет не только медицинский, но и технический персонал телемедицинской сети;
- правовой защитой участников телемедицинской консультации от недобросовестного использования результатов консультации.

Таким образом, предоставление услуг по защите конфиденциальной информации, передаваемой в медицинских учреждениях, с учетом обеспечения совместимости с иными услугами (например, медицинского характера) создаст основу для универсальной инфраструктуры безопасности и, соответственно, принятия единых стандартов на правила защиты и конфиденциальности, а также на процедуры, связанные с их исполнением, для всех сегментов медицинской индустрии. Кроме того, деятельность по защите информации позволит продолжить работу консультативного комитета, в который входят представители ведущих медицинских организаций, в целях предоставления консультаций по правилам защиты медицинской информации на этапе внедрения в здравоохранении технологий электронного бизнеса.

Выводы

Безопасность информации в лабораторной информационной системе в значительной степени зависит от качества организации правовых аспектов внутри самой медицинской

организации. Так же необходима разработка рекомендаций в министерстве здравоохранения по организации информационной безопасности в медицинских учреждениях.

Литература

1. Назаренко Г.И., Гулиев Я.И., Ермаков Д.Е. Медицинские информационные системы: теория и практика, Под ред. Г.И. Назаренко, Г.С. Осипова -М.: Физматлит, 2005. -320 с.
2. Ильин А.В. Опыт интеграции ЛИС Innovasystem и МИС «Медиалог» в ФГБУ «Эндокринологический научный центр Минздравсоцразвития России // Медицинский алфавит. Современная лаборатория – 2012.

Научный руководитель: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им.Н.Э.Баумана, v.tsirlov@bmstu.ru

Legal Aspects of Information Protection in Laboratory Information Systems

Leviev D.O.¹⁵⁶, Gerasimchuk S.N.¹⁵⁷

Abstract: The legal aspects of information protection in the laboratory and health information systems and telemedicine. Consideration of the embodiment of Western companies protection

Keywords: information system, LIS, MIS, telemedicine, medical secret, personal information.

УДК 004.056.55

Квантовое распределение ключей с доверенным центром

Лебедев А. Н., Соколов А.В.¹⁵⁸

Предложен алгоритм, позволяющий увеличить криптографическую стойкость известного протокола квантового распределения ключей BB84 за счет введения доверенного центра. В результате удастся повысить криптографическую стойкость протокола распределения ключей при неизменных затратах в ходе передачи для каждой из сторон, участвующих в процессе квантового распределения ключа. Данный результат представляет интерес для приложений квантовой криптографии.

Ключевые слова: протокол BB84, квантовая криптография, квантовое распределение ключей, доверенный центр, повышение криптографической стойкости.

Введение. В последнее время вся чаще публикуются сообщения о практических разработках и научные работы об успехах в области квантовой криптографии, в частности, об аппаратной реализации устройств, принцип действия которых основан на законах квантового взаимодействия [1-3]. С другой стороны, растущий объем практических результатов предвещает появление квантового компьютера, готового к массовому производству, принципиально превосходящего современные компьютеры. Это будет означать радикальное изменение дел в современной криптографии [4]. Криптографы с

¹⁵⁶ Leviev Dmitrii, Bauman Moscow State Technical University, leviev@bmstu.ru

¹⁵⁷ Gerasimchuk S. Bauman Moscow State Technical University, s.gerasimchuk@galen.ru

¹⁵⁸ ¹ Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lan@lancrypto.com,

² Соколов Александр Владимирович, МГТУ им. Н.Э. Баумана, Москва, sav193@yahoo.com

начала 80-х годов XX века готовятся к появлению квантовых компьютеров и разрабатывают алгоритмы, устойчивые к квантовым вычислениям.

Первым протоколом распределения квантового ключа стал созданный в 1984 году Чарльзом Беннетом и Жилем Brassаром протокол «BB84». В основе стойкости данного протокола лежит фундаментальный принцип неопределенности Гейзенберга, согласно которому не представляется возможным детектировать квантовую частицу, при этом, не изменив ее состояния [3-5].

Протокол BB84. Он был разработан для секретного распределения ключей между абонентами. Физической средой передачи информации являются фотоны, поляризованные определенным образом. По традиции абонентов, участвующих в криптографической передаче ключей называют Алисой и Бобом, а противника, пытающегося добыть защищаемую информацию, называют Евой. Алиса генерирует поток фотонов и отправляет их Бобу.

Полученные фотоны Боб детектирует одним из двух способов для каждого из фотонов. Фотоны могут быть поляризованы под углом в 0, 45, 90, 135 градусов, чему соответствуют обозначения: «|» - вертикальная поляризация, «--» - горизонтальная поляризация, «/» - поляризация под углом 45 градусов и «\» - поляризация под углом 135 градусов. В случае попадания вертикально или горизонтально поляризованного фотона на прямоугольный детектор, обозначаемый «+», фотон распознается однозначно и не изменяется.

Аналогично для ситуации прохождения фотона, поляризованного под углом 45 или 135 градусов через диагональный детектор, обозначаемый «x». В противном случае, когда поляризация фотона не совпала с формой детектора, через который он прошел, фотон может принять случайное значение из диапазона допустимых для данного детектора значений поляризации фотона. Иными словами, если, например, фотон «/» с поляризацией 45 градусов прошел сквозь прямоугольный детектор «+», то на выходе с вероятностью 0,5 фотон будет поляризован либо как горизонтальный, «--», либо как вертикальный «|».

Протокол взаимодействия сторон выглядит следующим образом:

Алиса отправляет Бобу последовательность фотонов, поляризованных случайным (на практике псевдослучайным) образом, при этом приняв фотоны «|» и «\» за единичный бит, а фотоны «--» и «/» за нулевой бит.

Боб принимает последовательность фотонов, анализируя каждый из них прямоугольным или диагональным детектором и записывает полученные значения.

Боб связывается с Алисой и сообщает какие детекторы были использованы им во время приема. В ответ Алиса сообщает какие детекторы были выбраны верно, а какие нет.

Боб и Алиса вычеркивают те позиции, в которых детектор был подобран неверно, а для оставшихся записывают значения в виде битов.

Таким образом, у Алисы и Боба имеется одинаковая последовательность двоичных символов, известных только им. Именно эта последовательность будет являться ключом шифрования.

Если злоумышленник, то есть Ева, попытается получить ключевую информацию, вмешавшись в процесс передачи, она изменит первоначальную последовательность фотонов, генерируемую Алисой. В таком случае Боб получит искаженную последовательность, в результате чего его ключ будет отличаться от ключа Алисы. Обычно, для проверки на отсутствия вмешательства в канал со стороны Евы выбирается некоторое количество n проверочных бит. Тогда с вероятностью $1 - 2^{-n}$ вмешательство будет обнаружено.

Слабые стороны протокола BB84. После анализа используемых детекторов выходная последовательность значительно уменьшается. В случае бесконечно длинной

последовательности это сокращение составляет 50%. Таким образом, только примерно половина переданной информации в дальнейшем может служить в качестве ключа. Кроме того, существуют некоторые другие недостатки, связанные с физическими особенностями квантовой физики, а также несовершенством существующих аппаратных реализаций.

Схема улучшения протокола BB84. Для решения проблемы потери половины ключа, а также для увеличения стойкости алгоритма предлагается использовать такую реализацию протокола BB84. Дополнительно вводится третья сторона, доверенный центр, называемый Чарли.

Алиса и Боб отправляют Чарли поляризованный поток фотонов по квантовому каналу (рис. 1).

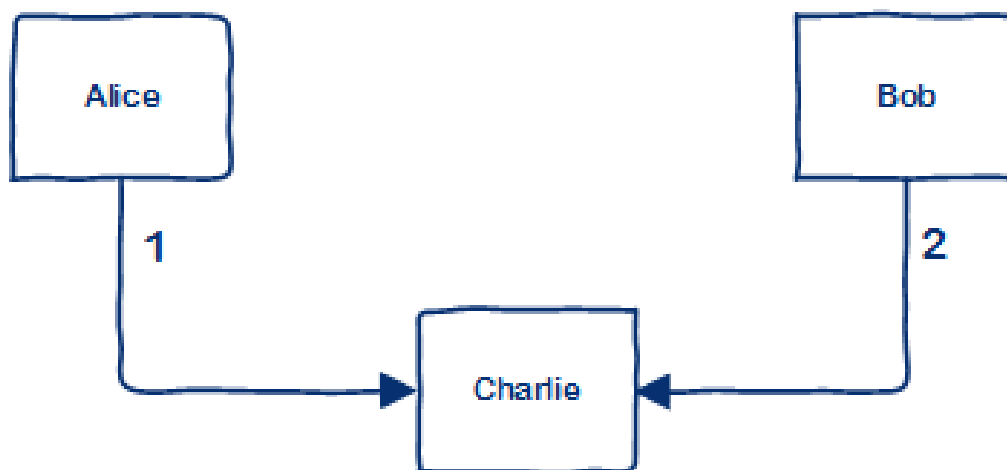


Рис. 1. Передача поляризованных фотонов доверенному центру

Чарли принимает фотоны и анализирует одним из детекторов. После этого Чарли связывается с Алисой и Бобом и узнает какие детекторы были применены верно, а какие нет (Рис. 2).

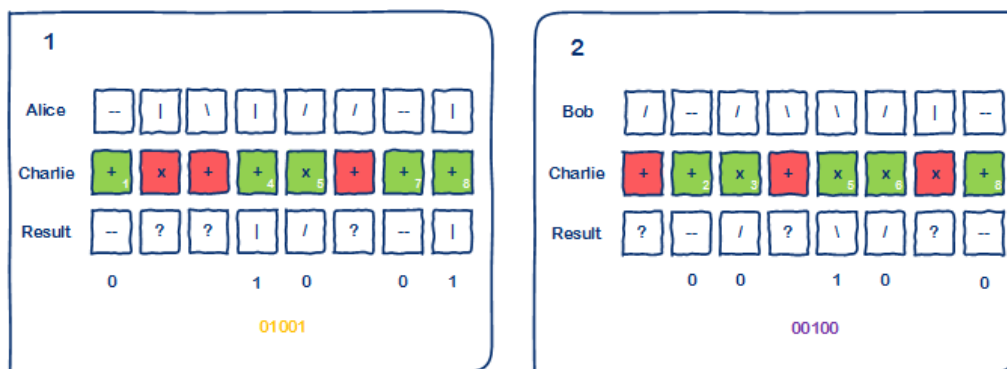


Рис. 2. Получение результатов ключа после проверки корректности выбора детекторов Чарли известны ключи Алисы и Боба, полученные им на предыдущем шаге. Далее Чарли необходимо передать Алисе ключ Боба, а Бобу ключ Алисы (Рис. 3).

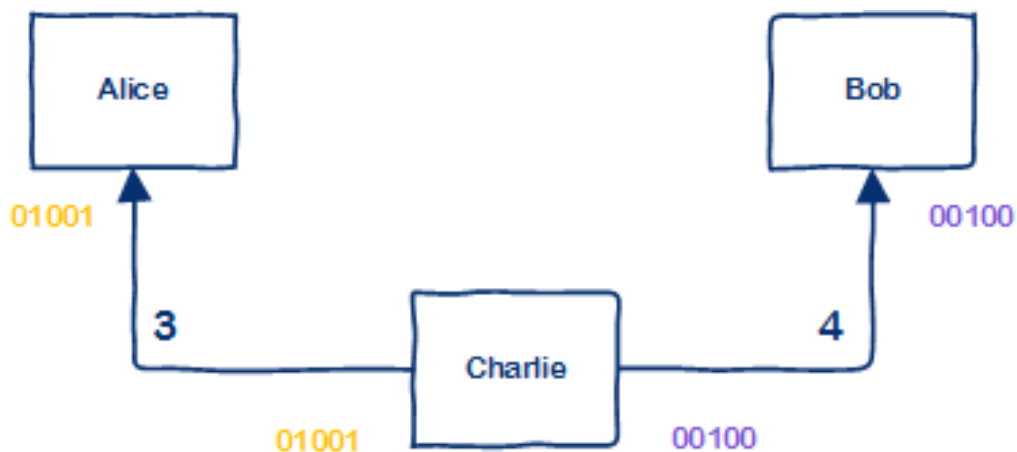


Рис. 3. Доверенный центр должен передать ключи Алисы и Боба Бобу и Алисе соответственно

Для передачи Алисе и Бобу ключей Боба и Алисы соответственно Чарли связывается с каждым и сообщает последовательность корректно выбранных детекторов на шаге 2 таким образом, чтобы их конечные значения повторяли ключ Боба и Алисы (Рис. 4).

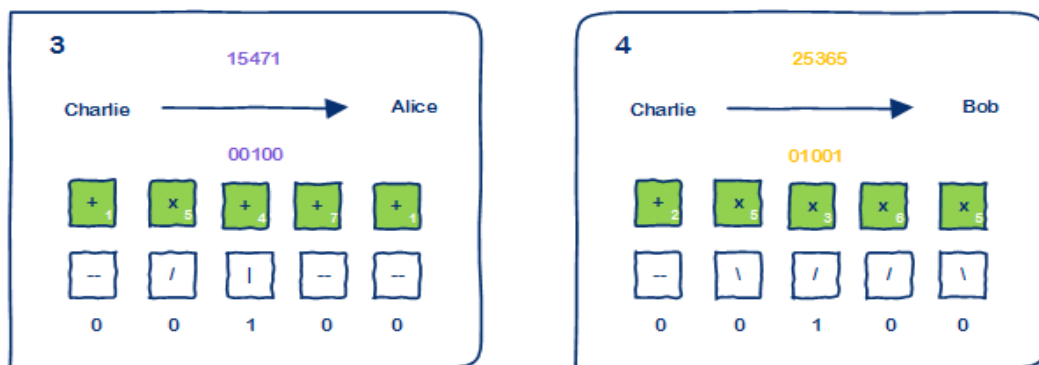


Рис. 4. Передача ключей на основании ранее выбранных верных детекторов

Получив ключ Боба, Алиса склеивает его ключ со своим, получая ключ большей длины. Боб делает то же самое, склеивая ключ Алисы со своим. В итоге Алиса и Боб имеют ключ длины равной сумме длин их ключей. Они могут шифровать и расшифровывать информацию на полученном ключе (Рис. 5).

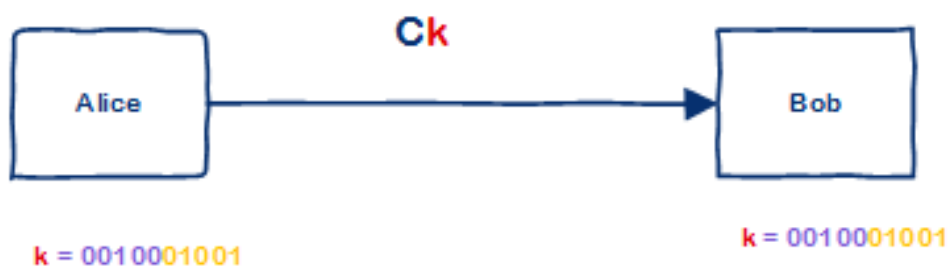


Рис. 5. Шифрование данных ключом, полученным конкатенацией ключей

Выводы. Достоинством предложенного авторами метода является увеличение полезной длины ключа при тех же значениях длины квантовой передачи в оригинальной схеме BB84 в R раз, где R принадлежит интервалу от 1 до 2. R стремится к 2, когда длина сообщений квантовой передачи стремится к бесконечности.

Кроме того, данный метод увеличивает стойкость за счет того, что для получения полного ключа шифрования злоумышленнику потребуется перехватывать информацию одновременно на двух каналах, что требует больших временных и материальных затрат. При этом вероятность обнаружения вмешательства в канал обмена фотонами вырастет. Временные затраты не оказывают значительного влияния, если доверенный центр способен принимать и передавать информацию одновременно для обоих абонентов, участвующих в процессе передачи.

Литература

1. Востоков Н., Борисова С.Н. Квантовая криптография // Успехи современного естествознания. 2012. №6. С. 88-90.
2. Кулик С., Квантовая криптография // Фотоника. 2013. №2. С. 36-41.
3. Кайраллапова А.Н. Стойкость протокола BB84. Караганда. 2014. С. 227-228.
4. Кронберг Д.А., Молотков С.Н. Квантовая схема для оптимального прослушивания протокола квантового распределения ключей BB84 // Известия Российской академии наук. Серия физическая. 2010. № 7. С. 954-960.
5. Пономарева В.В., Розова Я.С. Протоколы квантового распределения ключей // Прикладная информатика. 2014. С. 113-123.

Quantum Key Distribution with a Trusted Centre

Lebedev A.N., Sokolov A. V.¹⁵⁹

Abstract. We propose to implement and use a trusted key distribution centre to make well known protocol BB84 more secure and more reliable. An exact scheme implementing the new protocol described in details and analyzed. The additional expenses to implement the trusted key distribution centre do not make the total cost of the system unacceptable. This method makes the new quantum key distribution protocol much more secure and reliable.

Keywords: quantum key distribution, quantum cryptography, key distribution centre, BB84 protocol.

¹⁵⁹ ¹ Anatoly Lebedev, PhD, Senior Researcher, BMSTU, Moscow, lan@lancrypto.com; ² Alexander Sokolov, BMSTU, Moscow, sav193@yahoo.com

Способ строгой многофакторной аутентификации**Лебедев А. Н., Степанов Б.А., Онуфриев С. В.¹⁶⁰**

В работе предложен способ строгой многофакторной аутентификации пользователей компьютерных систем, сочетающий криптографические алгоритмы с биометрическими. Способ позволяет значительно повысить надежность аутентификации, а также защититься от угрозы несанкционированного проникновения в систему при работе пользователя под внешним контролем или принуждением. Предлагаемый способ строгой многофакторной аутентификации может быть применен в различных практических системах, от систем дистанционного банковского обслуживания до систем регулирования доступа в выделенные помещения.

Ключевые слова: строгая многофакторная аутентификация, биометрические методы, криптографические преобразования, ключи, системы регулирования доступа

Введение. В большинстве современных компьютерных систем, систем дистанционных электронных интернет-услуг, дистанционных банковских услуг, систем регулирования доступа к облачным хранилищам данных и др. используют двухфакторную аутентификацию пользователей. Первым фактором является комбинация логина и пароля пользователя, а главным фактором – результат выполнения криптографического преобразования информации, составляющей запрос сервера или формируемое пользователем сообщение (такая аутентификация называется строгой) [1-2].

С другой стороны, в системах регулирования доступа в выделенные важные помещения или рабочие зоны как правило используются методы аутентификации пользователей по их биометрическим характеристикам таким, как отпечатки пальцев, рисунок кисти руки или сетчатки глаз и т.п. [3-5].

Двухфакторная строгая аутентификация. Каждый из этих методов аутентификации имеет свои достоинства и недостатки. Какой бы стойкий криптографический алгоритм не лежал в основе строгой аутентификации, но пользователь аутентифицируется системой лишь по наличию в его распоряжении средства выполнения криптографического преобразования, а также по знанию ключей аутентификации.

Передача логина, пароля, средства и ключей аутентификации другому пользователю или кража их (компрометация) лишает систему возможности отличить легального пользователя от злоумышленника. Для борьбы с этой опасностью предпринимаются определенные меры. Криптографические преобразования выносятся на отдельные аппаратные модули аутентификации – токены или смарт-карты, в защищенной памяти которых закрытые ключи аутентификации хранятся без возможности их извлечения. Доступ к ключам, а также к самим токенам защищается паролем. Это позволяет снизить опасность обмана системы злоумышленником, но не исключает такой возможности.

Биометрическая аутентификация. При аутентификации пользователей по их биометрическим характеристикам гарантируется невозможность передачи этих параметров. Аутентификация пользователя невозможна без его участия. Однако уровень надежности такой аутентификации уступает уровню надежности при использовании криптографических преобразований [3-5].

Успешное прохождения процедуры аутентификации не подтверждается

¹⁶⁰ ¹Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., МГТУ им. Н.Э. Баумана, Москва, lan@lancrypto.com, ² Степанов Борис Александрович, МГТУ им. Н.Э. Баумана, Москва, gtx360@mail.ru, ³ Онуфриев Сергей Владимирович, МГТУ им. Н.Э. Баумана, Москва, gtx360@mail.ru

документально, а только реакцией сервера. Поэтому такой факт не может быть в дальнейшем проверен при расследовании инцидентов с той степенью достоверности, с какой это может быть проделано на основании электронных документов с электронной подписью [1-2].

Строгая многофакторная аутентификация. До настоящего времени перечисленные два подхода к аутентификации существуют в технических решениях изолированно и используются для различных целей. Так, в системах электронных платежей через интернет применяются способы аутентификации первого типа, а в локальных системах регулирования доступа в помещения с ограничением доступа применяются системы аутентификации второго типа.

Современный уровень развития микроэлектроники позволяет успешно сочетать оба этих подхода для реализации гораздо более надежных способов аутентификации как локально, так и дистанционно через интернет. Мы предлагаем такой способ.

Пользователь располагает по меньшей мере двумя персональными устройствами для аутентификации: биометрическим датчиком, позволяющим локально снимать показания некоторых биометрических показателей пользователя, а также аппаратным персональным модулем аутентификации (смартфоном, токеном или смарт-картой, мы будем в дальнейшем называть его просто токеном).

В качестве биометрического датчика могут выступать «умные часы», которые позволяют частоту пульса, артериальное давление, частота дыхания и др. Другими вариантами биометрического датчика могут выступать сканеры отпечатков пальцев, сетчатки глаза, фотокамеры, и т.д.

Биометрические датчики выступают в роли дополнительного фактора аутентификации, защищающего от попытки аутентификации без участия пользователя, которая возможна в системах строгой двухфакторной аутентификации [1-2].

Кроме того, дополнительно к привычным биометрическим характеристикам пользователя (отпечатки пальцев, рисунок сетчатки глаза), современные дешевые и компактные микропроцессорные устройства измерения показателей пользователя такие, как микро акселерометры, позволяют внести в список возможных биометрических характеристик пользователя более тонкие характеристики. Например, характерные движения кистей рук при наборе на клавиатуре компьютера.

В дополнение к индивидуальным биометрическим характеристикам пользователя, которые являются его неотторжимыми параметрами, для аутентификации применяется также персональный аппаратный модуль аутентификации. Этот модуль позволяет выполнять непосредственно в защищенной памяти своего процессора криптографические преобразования информации, которые собственно и делают аутентификацию строгой (генерацию ключевых пар, хэширование данных, создание и проверку электронной подписи).

Такое сочетание биометрического подхода к аутентификации пользователей с криптографическим подходом позволяет значительно повысить надежность аутентификации без внесения дополнительного неудобства для пользователей и без значительного удорожания всей системы аутентификации.

Выводы.

Разработан комплексный способ строгой многофакторной аутентификации, включающий в себя следующие четыре фактора: постоянные (долговременные) логин и пароль пользователя; имя и ПИН-код или биометрические характеристики пользователя для доступа к памяти и функциям аппаратного криптографического модуля

аутентификации (токена или смарт-карты); цифровой ответ токена на запросы сервера аутентификации на основе криптографических преобразований с индивидуальными ключами аутентификации непосредственно в защищенной памяти процессора токена (в виде одноразового пароля или электронной подписи под запросом сервера аутентификации); дополнительные биометрические (или поведенческие) характеристики пользователя (пульс, движение кистей рук и т.п.), измеряемые другим пользовательским устройством (умные часы, акселерометры и т.п.), используемые как дополнительный фактор аутентификации.

Этот способ аутентификации позволяет значительно расширить спектр областей применения строгой комплексной аутентификации без снижения ее надежности и внесения неудобства для пользователей.

Подготовлена заявка на патент.

Литература

1. Афанасьев А.А., Веденев Л.Т., Воронцов А.А., Газизова Э.Р., Додохов А.Л., Крячков А.В., и др. Аутентификация. Теория и практика обеспечения доступа к информационным системам. Учебное пособие для вузов. 2-е изд., стереотип. М.: Горячая линия – Телеком, 2012. 550с.
2. Лебедев А. Н. Электронная подпись: новый этап // ВестникМГАДА. 2013 № 1(20). С. 43-51.
3. Global Platform Trusted User Interface API Specifications // Global Platform // Accessed March 2014. URL: <https://globalplatform.org/specifications.asp>
4. A. Barth The Web Origin Concept // RFC 6454. IETF. 2011. 67 с. URL: <http://www.ietf.org/rfc/rfc6454.txt>
5. J. Altman, N. Williams, L. Zhu, hannel Bindings for TLS // RFC 5929 // IETF. 2010. 73 с. URL: <http://www.ietf.org/rfc/rfc5929.txt>

A Strong Multifactor Authetication Method

Lebedev A.N., Stepanov B. A., Onufriev S.V.¹⁶¹

Abstract. A new strong multifactor authentication method has been invented. The method is a combination of some biometric authentication procedures with some cryptographic transformations used as a part of strong two-factor authentication. The method gives an opportunity to rise up security level of authentication without additional inconvenience for a user. This method of authentication could be effectively used for a wide range of computer networks as well, as for the internet payments systems and access management systems.

Keywords: strong multifactor authentication, biometric authentication, cryptographic transformations, access regulation.

¹⁶¹ Bauman Moscow State Technical University, Moscow

Кибербезопасность в критических инфраструктурах (на примере энергетики)

Массель А.Г.¹⁶², Массель Л.В.¹⁶³, Гаськова Д.А.¹⁶⁴

Предлагается осуществлять выявление и ранжирование критически важных объектов энергетической инфраструктуры, с учетом требований кибербезопасности, на основе риск-ориентированного подхода, включающего анализ угроз критических ситуаций, уязвимостей энергетических объектов и ущербов при реализации угроз. Для выявления уязвимостей энергетических объектов разработаны «Методика анализа угроз и оценки рисков нарушения безопасности энергетических комплексов» и реализующий ее научный прототип экспертной системы.

Ключевые слова: критическая инфраструктура, энергетический сектор, кибербезопасность, критически важный объект, риск-ориентированный подход

Критической инфраструктурой называется часть гражданской инфраструктуры, представляющая собой совокупность физических или виртуальных систем и средств, важных для государства в такой мере, что их выход из строя либо уничтожение может привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации. В случае военных действий одной из важнейших целей для поражения считается такая инфраструктура, выведение из строя или уничтожение которой может привести к ущербу, сопоставимому с ударами, наносимыми по вооруженным силам. Современные тенденции в исследовании критических инфраструктур в США рассмотрены, например, в [1]. Выделены 11 важнейших секторов, которые представляют собой иерархическую структуру: на первом (базовом) уровне выделяют информационно-телекоммуникационный сектор, энергетический сектор и сектор водообеспечения; на втором – банковский сектор, транспортный и сектор химической промышленности; третий уровень представлен военно-промышленным комплексом, почтовой службой, морским транспортом, продовольственным сектором, здравоохранением, а также чрезвычайными службами.

Под энергетической инфраструктурой России, которую относят к критически важным инфраструктурам, понимается совокупность энергетических объектов и систем энергетики, включая энергетические транспортные магистрали. Авторы считают, что безопасность энергетической инфраструктуры должна рассматриваться в тесной связи с кибербезопасностью [2, 7].

Согласно стандарту ISO 27032:2012, кибербезопасность базируется на пяти составляющих: безопасность приложений, информационная безопасность, сетевая безопасность, безопасность интернет-приложений и защита ключевых информационных систем объектов критических инфраструктур, но не является синонимом ни одного из них [3]. Защита ключевых информационных систем объектов критической инфраструктуры рассматривается авторами в контексте критически важных секторов, например, таких, как энергетика. Защита критической информационной инфраструктуры предполагает обеспечение гарантии того, что подобные системы и сети устойчивы в отношении рисков информационной безопасности, сетевой безопасности, безопасности Интернет, равно как и рисков кибербезопасности.

Важную роль в обеспечении безопасности энергетической инфраструктуры играет энергетическая безопасность (ЭБ). Угрозы ЭБ традиционно систематизируются в пять

¹⁶² Массель Алексей Геннадьевич, канд. техн. наук, ИСЭМ СО РАН, Иркутск, amassel@isem.irk.ru

¹⁶³ Массель Людмила Васильевна, д-р техн. наук, профессор, ИСЭМ СО РАН, Иркутск, massel@isem.irk.ru

¹⁶⁴ Гаськова Дарья Александровна, ИСЭМ СО РАН, Иркутск, 256341@mail.ru

основных групп: экономические, социально-политические, техногенные, природные и управленческо-правовые [4]. Авторами предложено расширить этот перечень угрозами кибербезопасности, реализация которых может спровоцировать серьезные чрезвычайные ситуации в энергетике, чреватые значительным снижением возможностей обеспечения энергоресурсами потребителей.

Критически важными объектами (КВО) называют ключевые объекты (или их совокупности) соответствующих инфраструктур, воздействие на которые может оказать наиболее негативный эффект на отрасль экономики, ключевой ресурс или всю инфраструктуру. В исследованиях критических инфраструктур особое внимание уделяется выявлению КВО, а также оценке последствий воздействия на них и разработке механизмов снижения рисков таких воздействий [1].

До настоящего времени в Российской Федерации не создана нормативная база стандартов (с учетом зарубежного опыта и специфики России), методик обеспечения кибербезопасности, регулирующая проблемы обеспечения кибербезопасности КВО в целом и объектов энергетики и энергетических систем в частности. В то же время МЧС России в 2012 г. утвердило «Методику отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности РФ». На ее основе разработана, в частности, методика формирования перечня КВО газотранспортной сети [5]. Данная методика направлена на одну из энергетических систем – газовую, в отдельно взятой проблеме её транспортировки. Авторами методики предложен показатель выявления КВО газотранспортной сети, определяемый на основе суммарной относительной недопоставки газа потребителям (5 % и более) в результате нарушения работы этих объектов. Ранжирование объектов по степени значимости для экономики страны в целом и отдельных ее регионов в данной методике не предусматривается. Авторы предлагают выполнять такое ранжирование на основе анализа возможных критических ситуаций (КС) и учета рисков КС.

Риск-ориентированный подход для выявления КВО в энергетике учитывает ущерб от повреждения или уничтожения объекта с использованием качественных (сложность восстановления, уничтожение уникальной природной среды, имидж и иное) и количественных (в денежном эквиваленте) параметров, а также вероятность повреждения или уничтожения объекта, с учетом возможности наступления каскадных аварий. Далее предлагается ранжировать критически важные объекты на основе анализа возможных КС и учета рисков КС.

Риски определяются тройкой $R = \{T, V, D\}$,

где T – угрозы КС, V – уязвимости КВО, D – ущерб при реализации угрозы.

Угрозы определяются через вероятности наступления событий, приводящих к критическим ситуациям (например, условные вероятности, используемые в байесовских сетях). Качественный ущерб выражается в денежном эквиваленте с использованием экспертных оценок. Для выявления уязвимостей энергетических объектов авторами разработана «Методика анализа угроз и оценки рисков нарушения безопасности энергетических комплексов», основанная на поэтапном анализе и методе экспертных оценок. В настоящее время реализован научный прототип экспертной системы, реализующей эту методику [6].

Литература

1. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах / Зарубежное военное обозрение. - 2012. - № 1. - С. 19-30.
2. Massel L., Massel A. Cyber security of Russia's energy infrastructure as a component of national security. / Proceeding of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. – 2015. – Saint Petersburg - С. 66-72.
3. Мохор В. В., Богданов А. М., Килевой А. С. Наставления по кибербезопасности : изложение стандарта ISO/IES 27032:2012 / Информационные технологии. - Методы обеспечения безопасности. - Наставления по кибербезопасности." - Киев: Три-К, 2013. - 129 с.
4. Энергетическая безопасность России: проблемы и пути решения / Н.И. Пяткова, В.И. Рабчук, С.М. Сендеров, М.Б. Чельцов. Отв. ред. Воропай Н.И. – Новосибирск: Изд-во СО РАН, 2011. – 211 с.
5. Еделев А.В., Сендеров С.М., Сидоров И.А. Применение распределенных вычислений для выявления критически важных объектов газотранспортной сети России // Информационные и математические технологии в науке и управлении. □ 2016. □ №1. □ С. 55-62.
6. Гаськова Д.А., Массель А.Г. Разработка экспертной системы для анализа угроз кибербезопасности в энергетических системах // Информационные и математические технологии в науке и управлении. - 2016. - №1. - С. 113-122.
7. Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4(17). С. 2-10.

Cybersecurity of Critical Infrastructures (On the Example of Energy Sector)

Massel A.G.¹⁶⁵, Massel L.V.¹⁶⁶, Gaskova D.A.¹⁶⁷

It is proposed to carry out the identification and ranging of critical facilities in energy infrastructure, taking into account the cybersecurity requirements, with using of risk-based approach that includes an analysis of the critical situations threats, vulnerabilities for energy facilities and damage at the implementation of threats. In order to identify vulnerabilities the authors developed "Methods for analysis of threats and risk assessment of security breaches in energy complexes" and implemented research prototype of an expert system realizing this methods .

Keywords: critical infrastructure, energy sector, cybersecurity, critical facilities, risk-based approach.

¹⁶⁵ Aleksei Massel, Ph.Dm, Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, amassel@isem.irk.ru

¹⁶⁶ Liudmila Massel, Dr.Sc., Professor, Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, massel@isem.irk.ru

¹⁶⁷ Daria Gaskova, Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, 256341@mail.ru

NTLM-авторизация при интеграции данных через ESBЛуценко А.Э.¹⁶⁸

В статье рассматривается работа с сервисной шиной предприятия: изучаются задачи, которые она выполняет, анализируются возможные подходы по взаимодействию систем с помощью шины данных. Также в данной статье рассматривается способ ограничения доступа к web-сервисам с помощью программных продуктов, реализующих работу с ESB.

Ключевые слова: шина данных, интеграция между системами, WebSphere Message Broker

Введение

ESB (enterprise service bus) или сервисная шина предприятия предназначена для объединения всех приложений и систем компании. Также шина данных позволяет централизованно управлять доступом, контролировать трафик и наблюдать количество обращений к сервисам предприятия, контролировать наличие ошибок при обращении к сервисам, отслеживать скорость работы сервисов.

Цели внедрения шины данных:

- ✓ интеграция существующих и подключение новых сервисов и приложений компании;
- ✓ управление взаимодействием сервисов и приложений, введение логики маршрутизации сообщений и трансформации данных сообщения;
- ✓ составление единого реестра используемых сервисов;
- ✓ централизованное управление доступом к сервисам;
- ✓ сбор информации и статистики по использованию сервисов;
- ✓ получение оперативной информации по работоспособности сервисов;
- ✓ протоколирование обращений к сервисам, логирование ошибок вызова сервисов.

К программным продуктам, которые реализуют работу с ESB, относятся WebMethods ESB, WebSphere Message Broker, ActiveMatrix Service Bus, Oracle Service Bus.

Принципы интеграции между системами

Самый простой случай взаимодействия представлен на рис.1. В данном варианте присутствует только одна система-источник (система, из которой посылается запрос) и только одна система-приемник (система, которая отвечает на запрос). Также возможны взаимодействия, при которых несколько систем-источников и несколько систем-приемников.



Рис. 1. Схема взаимодействия систем при помощи ESB

Система-приемник может использовать для определения уникальности объекта идентификаторы НСИ (номенклатурно-справочная информация), Крок-коды (Уникальный для всех систем код объекта, присваиваемый в момент создания в мастер-системе и неизменный на протяжении существования объекта), либо пользоваться собственными идентификаторами.

¹⁶⁸ Луценко Анна Эдуардовна, МГТУ им.Н.Э.Баумана, г.Москва, lutsenko.anna.94@gmail.com

Взаимодействие также может осуществляться различными способами с технической точки зрения:

- ✓ через MQ-очереди. В них помещается сообщение, которое чаще всего содержится в XML-формате
- ✓ через SOAP-сервис. При этом способе взаимодействия системы предоставляют сервис, способный обрабатывать датаграммы.
- ✓ через HTTP-запрос. В данном случае сообщения передаются в формате JSON.

При этом методы взаимодействия у систем-приемников и систем-источников могут отличаться.

Ответ от системы может содержать собственно нужную информацию, информацию о произошедших ошибках, либо просто информацию об успешности обработки датаграммы. Также можно работать с интеграциями, которые осуществляют сообщение только в одну сторону (система-источник → ESB → система-приемник).

Аутентификация на web-сервисах ESB

Шина предоставляет возможность использования Basic или NTLM –аутентификации. Протокол NTLM (NT LAN Manager) применяется для аутентификации компьютеров рабочих групп, в доменных сетях Active Directory. При разработке это реализуется путем добавления специального модуля (в рамках работы с IBM Websphere называется нодой) при разработке Security PEP:

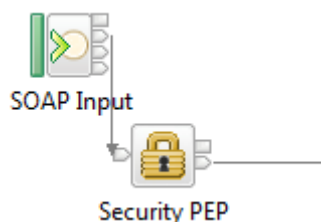


Рис.2. Security REP

Данная нода позволяет создать настройки на брокере, которые позволяют подключаться к web-сервису только определенным пользователям или роботам. В противном случае появляется ошибка 401 Unauthorized. Например, после соответствующей настройке подключиться сможет только пользователь ALutsenko.
mqsisetdbparms testBrocker -n ldap::acdc -u alutsenko@croc.ru -p password

Пример подключения показан на рис.3. Для тестового подключение используется программы SOAP UI.

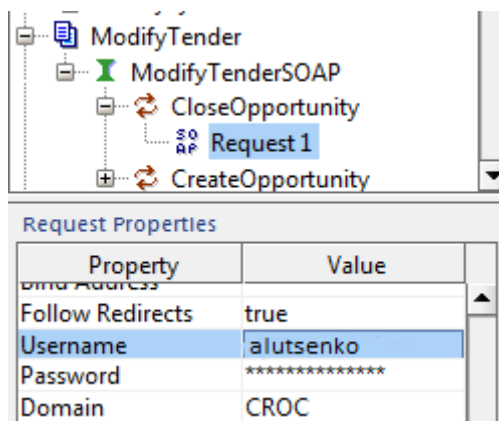


Рис.3. Пример подключения пользователя

При настройке авторизации ссылка на сервис никак не изменяется, соединение осуществляется по http.

Шифрование пароля

В рамках данной работы разработана отдельная программа, которая позволяет шифровать пароль для доступа к web-сервису. Принцип кодирования данных зависит от стенда, на котором выполняется запрос. Это сделано для того, чтобы шифрование боевого пароля могло быть произведено только на боевом стенде, доступ к которому есть только у менеджеров проекта.

На рис.4. и рис.5. представлен пример работы данного метода на тестовом стенде.

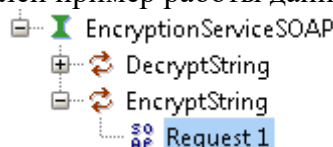


Рис.4. Сервис для шифрования пароля

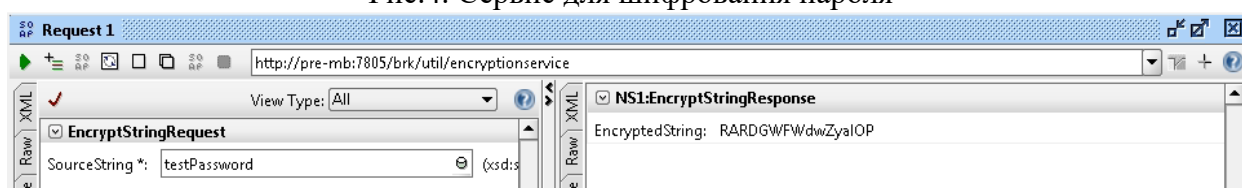


Рис.5. Пример работы сервиса

Заключение

В результате данной работы был проведен разбор способов взаимодействия с сервисной шиной предприятия (ESB) и методов ограничения доступа для подключения к web-сервисам шины. Также был изучен метод NTLM-авторизации. Был разработан специальный метод для шифрования паролей пользователей или роботов, который зависит от среды запуска.

Литература

1. Корпоративная сервисная шина - "бюджетный" подход к решению задач интеграции // citforum URL: <http://citforum.ru/internet/webservice/esb/> (дата обращения: 30.10.2016).
2. Программное обеспечение websphere // IBM URL: <https://www-01.ibm.com/software/ru/websphere/> (дата обращения: 30.10.2016).
3. IBM WebSphere MQ Explorer // IBM URL: <https://www-01.ibm.com/software/integration/wmq/explorer/downloads/> (дата обращения: 30.10.2016).
4. Аутентификация в системах Windows. Часть 1 - NTLM // Записки IT специалиста URL: https://interface31.ru/tech_it/2015/03/autentifikaciya-v-sistemah-windows-chast-1-ntlm.html (дата обращения: 31.10.2016).
5. SecurityLab.ru // NTLM и корпоративные сети URL: <http://www.securitylab.ru/contest/212100.php> (дата обращения: 31.10.2016).

Научный руководитель: Волосатова Тамара Михайловна, канд. техн. наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, г. Москва, tamaravol@gmail.com

NTLM-Authentication in Case of Integration of Data Through ESB

Lutsenko A. E.¹⁶⁹

Abstract. In article operation with the service bus of the enterprise is considered: tasks which it carries out are studied, possible approaches on interaction of systems by means of the data bus

¹⁶⁹ Bauman Moscow State Technical University, Moscow

are analyzed. Also in this article the access restriction method to web services by means of the software products realizing operation with ESB is considered.

Keywords: the data bus, integration between systems, WebSphere Message Broker

УДК 004.382.7

Современные криптоконтроллеры для построения эффективных подсистем безопасности автономных систем

Максимов Р.Л.¹⁷⁰, Рафиков А.Г.¹⁷¹

Проведён анализ доступных на рынке микроконтроллеров известных фирм-производителей. Сформулирован ряд требований для подсистемы обеспечения информационной безопасности автономных устройств. Сформирован перечень доступных криптоконтроллеров ведущих производителей, удовлетворяющих требованиям, предъявляемым к компонентам подсистемы безопасности автономных систем. Предложен алгоритм выбора криптоконтроллера для решения задач информационной безопасности.

Ключевые слова: автономные системы, микроконтроллеры, криптоконтроллеры, аппаратная поддержка шифрования, AES, DES, режимы энергосбережения, банкоматы, АТМ.

Введение

Типичными примерами автономных систем являются банкоматы, торговые автоматы, билетопечатающие автоматы. Денежные машины ведут своё начало с далекого 1967 года, когда в отделении банка Barclays в Лондоне был установлен первый экземпляр банкомата. В настоящее время миллионы человек по всему миру ежедневно используют банкоматы для снятия наличных, пополнения счетов, оплаты различных услуг. Люди пользуются банкоматами, зачастую не задумываясь об их аппаратной начинке, программных особенностях и безопасности. К сожалению, производители банкоматов и их непосредственные потребители – банки не уделяют вопросам защищенности банкоматов достаточного внимания. Такая беспечность привела к тому, что киберпреступность в части информационных атак на банкоматы приобрела небывалый размах. Это обстоятельство выдвигает на повестку дня проблему создания и повсеместного внедрения средств защиты автономных систем. Особенно остро эта проблема касается автономных систем, имеющих функции выдачи и хранения наличных денег.

Для построения подсистем безопасности автономных систем используются методы, основанные на применении шифрования и защитного кодирования, для программной реализации которых требуются высокопроизводительные микропроцессоры и микроконтроллеры. В настоящее время ведущие производители полупроводниковых приборов наряду с созданием высокопроизводительных универсальных микроконтроллеров выпускают специализированные микроконтроллеры, ориентированные, например, на решения с использованием криптоалгоритмов и имеющих для их реализации соответствующую аппаратную поддержку.

При создании подсистем безопасности крайне важно обеспечить надёжный обмен информацией и предотвратить любые попытки несанкционированного доступа к информационным и вычислительным ресурсам, а также перехвата и/или изменения информации, в частности команд управления или кодов аутентификации.

¹⁷⁰Максимов Роман Леонидович, МГТУ им. Н.Э. Баумана, г. Москва, r.l.maksimov@gmail.com.

¹⁷¹Рафиков Андрей Гызович, МГТУ им. Н.Э. Баумана, г. Москва, iu8asvt@gmail.com.

Криптоконтроллеры предоставляют разработчикам обширный арсенал для высокопроизводительной и надёжной реализации криптографических алгоритмов:

- получение истинно случайных чисел для формирования надёжных ключей шифрования (используя встроенный ГИСЧ);

- получение псевдослучайных чисел для формирования сеансовых ключей и их синхронизации;

- аппаратное шифрование и расшифровывание данных стойкими алгоритмами;

- обеспечение надёжного и безопасного способа хранения и обновления ключей в течение продолжительного времени непосредственно в памяти, на кристалле микроконтроллера или памяти, расположенной в пределах печатной платы системного контроллера;

- аппаратная поддержка вычисления хэш-функций;

- обеспечение целостности используемых криптографических алгоритмов.

Отдельно следует отметить, что такие устройства должны функционировать продолжительное время даже в отсутствие внешнего питания. Для этого следует ориентироваться на микроконтроллеры с низким энергопотреблением и наличием возможностей для подключения автономного источника резервного электропитания, который позволяет избежать внезапного обесточивания микроконтроллера.

Одной из главных задач разработчика средств защиты информации является грамотный, взвешенный и обоснованный выбор криптоконтроллера, который должен иметь оптимальный и эффективный набор средств аппаратной поддержки вычислений, с учётом всех сопутствующих требований и возможных угроз со стороны злоумышленников.

Приведённый перечень криптоконтроллеров и набор их ресурсов позволяют понять существующие возможности в части аппаратной поддержки криптографических алгоритмов. Перечень можно рассматривать как набор требований для идеального криптоконтроллера, предназначенного для решения задач защиты информации любой сложности. Однако, далеко не каждый криптоконтроллер имеет весь арсенал необходимых средств, и далеко не все задачи информационной безопасности требуют для своего решения одинаковых ресурсов.

Для правильного и обоснованного выбора криптоконтроллера, являющегося, зачастую, ядром разрабатываемой подсистемы защиты от кибератак, рассмотрим криптоконтроллеры ведущих фирм-производителей с учётом сформулированных требований к «идеальному» криптоконтроллеру.

Микроконтроллеры ведущих фирм-производителей

Микроконтроллеры PIC компании Microchip

Компания Microchip выпускает обширную номенклатуру 8-, 16- и 32-битных микроконтроллеров. В рамках публикации будем рассматривать микроконтроллеры, которые имеют аппаратную поддержку шифрования, называемые также криптоконтроллерами.

Семейство 16-битных микроконтроллеров (PIC24)

Особый интерес представляет семейство PIC24FJ, представленное двумя основными линейками: «GB» и «GA» (с поддержкой USB и без, соответственно). Микроконтроллеры ориентированы на применение в промышленных контроллерах и имеют обширный набор встроенного периферийного оборудования и подсистем для решения широкого круга производственных задач. Микроконтроллеры семейства имеют схожие характеристики; основные отличия связаны с типом корпуса, количеством выводов, объёмом памяти программ и размером ОЗУ. Типичные представители семейства – микроконтроллеры с аппаратной поддержкой шифрования: PIC24FJ128GB202(204).

Все криптоконтроллеры семейства обеспечивают аппаратную поддержку AES с ключом 128, 192 и 256 бит (включая режимы ECB, CBC, OFB, CTR и CFB128), DES, 3DES (включая до трёх ключей шифрования 3DES). При этом, обеспечивается дополнительная безопасность ключа шифрования при помощи его однократного программирования и защиты от считывания и перезаписи.

Реализация алгоритма TDES на микроконтроллерах PIC24 в обычном режиме для шифрования\расшифровывания одного блока (8 байт) данных потребуются 6403 или 13557 циклов (в зависимости от требований к ключу) синхронизации, что при частоте 32 МГц займёт 200 мкс и 423 мкс, соответственно. Реализация AES-128 потребует 2808 циклов синхронизации для шифрования блока данных (16 байт), расшифровывание – 4490, что займёт 87,75 мкс и 140,3 мкс, соответственно.

Режим с использованием батарейного питания Vbat обеспечивает работу часов реального времени и регистров DSGPR0 и DSGPR1, которые могут быть использованы для сохранения критических данных, при низком потреблении (менее 0.4 мкА). Криптографические возможности микроконтроллера в данном режиме недоступны.

Дополнительный режим энергосбережения «Deep Sleep» схож с предыдущим, но является программируемым и, кроме всего прочего, обеспечивает работу генератора с частотой 32 кГц, потребляемый ток ~ 1 нА при напряжении 2,0 В и ~ 75 нА при 3,3 В.

Семейство 32-битных микроконтроллеров (PIC32)

Аппаратная криптография, в дополнение к имеющимся возможностям в 16-битных криптоконтроллерах, имеет поддержку SHA, MD5 и HMAC. Отсутствие таких режимов энергосбережения, как Vbat и «Deep Sleep», ограничивает использование продукции данного семейства в проектах критичных к энергопотреблению.

Отличительной особенностью продукции компании Microchip является наличие моделей микроконтроллеров с технологией сверхмалого энергопотребления «eXtreme Low Power», в режиме хранения ОЗУ потребляемый ток не превышает 330 нА (<https://www.microchip.com/design-centers/xlp>), что позволяет использовать их в проектах с повышенными требованиями к энергопотреблению. Это особенно важно в случае применения алгоритмов, где для обеспечения высокой криптостойкости не один – два, а целые массивы криптоключей, которые необходимо длительное время хранить в энергонезависимой памяти.

Помимо самих криптоконтроллеров Microchip предоставляет для своей продукции интегрированную среду разработки MPLAB X и бесплатные библиотеки для работы с USB, TCP/IP стеком, криптографией (<https://www.microchip.com/mplab/microchip-libraries-for-applications>).

Микроконтроллеры ARM компании STMicroelectronics

Основные изделия в линейке продукции STMicroelectronics – это 8- и 32-битные микроконтроллеры с ARM архитектурой. В рамках тематики рассматриваются только те микроконтроллеры, у которых имеется аппаратная поддержка криптографических алгоритмов.

Семейство «Very high performance»

Линейка STM32 F7 имеет высокие показатели энергосбережения, при работе от батареи Vbat с сохранением состояния ОЗУ и активными часами реального времени (от 1.06 мкА и выше в зависимости от модели при напряжении 1.7 В и от 1.41 мкА при 3.3 В), включает обширный набор поддерживаемой криптографии (AES 128, 192, 256, 3DES, хеш-функции (MD5, SHA-1, SHA-2), HMAC) и наличие генератора истинно-случайной последовательности. Использование встроенного генератора 16 МГц позволяет зашифровать блок данных алгоритмом AES-128 за 46 мкс и расшифровать за 53,3 мкс, алгоритмом TDES – 42,1 мкс и 43,1 мкс, соответственно.

Семейство «High performance»

Линейка STM F4 имеет сравнимые показатели с микроконтроллерами семейства «Very high performance» (потребляемый ток при работе тока в режиме Vbat с сохранением состояния ОЗУ и активными часами реального времени от 1.29 мкА при напряжении 1.8 В и от 1.68 мкА при 3.3 В). Аппаратная поддержка криптографии чуть скромнее, чем в старшем семействе (AES 128, 192, 256, 3DES, хеш-функции (MD5, SHA-1), HMAC). Линейка STM F2 по рассматриваемым параметрам полностью повторяет STM F4, за исключением отсутствия аппаратной поддержки HMAC.

Семейство «Ultra-low-power»

Типичными представителями семейства с ультранизким энергопотреблением являются линейки приборов:

STM L4. Невозможно подключить дополнительную батарею без использования дополнительных схем, так как отсутствуют выводы Vbat, но в отличие от других семейств режим «Stop 2 mode» обеспечивает сохранение состояния ОЗУ и работоспособность часов реального времени при токе от 1.3 мкА при напряжении 1.8 В и 1.5 мкА при 3 В. Аппаратная поддержка шифрования подразумевает только AES и недоступна в режимах «Stop mode». В режимах «Low-power-run» и «Low-power-sleep» реализована поддержка большей части периферии, в том числе аппаратной поддержки AES, но отсутствует возможность использования генератора истинно-случайных чисел. В режиме «Low-power-run» обеспечивается ток от 211 нА при рабочем генераторе 2 МГц и от 30 нА при генераторе 100 кГц.

STM L1. Отсутствует генератор истинно-случайной последовательности.

STM L0. Не все микроконтроллеры с аппаратной поддержкой криптографии в линейке имеют генератор истинно-случайной последовательности. Аппаратная поддержка шифрования подразумевает только алгоритм AES. Отсутствует возможность подключения батарейного питания, но в отличие от других семейств режим «Stop mode» обеспечивает сохранение состояния ОЗУ и работоспособность часов реального времени при токе 0,86 мкА и напряжении от 1.65 до 3.0 В. Доступен режим «Low-power-run», в котором доступна большая часть периферии, в том числе аппаратная поддержка AES. Режим «Low-power run» обеспечивает ток ~ 24,5 нА при рабочем генераторе 32/65 кГц и напряжении от 1,65 В до 3,6 В.

STMicroelectronics внимательно относится к проблемам разработчиков систем безопасности и предоставляет бесплатную интегрированную среду для разработки System Workbench for STM32 и внушительное количество дополнительных библиотек, включая STM32 Cryptographic Library (http://www.st.com/content/st_com/en/products/embedded-software/mcus-embedded-software/stm32-embedded-software/stm32-standard-peripheral-libraries-expansions/stm32-cryp-lib.html).

Выводы

Анализ продукции ведущих производителей криптоконтроллеров показывает, что в арсенале разработчиков есть разнообразные средства и инструменты для решения широкого класса задач с использованием криптоалгоритмов по защите автономных систем от различного рода атак. Большинство криптоконтроллеров имеют необходимые для этого показатели: разнообразные режимы пониженного энергопотребления, активные часы реального времени, энергонезависимую память для хранения состояния ОЗУ, аппаратную поддержку широкого спектра криптографических алгоритмов, включая AES, DES, хэш-функции (MD5, SHA), HMAC, генераторы истинно- и псевдослучайных чисел.

Большинство средств защиты информации автономных систем, рассчитанных на защиту от атак типа «black box», должны обеспечивать обнаружение и распознавание атак на автономную систему с последующей блокировкой доступа к критически важному

оборудованию даже в условиях полного отключения питания от защищаемого объекта. В таких условиях особое значение приобретают энергопотребление и производительность криптоконтроллера.

Таким образом, выбор криптоконтроллера, как ядра системы защиты информации, крайне важен и во многом определяет основные параметры будущей подсистемы безопасности. Для того, чтобы сделать правильный выбор криптоконтроллера, необходимо проанализировать все параметры и функционал объекта защиты, рассмотреть возможные угрозы и уязвимости и оценить затраты по их устранению, определить возможности современных доступных криптоконтроллеров различных производителей. На основании проведенного всестороннего анализа - построить модель подсистемы, рассчитать временные затраты для применяемых алгоритмов, сравнить по быстродействию полученные результаты и возможности криптоконтроллеров в части аппаратной поддержки криптопреобразований. После этого можно сделать обоснованный выбор подходящего криптоконтроллера для решения задач по созданию эффективных подсистем безопасности Автономных систем.

Из-за ограничений на объём представляемых материалов в обзор не попали криптоконтроллеры таких известных производителей полупроводниковых компонентов, как NXP (Philips) и Atmel. Кроме того, компания Atmel, не так давно, стала подразделением Microchip, и, поскольку, дальнейшая политика и планы Microchip в отношении Atmel не ясны, продукция компании Atmel не рассматривалась.

Литература

1. Деднев М.А., Дыльников Д.В. и др. Защита информации в банковском деле и электронном бизнесе. М.: КУДИЦ-ОБРАЗ, 2004. 512 с.
2. Кривченко И. Аппаратно-защищенные микросхемы семейства Crypto Authentication: потенциальные применения ATSHA204A // Компоненты и технологии, №10, 2015. СПб.: Издательство Файнстрит. С. 87-93.
3. Юргенсен Т.М., Гатери С.Б. Смарт-карты: настольная книга разработчика / Пер. с англ. М.: КУДИЦ-ОБРАЗ, 2013. 416 с.
4. NIST. P. 800-86 // Guide to Integrating Forensic Techniques into Incident Response. 2006. С. 80-86.
5. Olga Kochetova, Alexey Osipov. Trust No One. ATMs and their dirty little secrets. HITB GSEC, 2016.
6. Материалы сайта компании Microchip [Электронный ресурс]. – Режим доступа: <http://www.microchip.com/design-centers/embedded-security/reference-designs/hardware-crypto-engine>, свободный.
7. Материалы сайта компании STM [Электронный ресурс]. – Режим доступа: <http://www.st.com/en/secure-mcus.html>, свободный.

Научный руководитель: Троицкий Игорь Иванович, канд. техн. наук, доц. каф. ИУ8, МГТУ им. Н.Э. Баумана, г. Москва, iitroickiy@mail.ru.

Modern Crypto-Controllers for Building Effective Technical Security Means of Autonomous Systems

A.Rafikov¹⁷², R.Maksimov¹⁷³

Abstract. Analysis of microcontrollers of well-known manufacturers available on the market is provided. A number of requirements for information security subsystem of stand-alone devices are formulated. The list of available microcontrollers that meet the requirements imposed on the components of security system of autonomous systems is formulated. The selection algorithm of crypto-controllers for solving information security issues is presented.

¹⁷² Rafikov A., Bauman Moscow State Technical University, Moscow, Russia, iu8asvt@gmail.com.

¹⁷³ Maksimov R. Bauman Moscow State Technical University, Moscow, Russia, r.l.maksimov@gmail.com.

Keywords: autonomous systems, stand-alone devices, microcontrollers, crypto-controllers, encryption hardware accelerator, AES, DES, low-power modes, automatic teller machine, ATM.

УДК: 003.26.004.7.004.9

Стеганография на основе ортогональных вейвлетов

Медведев Н.В.¹⁷⁴, Глинская Е.В.¹⁷⁵

Аннотация. В настоящее время в мире предложено огромное количество алгоритмов незаметного встраивания информации в мультимедийные сигналы с использованием вейвлет-преобразования. В данной статье описывается метод защиты изображений на основе ортогональных вейвлет-преобразований. Защита осуществляется путем адаптации используемых вейвлетов к кодируемому сигналу и введения зависимости формы вейвлетов от внешних параметров.

Ключевые слова: защита информации, стеганография, скрывание данных, вейвлет

Введение

Рост объёмов мультимедиа-трафика в глобальной сети Интернет и сотовых сетях связи, широкое распространение цифровых устройств записи - фото- и видеокамер, диктофонов, сканеров привело к увеличению источников мультимедиа-данных, цифровые потоки с которых могут быть использованы для скрытой передачи и хранения информации. За последние десятилетия быстро развиваются методы обработки и анализа информационных сигналов с применением вейвлет-преобразования [4]. Они позволяют исследовать свойства нестационарных сигналов, благодаря операциям масштабирования и сдвига. Разработаны вейвлеты для обработки изображений, обеспечивающие сжатие, декомпозицию, реставрацию, идентификацию изображений, а также удаление из них шумов. В большинстве методов скрывания данных используется та или иная декомпозиция изображения-контейнера.

Линейные ортогональные преобразования в стеганографии

Среди всех линейных ортогональных преобразований наибольшую популярность в стеганографии получили вейвлет-преобразования.

Вейвлет-преобразование несет огромное количество информации о сигнале, но обладает сильной избыточностью, так как каждая точка фазовой плоскости оказывает влияние на его результат.

Для точного восстановления сигнала достаточно знать его вейвлет-преобразование на некоторой довольно редкой решетке в фазовой плоскости и вся информация о сигнале содержится в этом довольно небольшом наборе значений. Идея здесь заключается в том, чтобы масштабировать вейвлет в некоторое постоянное (например, 2) число раз, и смещать его во времени на фиксированное расстояние, зависящее от масштаба. При этом все сдвиги одного масштаба должны быть попарно ортогональны – такие вейвлеты называются ортогональными.

При таком преобразовании выполняется свертка сигнала с некоторой функцией и с вейвлетом, связанным с этой функцией. В результате получаем "сглаженную" версию

¹⁷⁴ Медведев Николай Викторович - канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им. Н. Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5), medvedevnick54@yandex.ru.

¹⁷⁵ Глинская Елена Вячеславовна, МГТУ им. Н.Э. Баумана, Москва, glinskaya-iu8@rambler.ru

исходного сигнала и набор "деталей", отличающих сглаженный сигнал от исходного. Последовательно применяя такое преобразование, можно получить результат нужной степени детальности (гладкости) и набор деталей на разных масштабах.

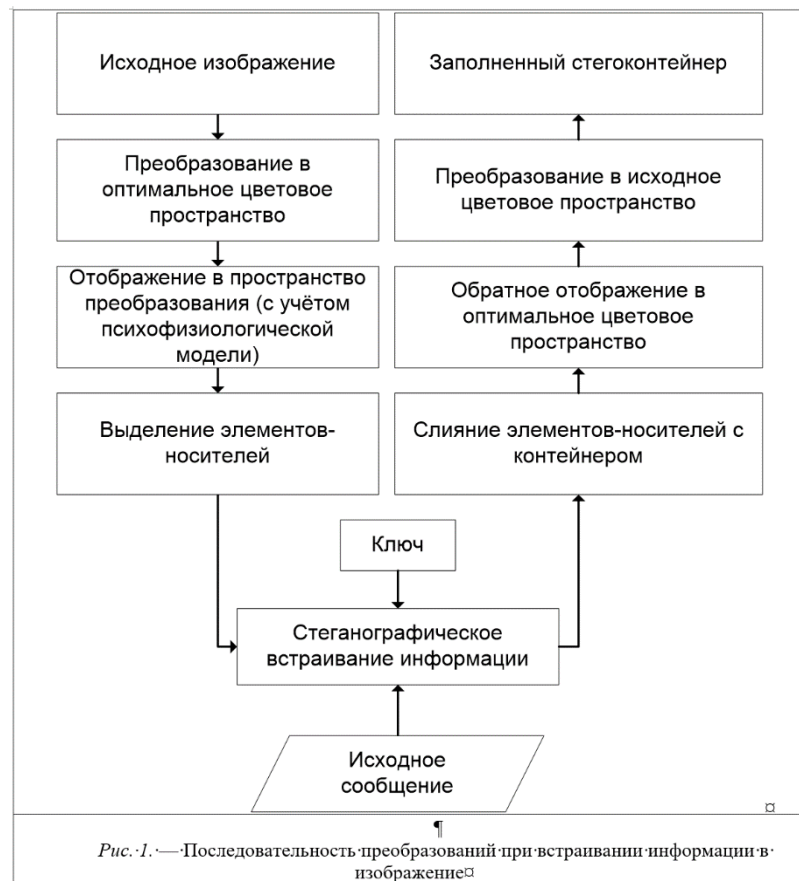
В большинстве случаев получаемые контейнеры представляют собой компрессированные файлы, на основе психофизиологической модели восприятия человека. Использование подобных форматов для встраивания информации непосредственно в пространственно-временной области нецелесообразно ввиду низкой стеганографической стойкости к обнаружению [1].

Использование множества НЗБ-методов (метод замены наименьших значащих бит) встраивания в таких случаях ограничивается областью преобразования, как правило, совпадающего с преобразованием, выполненным при получении контейнера, и сводится к прямой модификации уже имеющихся коэффициентов. При таком подходе к сокрытию информации для её обнаружения достаточно применения традиционных методов стегоанализа. В случае необходимости передачи малых объёмов информации с высокой скрытностью и отсутствии ограничений на вычислительную сложность алгоритмов, актуальными становятся методы стеганографии, основанные на внесении изменений в сигнал на макроуровне, что позволяет производить встраивание сообщений в перцептивно значимые области, которые не подвергаются существенным искажениям во время обработки алгоритмами компрессии.

Алгоритмах сокрытия информации.

Наиболее перспективным на настоящий момент является выбор, в качестве отображающего преобразования, многоуровневого вейвлета-декомпозиции [2]. На настоящий момент вейвлеты широко используются для анализа особенностей, сжатия и реконструкции сложных сигналов, что объясняется простотой реализации задач компрессии мультимедиа-данных, возможностью адаптации используемых вейвлетов к кодируемому сигналу и введения зависимости формы вейвлетов от внешних параметров. Рассмотрим данный подход при встраивании скрытой информации в изображения.

На рисунке 1 приведена последовательность обобщённых преобразований выполняемых в алгоритмах сокрытия информации в изображении в области ортогональных преобразований.



Предлагаемый метод встраивания позволяет производить сокрытие информации в полноцветных изображениях и изображениях в градациях серого.

Цветоразностные компоненты до этапа восстановления изображения не используются. После преобразования цветового пространства и выделения яркостной компоненты она отображается в пространство преобразования при помощи многоуровневой вейвлет-декомпозиции.

Заключение

Несмотря на то, что математический аппарат вейвлет-анализа хорошо разработан и теория, в общем, оформилась, вейвлеты оставляют обширное поле для исследований. Достаточно сказать, что выбор вейвлета, наиболее подходящего для анализа конкретных данных, представляет собой скорее искусство, чем рутинную процедуру. Кроме того, огромное значение имеет задача разработки приложений, использующих вейвлет-анализ — как в перечисленных областях, так и во многих других, перечислить которые просто не представляется возможным.

Литература

1. J. Fridrich and M. Goljan, "Practical Steganalysis of Digital Images -- State of the Art", Security and Watermarking of Multimedia Contents, 2015, vol. SPIE-4675, pp. 1-13
2. Дьяконов В.П. Вейвлеты – от теории к практике. М. СОЛОН-ПРЕСС, 2014.
3. Maity, S.P. Kundu, M.K. Mandal, M.K. Capacity improvement in spread spectrum watermarking using biorthogonal wavelet, 48th Midwest Symposium on Circuits and Systems, 2015. Vol. 2, p.1426-1429

Steganography Based on Orthogonal Wavelet

Medvedev NV¹⁷⁶, Glinskaya EV.¹⁷⁷

Annotation. Currently, in the world to offer a huge number of algorithms for embedding imperceptible information into multimedia signals using wavelet transform. This article describes the image protection method based on orthogonal wavelet transforms. Protection is carried out by adapting the use of wavelets to the encoded signal, and the introduction of forms of wavelets depending on external parameters.

Keywords: information security, steganography, hide data, wavelet, wavelet transform

УДК 004.046

Определение оптимального базиса для представления сигнала со сложным спектральным составом в реальном масштабе времени

Медведев Н.В., Карташова Ж.К.¹⁷⁸

Предлагаемый в данной публикации способ позволяет определять частотно-временное разрешение в зависимости от свойств анализируемого сигнала, что необходимо для адекватного анализа процессов утечки информации в технических каналах.

Ключевые слова: вейвлет, сигнал, базис, утечка информации

Основными факторами, определяющими точностные характеристики вейвлет-преобразования являются:

- материнский вейвлет;
- размер анализируемого блока;
- максимальная глубина дерева разложения;
- структура дерева разложения, которая фактически определяет структуру покрытия частотно-временной плоскости

Влияние свойств материнского вейвлета на точностные характеристики результирующего определяет то, что число нулевых моментов и гладкость вейвлета оказывают основное влияние на способность вейвлета к представлению определенных классов сигналов, а размер носителя является характеристикой, напрямую влияющей на число операций, которые необходимо выполнить для разложения сигнала по базису.

Для построения оптимального базиса необходимо на основе исходных данных о свойствах анализируемых классов сигналов и имеющихся вычислительных ресурсов выбрать материнский вейвлет, максимальную глубину дерева разложения и размер анализируемого блока.

В качестве базового алгоритма выбора оптимального базиса может быть использован алгоритм который должен включать следующие шаги:

- Определение имеющихся вычислительных ресурсов.
- Определение того, какие из свойств сигнала являются существенными.
- Определение желаемых точностных характеристик существенных амплитудно- и частотно-временных параметров информационного сигнала.

¹⁷⁶ Nikolai Medvedev — Cand. Sci. (Eng.), Assoc.Professor of the Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation), medvedevnick54@yandex.ru.

¹⁷⁷ Elena Glinskaya, Bauman Moscow State Technical University, Moscow, glinskaya-iu8@rambler.ru

¹⁷⁸ МГТУ им.Н.Э.Баумана, iu8-Bauman Moscow State Technical University@yandex.ru

- Определение минимального размера анализируемого блока, позволяющего получить необходимые точностные характеристики.
- Определение максимального блока, на основе частоты дискретизации сигнала и, при этом, может быть проанализирован в реальном времени. Анализ блока максимально-допустимого размера позволит избежать дополнительных искажений, которые возникают из-за конечной природы анализируемых сигналов.
- Определение доступного времени на вычисления на основе размера анализируемого блока.
- Выбор материнского вейвлета на основе требуемых свойств преобразования осуществить.
- Определение необходимой глубины дерева разложения для обеспечения желаемых точностных характеристик.
- Определение контекста, в котором выделяемые свойства сигнала являются существенными.
- Определение минимального базиса, который позволяет выполнить уточнение контекста.
- Осуществление частичного разложения сигнала по базису.
- Получение необходимой информации о контексте и существенных признаках на основе частичного разложения сигнала по базису,.
- Анализ полученной информации и принятие решения о дальнейшем разложении сигнала по базису, или о наличии достаточной информации о сигнале для его дальнейшей обработки.
- Построение адаптивного базиса для каждого контекста.

Следует заметить, что часть операций, в том числе и расчет адаптивных оптимальных базисов для каждого контекста могут быть выполнены предварительно и не требуют реализации в реальном масштабе времени. Это позволяет заключить, что вычислительные затраты на выбор оптимального базиса в реальном масштабе времени будут пропорциональны количеству контекстов, число которых гораздо меньше чем число допустимых деревьев вейвлет-пакетов.

Общие суммарные вычислительные затраты на разложение сигнала длины N по оптимальному базису будут состоять из затрат на выбор оптимального базиса, которые составляют $O(K)$, где $K \ll N$ – среднее число вершин в получаемых оптимальных деревьях, числа операций необходимых для вычисления функции стоимости, которые имеют порядок $O(M)$, где $M \ll N$, затрат на разложение сигнала по оптимальному базису, которые, ограничены снизу и сверху соответственно $O(N)$ и $N \log_2 N$. Учитывая что, число узлов оптимального дерева гораздо меньше количества узлов полного дерева, затраты на разложение сигнала по оптимальному базису в большинстве случаев будут соответствовать $O(N)$.

На основе информации приведенной выше, можно сделать вывод о том, что разработанный метод определения оптимального базиса для представления сигнала со сложным спектральным составом может быть реализован в реальном масштабе времени.

Литература

1. Добеши И. Десять лекций по вейвлетам: Пер с англ. – М.: РХД, 2004. – 464 с.
2. Cohen and J. P. Conze. Regularite des bases d'ondelettes et mesures ergodiques. Technical report, CEREMADE, Universite Paris Dauphine, 1991.
3. Daubechies and J. Lagarias. Two-scale difference equations: II. Local regularity, infinite products of matrices and fractals. SIAM J. of Math. Anal., 24, 1992.
4. P. Abry. Ondelettes et turbulence. Multirésolutions, algorithmes de décomposition, invariance d'échelles, Diderot Editeur, Paris 1997.
5. N. Delprat, B. Escudie, P. Guillemain, R. Kronland-Martinet, P. Tchamitchian, and B. Torresani. Asymptotic wavelet and Gabor analysis: extraction of instantaneous frequencies. IEEE Trans. Info. Theory, 38(2):644-664, March 1992.

Determination of Optimum Basis for Representation of the Signal with a Complex Spectral Composition Real Time

Medvedev NV, Kartashov JK¹⁷⁹

The proposed method in this paper allows to determine the time-frequency resolution depending on the analyzed signal characteristics, it is necessary for an adequate analysis of information leakage processes in technical channels.

Keywords: wavelet, the signal basis, information leaks

УДК 004.056

Критический обзор методических документов в сфере защиты персональных данных

Мусихина Д. А.¹⁸⁰

В статье представлен обзор проекта Методики определения угроз безопасности информации в информационных системах, а также проведен сравнительный анализ действующей методики с предварительной версией: выделены положительные нововведения, отмечен спорный метод определения показателя уровня защищенности информационной системы персональных данных, влияющий на выявление актуальных для нее угроз.

Ключевые слова: информационная безопасность, персональные данные, модель нарушителя

Введение

В прошлом году ФСТЭК России опубликовала проект документа – «Методика определения угроз безопасности информации в информационных системах», который должен был заменить «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14 февраля 2008 года. В итоге обновленная Методика так и не вступила в силу, а регулятор в следующем году обещает представить еще один проект. Тем не менее, нам, как компании, осуществляющей услуги по разработке систем защиты персональных данных, хотелось бы придерживаться во всех проектах унифицированного алгоритма определения актуальных угроз безопасности персональных данных, соответствующего развитости информационных технологий сегодняшнего дня [1-9]. В данной статье рассмотрены наглядные графические модели алгоритмов определения актуальных угроз безопасности персональных данных обеих Методик, отмечены их недостатки, а также представлены собственные видения Компании по актуализации данных алгоритмов.

¹⁷⁹ Bauman Moscow State Technical University, Moscow

¹⁸⁰ Мусихина Дарья Андреевна, ЗАО «НПО «Эшелон», г. Москва, d.musikhina@npo-echelon.ru

Общая структура методического документа

Процесс определения угроз безопасности информации проекта Методики, в отличие от действующего руководящего документа, делится на четыре этапа (см. Рис. 1) [5]:

1. Определение области применения процесса определения угроз безопасности информации;
2. Идентификация источников угроз и угроз безопасности информации;
3. Определение актуальных угроз безопасности информации;
4. Мониторинг и переоценка угроз безопасности информации.

Добавлены первый и четвертый этапы, регламентирующие действия, которые необходимо проводить до и после самого процесса определения актуальных угроз безопасности информации, таким образом ФСТЭК России устанавливает для него непрерывный жизненный цикл.

В процесс определения области применения входит выявление физических и логических границ ИС, в которых принимаются и контролируются меры защиты информации ответственным оператором, а также определяются объекты защиты и сегменты информационной системы.

Мониторинг и переоценка угроз безопасности информации представляют собой пересмотр логических и физических границ ИС, ее базовых конфигураций и структурно-функциональных характеристик, которые могли быть изменены в результате переопределения целей и задач ИС, и повторную оценку актуальных угроз безопасности информации с последующим анализом этих изменений. Пересмотр модели угроз рекомендовано проводить не реже одного раза в год.

К проекту Методики добавлены три приложения:

1. Приложение № 1 «Рекомендации по формированию экспертной группы и проведению экспертной оценки при определении угроз безопасности информации»;
2. Приложение № 2 «Структура модели угроз безопасности информации»;
3. Приложение № 3 «Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации в информационной системе».

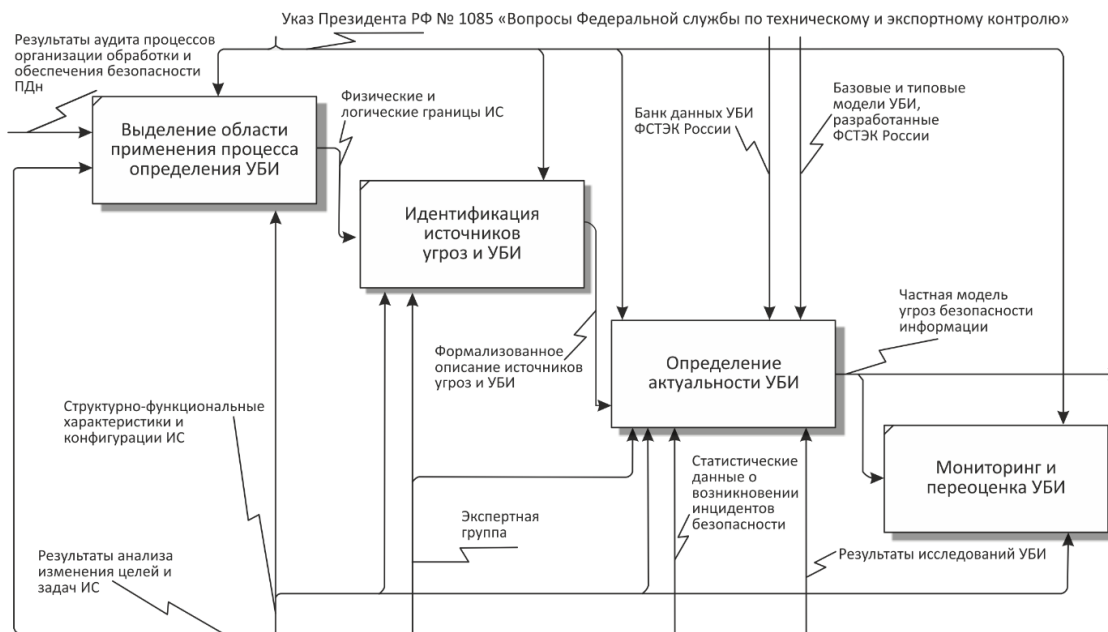


Рис. 1. Процесс определения УБИ согласно проекту Методики

Стоит отметить, что темы приложений, не раскрытые в действующем методическом документе, являются актуальными и вносят конкретику, например, в части формирования структуры документа «Частная модель угроз безопасности информации», получаемого на выходе процесса определения угроз безопасности информации в ИС.

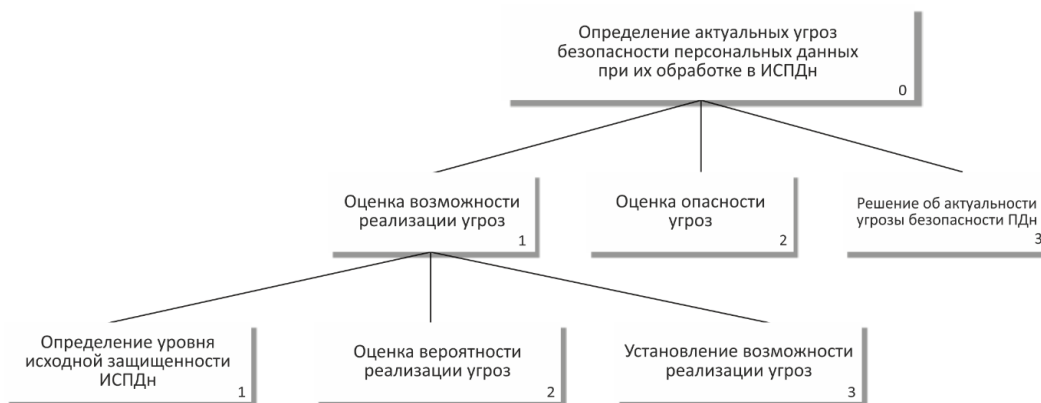


Рис. 2 Этапы процесса определения УБИ согласно действующей Методике

На рисунках 2 и 3 показаны этапы процессов, построенные в виде дерева узлов, для каждой из методик. Сравнив данные модели можно сделать вывод, что в проект Методики добавлены этапы подготовительно-организационного характера, такие как: исследование и выделение области, в которой будут идентифицироваться угрозы, проведение самой идентификации угроз и составление модели нарушителя. Далее добавлен процесс переоценки и пересмотра модели угроз, период которого определен в самой Методике – не реже раза в год, и сокращен по сравнению с тем, что указан в Федеральном законе № 152-ФЗ «О персональных данных» – не реже 3 лет.

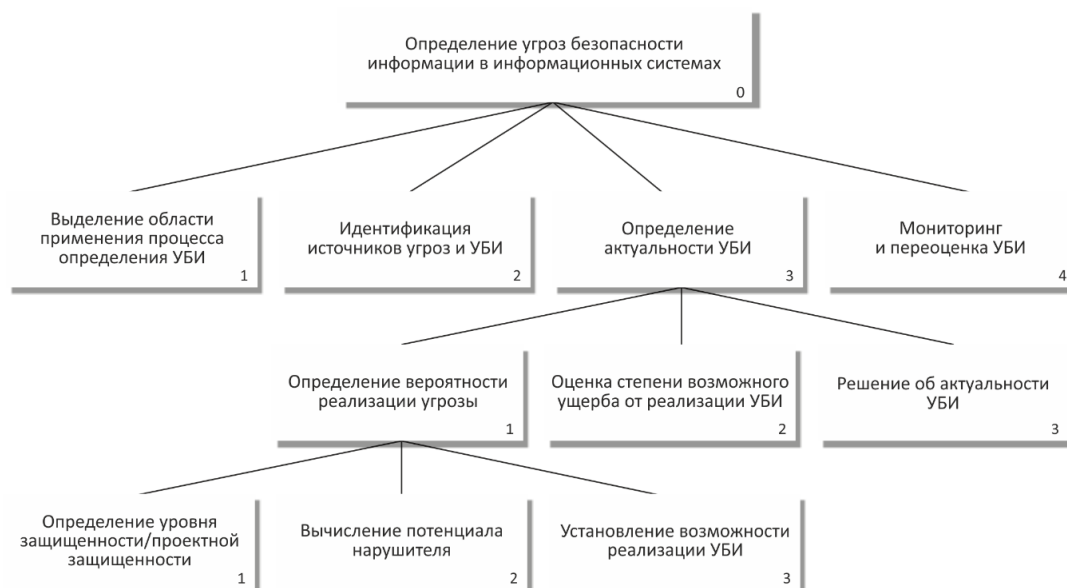


Рис. 3 Этапы процесса определения УБИ согласно проекту Методики

Выводы

В данной работе был проведен сравнительный анализ документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и его проекта, готовящегося на замену и представленного на рассмотрение и внесение предложений.

В результате были выделены следующие положительные нововведения:

- определена структуры документа «Модель угроз безопасности информации» и приведены рекомендаций к ее содержанию;
- внесены дополнительные итерации в процесс идентификации угроз, такие как очерчивание области применения процесса определения угроз безопасности информации, а также их мониторинг и переоценка,

- подробно описана модели нарушителя, что необходимо для создания полной картины об источниках угроз, возможных действиях нарушителя, способах и методах реализации угроз, а также последствиях от их реализации;

- установлена взаимосвязь с банком банных угроз ФСТЭК России.

Однако есть весомый недостаток в самом процессе определения угроз безопасности информации – для современных информационных систем показатель уровня проектной защищенности в любом случае получается «высокий», что приводит к актуальности большей части угроз безопасности информации, присущих ИС, и сказывается на построении систем защиты. Такая ситуация затрудняет использование методического документа на практике, в случае его утверждения в данной редакции [5]. Поэтому ФСТЭК России, учитывая все замечания к проекту Методики, обещала пересмотреть данную версию и выпустить в начале 2017 года переработанный документ.

Литература

1. Булдакова Т.И., Кривошеева Д.А. Угрозы безопасности в системах дистанционного мониторинга // Вопросы кибербезопасности. 2015. № 5 (13). С. 45-50.
2. Кубарев А.В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков // Вопросы кибербезопасности. 2013. № 2. С. 29-33.
3. Макеев С.А. Проблемы нейтрализации негативных информационных воздействий на бизнес-процесс кредитной организации // Вопросы кибербезопасности. 2015. № 5 (13). С. 51-54.
4. Марков А.С., Никулин М.Ю., Цирлов В.Л. Сертификация средств защиты персональных данных: революция или эволюция // Защита информации. Инсайд. 2008. № 5 (23). С. 20-25.
5. Мусихина Д.А. Методические документы по защите персональных данных по новейшим требованиям // Правовая информатика. 2016. № 2. С. 12-18.
6. Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции // Вопросы кибербезопасности. 2016. № 1 (14). С. 17-23.
7. Петренко С.А., Фабричных Л.С., Обухов А.В. Методы организации защиты персональных данных в информационных системах // Защита информации. Инсайд. 2009. № 4 (28). С. 64-70.
8. Плигин В.Н., Макаренко Г.И. Страна нуждается в обновлении общественных договоров в современном российском обществе // Мониторинг правоприменения. 2015. № 1 (14). С. 4-11.
9. Doroveev 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. V. 674. P. 441-449.

Научный руководитель: Марков Алексей Сергеевич, доктор технических наук, профессор кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, a.markov@bmstu.ru

Critical Review of the Methodical Documents in the Field of Protection of Personal Data

Musikhina Daria¹⁸¹

In the present time, there is no universal algorithm for detecting actual threats of personal data security, processed in information systems. FSTEC of Russia, controlling the field of personal data security, is reviewing the existing methodology. Last year in May an updated version of this document was introduced by the regulator. The article presents an overview of the project of the Methodology for determining the information security threats in information systems. A comparative analysis between the current methodology and the previous version has been carried out: positive innovations have been highlighted and a controversial method for detecting the indicator of the level of personal data security in information systems has been pointed out, influencing the actuality of corresponding threats.

Keywords: IT security, personal data, personal data systems, FSTEC of Russia, information security threats, violator model.

¹⁸¹ Musikhina Daria, NPO Echelon, Moscow, d.musikhina@npo-echelon.ru

Приведение общей классификации факторов аутентификации**Песков А.В.¹⁸²**

В статье рассмотрены существующие методы аутентификаций и классификации факторов. Проведен анализ существующих факторов. Разработана и приведена наиболее полная классификация факторов.

Ключевые слова: информационная безопасность, аутентификация, факторы аутентификации, многофакторная аутентификация, классификация факторов аутентификации.

Введение

Первой и важнейшей ступенью защиты любого ресурса является авторизация пользователя – этап определения личности пользователя (аутентификации) и распределения ему прав доступа. Существующие методы аутентификации большинства ресурсов не отвечают требованиям пользователей: либо они слишком сложны, либо не обеспечивают должной защиты, и пользователи идут на определенный риск, пользуясь услугами ресурса. При этом разработка новых механизмов аутентификации сталкивается с целым рядом проблем, важнейшей из которых является отсутствие полной и актуальной нормативной базы в отношении методов и факторов аутентификации. Приведение классификации факторов аутентификации в дальнейшем позволит облегчить создание многофакторных методов аутентификации на этапе выбора сочетания факторов, используемых в ней.

Механизмы аутентификации

До сих пор не существует общепринятой классификации методов аутентификации пользователей, однако, из существующих можно выделить определенные законы классификации [1-3]. Каждый механизм аутентификации обладает тремя основными характеристиками:

- Степень автоматизации
- Приоритет использования
- Используемый фактор аутентификации

Степень автоматизации механизма может быть полной и частичной. Речь идет об автоматизации со стороны системы, а не пользователя. Например, система аутентификации электронной почты mail.ru по данной классификации полностью автоматизирована, а аутентификация с помощью домофона – частично. Для аутентификации гостя по домофону требуется вмешательство владельца системы.

Приоритет использования – порядок использования механизма пользователем в сравнении с другими методами, присутствующими в системе.

Основной метод аутентификации – приоритетно используемый пользователем метод для штатного входа в систему. Самый распространенный – вход по паролю. Он используется в наибольшем количестве существующих на сегодняшний день ресурсов. Менее распространенным методом, в качестве основного, являются аппаратные идентификаторы, на которые записываются ключи доступа или пользовательские пароли.

Резервный метод аутентификации. В случае утери пароля или аппаратного токена, либо взлома учетной записи, в силу вступают резервные методы аутентификации. Под резервными методами чаще всего понимаются механизмы сброса пароля и восстановления доступа к своей учетной записи. Самыми распространенными являются два метода: ответ на секретный вопрос и отправка пароля на доверенный почтовый ящик, который пользователь указал при регистрации.

¹⁸² Песков Алексей Всеволодович, МГТУ им. Н.Э. Баумана г. Москва, arnumen@gmail.com

С другой стороны, метод отправки пароля на почтовый ящик является неким «перекладыванием на чужие плечи». Аутентификация пользователя через почтовый ящик передаёт ответственность за успешную и верную аутентификацию провайдеру почтового ресурса. В таком же русле действует отправка паролей через смс-сообщения. Проблемой резервных методов является их крайняя незащищенность. Заполучив доступ к почте, злоумышленник получает доступ сразу к целому ряду ресурсов, к которым привязана эта почта.

«*Last-resort*» аутентификация – аутентификация последней инстанции, механизма, к которому прибегают в самом крайнем случае. На данный момент к этим методам относится обращение к администрации информационной системы или в специальные отделы поддержки клиентов. Такие процедуры непомерно дороги, ведь количество клиентов у, например, крупнейших почтовых провайдеров превышает миллиард активных пользователей в год [4].

Классификация факторов аутентификации

Информация, предоставляемая пользователем, сравниваемая с эталоном на ресурсе. Существующие нормативные документы не в полной мере охватывают существующие факторы аутентификации или вообще обходят этот момент стороной [5]. Однако, во многих источниках классификации приводятся как часть проработки методов аутентификации. Они либо не полные, либо не актуальны на сегодняшний день. По итогам анализа существующих факторов и их классификаций приведена наиболее полная версия. Любой фактор можно отнести к одному из четырех основных классов, либо к их комбинации. Фактор знания - Первый и самый распространенный на данный момент фактор аутентификации. Ввод чего-либо, известного лишь пользователю – пароля или ответа на секретный вопрос. Теоретически он является самым простым и безопасным проверки подлинности субъекта, так как он обладает достаточной криптостойкостью, его просто и дешево реализовать на ресурсе, а все что нужно от пользователя - запомнить комбинация из букв, цифр или знаков. Однако, пользователь как правило задает слишком слабый пароль, что связано с физиологией самого человека, точнее его мозга. Мышление человека тесно связано с образами, и каждый из них имеет свое название. Поэтому в качестве пароля пользователь выберет название одного из образов и большинство заданных паролей можно найти в обычном словаре. Это ставит под угрозу учётную запись перед простым перебором пароля по заготовленным словарям. В случае с секретным вопросом криптостойкость еще меньше, чем у выбираемых ими паролей. В 2009 году на конференции IEEE Security and Privacy был опубликован доклад о исследовании, в котором приняло участие 130 человек [6]. Результаты показали, что чуть менее трети испытуемых – 28 процентов – смогли «угадать» ответ на секретный пароль, в случае, если близко знали своего оппонента. Если же оппонент был полностью незнаком, то ответ на вопрос угадали 17 процентов испытуемых.

Вещественный фактор - второй по популярности фактор аутентификации пользователей. Прежде всего под этим понимаются аппаратно-программные средства идентификации и аутентификации (СИА) или устройства ввода идентификационных признаков [10]. Элементами СИА являются аппаратные идентификаторы, устройства ввода-вывода (считыватели, контактные разъемы, адаптерные устройства и т.д.) и ПО к ним. Идентификаторы рассчитаны на хранение уникальных идентификационных признаков субъекта аутентификации в виде цифрового кода. Помимо этого, они могут обрабатывать конфиденциальные данные и осуществлять обмен данными с защищаемой системой. Существует разделение СИА по способу обмена данными с устройством ввода-вывода. Контактное считывание подразумевает непосредственное соприкосновение

идентификатора с устройством ввода-вывода. Бесконтактный (дистанционный) способ обмена не требует четкого позиционирования идентификатора и устройства ввода-вывода. Чтение или запись данных происходит при поднесении идентификатора на определенное расстояние к устройству ввода-вывода. Ключевой элемент системы СИА, сам идентификатор, является ее самым слабым звеном. Надежность идентификаторов прежде всего оценивают по их степени защищенности от механического воздействия, температурных воздействий, внешних электромагнитных полей, агрессивных сред, влаги, пыли и др. Кроме того учитывают фактор защищенности от внешних атак, направленных на цифровые данные, хранящиеся внутри чипа.

Биологический фактор - биометрические данные. Для их снятия чаще всего требуются специальные программно-аппаратные средства: биометрические сканеры. Большая часть биометрических сканеров классифицируется по характеру считываемых данных. Биометрические сканеры, основанные на статических методах: распознавание по отпечаткам пальцев, распознавание по геометрии руки, распознавание по радужной оболочке глаза. Биометрические сканеры, основанные на динамических методах: распознавание по рукописному почерку, распознавание по клавиатурному почерку, распознавание по голосу.

Географический фактор - такую систему можно назвать основанной на материальном факторе. За одним исключением. Геопозицию невозможно «потерять» в привычном смысле этого слова. Ее можно подделать, можно повредить оборудование для передачи геолокационных данных, но от действий пользователя напрямую не зависит успешность подтверждения этого фактора. Простейшим примером являются GPS данные. Совокупность координат, передаваемых спутнику, а точнее трем спутникам является достаточно стойким в плане подделки набором данных. Однако надежность передачи и вероятность успешного прохождения аутентификации пользователя могут не соответствовать требованиям многих систем в виду нестабильности спутникового канала передачи данных. Поэтому вторым примером фактора этого класса может служить сетевой адрес АС пользователя. Каждый персональный компьютер в сети обладает собственным (пусть не всегда уникальным) адресом. Множество домашних беспроводных сетей используют так называемые white и black листы MAC-адресов. Фильтрацию MAC применять как фактор аутентификации не столь сподручно в виду особенностей пакетной передачи данных, но IP-адрес компьютера как раз определяет «виртуальную» точку входа в сеть.

Общий перечень достоинств и недостатков, перечисленных выше факторов приведен в Таблице 2.

Таблица 2

Достоинства и недостатки классов факторов

Класс	Примеры	Достоинства	Недостатки
Фактор знания	Пароли, секретные вопросы, PIN	Распространенность, дешевизна, привычность	Сложно сохранить в тайне, легко забыть, образность мышления человека
Фактор наличия	Токены, файл ключей, приложения-аутентификаторы, электронные подписи	Сложно взломать, удаленная блокировка	Ненадежность технологии, дополнительное оборудование, многоступенчатость
Биометрический фактор	Отпечатки пальцев, радужная оболочка глаза, голос, подпись	Не потерять, простота для пользователя	Стоимость, чувствительность оборудования
Географический фактор	GPS координаты, IP, адрес хостинга	Доступность оборудования	Привязка к местности или конкретной системе

Выводы

Помимо существующих «общепринятых» групп факторов аутентификации, в процессе анализа выделена четвертая группа: географический фактор. Она охватывает те спорные факторы, которые не могли быть однозначно определены в тот или иной класс. Таким образом, приведенная классификация является наиболее полной и охватывает все существующие примеры факторов аутентификации, а также потенциальные разработки.

Литература

1. NCSC-TG-017 "Rainbow series books"
2. ГОСТ Р 51241-98 «Информационная безопасность»
3. ГОСТ Р ИСО/МЭК 9594-8-98 «Информационная технология. Взаимосвязь открытых систем»
4. It's not what you know, but who you know: A social approach to last-resort authentication. // S. Schechter, S. Egelman, and R. W. Reeder. // In CHI '09: Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems. Boston, MA. 2009.
5. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»
6. It's no secret: Measuring the security and reliability of authentication via 'secret' questions. // S. Schechter, A. J. B. Brush, and S. Egelman. // In IEEE Security and Privacy. IEEE. 2009.

Научный руководитель: Гудков Олег Владимирович, ст. преподаватель кафедры ИУ8 «Информационная безопасность» МГТУ им. Н.Э. Баумана, od@snpro.ru

Elaboration of Authentication Factor Classification

Peskov A.V.¹⁸³

This article presents most actual classification for authentication factors. An overview of authentication methods is given in detail. Factor classes highs and lows also presented.

Keywords: information security, authentication, classification, authentication factors, authorization process, passwords.

¹⁸³ Peskov Alexey Vsevolodovich, Bauman Moscow State Technical University, Moscow, apnumen@gmail.com

Базовая системы ввода-вывода как объект реализации угроз безопасности информации

Надеина И.С.¹⁸⁴

В статье рассмотрены вопросы актуальности реализации угроз безопасности информации с учетом структурно-функциональных характеристик базовых систем ввода/вывода (БСВВ) и реализация мер защиты, направленных на нейтрализацию данных угроз. На основе анализа угроз безопасности информации сформированы подходы по организации защиты БСВВ.

Ключевые слова: базовая система ввода/вывода, угроза безопасности информации, уязвимость, меры защиты информации.

Базовая система ввода/вывода (БСВВ) является одним из важнейших объектов защиты информации. Угрозы на БСВВ, а точнее на ее составляющую - стадию первоначальной загрузки операционной системы – могут нанести серьезный ущерб информационной системе. Проблеме защиты средств вычислительной техники от реализации угроз безопасности информации, связанных с особенностями функционирования БСВВ и наличием уязвимостей в них, уделяется пристальное внимание [1-3, 9, 10].

В настоящее время активно ведутся работы по разработке методов и средств защиты БСВВ. На их основе разрабатываются стандарты, содержащие требования по обеспечению безопасного функционирования БСВВ, а также некоторые нормативные документы, определяющие организационные и технические меры обеспечения безопасности БСВВ [4, 5].

При этом в данных документах не представлено четкого определения БСВВ, о структуре модулей и принципах ее функционирования, что не позволяет в полной мере оценить возможности злоумышленника, а также последствия от реализации угроз безопасности информации.

В связи с чем, возникает необходимость провести оценку БСВВ с точки зрения объекта реализации угроз безопасности информации.

БСВВ представляет собой совокупность программ, основными функциями которых являются определение компонентов средства вычислительной техники и загрузка операционной системы. На современных компьютерах ее главная роль заключается в инициализации устройств, тестировании аппаратных компонентов и обеспечение загрузки операционной системы. Кроме того, БСВВ предоставляет пользователю интерфейс для настройки параметров программных и электронных компонентов средства вычислительной техники.

На замену устаревшей вариации BIOS разработан UEFI (Unified Extensible Firmware Interface). UEFI выполняет не только процесс загрузки операционной системы, а также обеспечивает новый способ разметки жесткого диска GPT (BIOS рассчитан для MBR); сервисы, которые функционируют время работы операционной (boot services и runtime services); модульную архитектуру, позволяющей создавать пользовательские приложения в UEFI [6].

Стандарт UEFI намного более документирован, чем спецификации BIOS, что создает дополнительные предпосылки для реализации угроз безопасности информации, эксплуатации уязвимостей, а также созданием разнообразных вредоносных программ.

Основными этапами выполнения BIOS/UEFI являются (рис. 1):

¹⁸⁴ Надеина Ирина Сергеевна, МГТУ им. Н.Э.Баумана, г. Москва, nadeina.irina2013@yandex.ru

- запуск загрузочного блока БСВВ (Boot block);
- первоначальная инициализация и тестирование компонентов, таких как системная плата, чипсет, память, центральный процессор (POST);
- загрузка и исполнение дополнительных программ из запоминающих устройств системной платы (Option ROMs);
- выбор устройства, содержащего основную загрузочную запись (MBR);
- передача управления первоначальному загрузчику ядра операционной системы (Boot loader);
- передача управления загрузчику ядра операционной системы;
- загрузка ядра операционной системы.

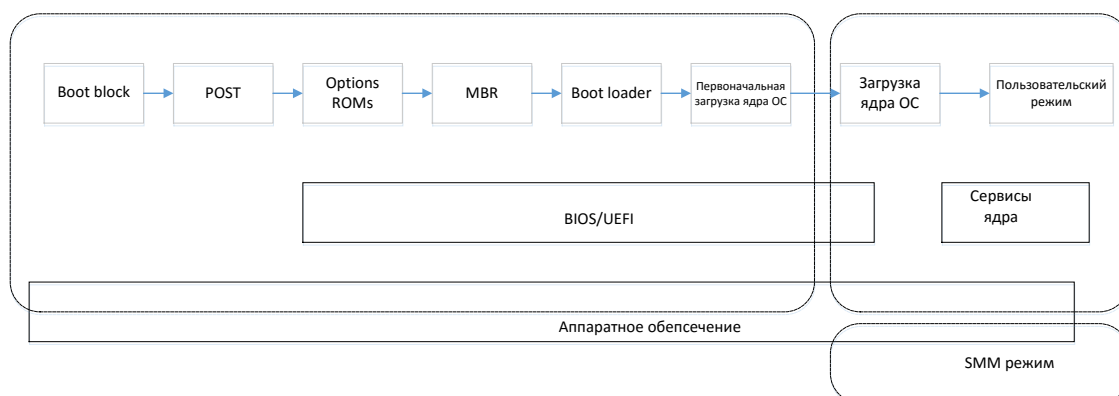


Рис.1. Процесс загрузки БСВВ

БСВВ разрабатываются как производителями компьютерного оборудования, так и независимыми разработчиками программного обеспечения. В процессе функционирования разработчиками осуществляются периодические обновления программного обеспечения БСВВ, предназначенные для устранения ошибок, уязвимостей, а также для обеспечения поддержки новых устройств. Возможность обновления программного обеспечения предусматривает возможность перепрограммирования БСВВ в постоянном запоминающем устройстве. Данная возможность позволяет реализовать такие угрозы безопасности информации, как несанкционированная модификация БСВВ, осуществляемая посредством получения доступа к функциям микросхемы, где хранится БСВВ; загрузка модифицированной прошивки БСВВ; несанкционированное изменение программного обеспечения БСВВ; внедрение вредоносного кода в БСВВ; восстановление уязвимой версии БСВВ [7].

Последствиями подобных действий может стать изменение режима настройки БСВВ, изменения режима функционирования средства вычислительной техники, внедрения вредоносных программ, а также приведения устройства в состояние неработоспособности.

После включения электропитания средства вычислительной техники управление передается Boot Block. Он производит первоначальную проверку оперативной памяти и энергонезависимой памяти.

После завершения работы Boot Block запускает программу самопроверки и тестирования при включении POST. Программа POST выполняет контроль целостности, инициализацию и тестирование центрального процессора, а также различных контроллеров, мостов между различными типами шин, а также осуществляет настройку прерываний. В UEFI данную фазу загрузки БСВВ принято называть Security Phase (SEC). Она является корневым элементом остального процесса загрузки. POST также предоставляет пользователю возможность вызова интерфейса, предназначенного для

настройки параметров системной платы и других устройств. После завершения выполнения POST осуществляется поиск и инициализация остальных периферийных устройств и микроконтроллеров. В UEFI данный этап обозначается как предварительная EFI инициализация (PEI).

На данном этапе возможна реализация угроз, связанных с несанкционированным изменением настроек БСВВ и конфигурации устройства; анализом криптографических алгоритмов и их реализации, а также подменой ключей, являющихся корневым элементом при проверке подлинности инициализируемых компонент устройства, угроза подмены аутентификационной информации, хранящейся в БСВВ.

После чего осуществляется поиск устройств, с которых осуществляется загрузка операционных систем. Для устройства, разрешенного для загрузки, осуществляется запуск на исполнение программного кода загрузочной записи MBR (GPT для UEFI), который запускает на исполнение загрузчик операционной системы (Boot Loader). PEI подготавливают средство вычислительной техники к загрузке операционной системы. На данном этапе нарушитель получает возможность загрузить собственную операционную систему, позволить получить контроль над устройством.

В процессе загрузки БСВВ также устанавливает обработчики прерываний управления системой, функционирующих в режиме системного управления (SMM). SMM обеспечивает запуск специализированной программы, хранящейся в защищенной области памяти, обслуживающей возникшие прерывания и имеющей доступ практически ко всем вычислительным ресурсам средств вычислительной техники. Так, злоумышленник через систему SMM получает доступ к привилегированному режиму процессора, из которого ему доступна на чтение и запись вся физическая память, а также большинство вычислительных ресурсов устройства. В данном случае возможно вывести из строя компоненты устройства [8].

Кроме того, во время работы информационной системы злоумышленник может воспользоваться уязвимостями, позволяющими программно модифицировать выполняемый блок БСВВ, находящийся в оперативной памяти. Подобные уязвимости позволяют злоумышленнику внедрить вредоносные программы без вмешательства в содержимое микросхемы БСВВ.

С учетом важности выполняемых БСВВ функций и его структурно-функциональных характеристик от реализации угроз безопасности информации на БСВВ в процессе его работы возможны следующие последствия:

- вывод из строя устройства;
- подмена (модификация) загрузчика операционной системы;
- доступ к файловой системе и параметрам настройки БСВВ, а также к вычислительным устройствам;
- перехват управления средством вычислительной техники до загрузки операционной системы.

Таким образом, несанкционированная модификация программного обеспечения БСВВ создает серьезную угрозу безопасности информации, обрабатываемой в информационной системе, так и средству вычислительной техники в целом. БСВВ как объект защиты информации представляет собой базовый компонент устройства, который также содержит в себе уязвимости, и подвержен угрозам безопасности информации.

Анализ угроз безопасности информации в БСВВ необходимо проводить с учетом производителя БСВВ, структуры БСВВ, а также особенностей функционирования конкретного средства вычислительной техники и потенциала возможного нарушителя.

При этом существует базовые рекомендации, позволяющие обеспечить безопасное функционирование БСВВ:

- обеспечение целостности прошивки БСВВ для предотвращения её несанкционированной модификации;
- проверка подлинности загрузчика операционной системы;
- обеспечение безопасности способа обновления БСВВ;
- разграничение доступа к интерфейсу конфигурации БСВВ;
- выявление и устранения уязвимостей программного обеспечения БСВВ.

С учетом постоянного развития информационных технологий и возрастающего вместе с ними разнообразия угроз безопасности информации, представленные меры защиты информации в БСВВ являются основой безопасного функционирования БСВВ и требуют дальнейшего совершенствования.

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. Иванников П. В., Алтухов Н. О. Современные типы атак на BIOS. Молодежный научно-технический вестник, № 06, июнь, 2015. URL: <http://sntbul.bmstu.ru>.
3. Марков А.С., Пугачев И.Б. Программный метод обеспечения безопасности загрузки операционной среды // Известия Института инженерной физики. 2009. Т. 1. № 11. С. 7-9.
4. D. Cooper, W. Polk, A. Regenscheid, and M. Souppaya, "BIOS Protection Guidelines (NIST 800-147)," National Institute of Standards and Technology, апрель 2011.
5. A. Regenscheid and K. Scarfone, "BIOS Integrity Measurement Guidelines (NIST 800-155)," National Institute of Standards and Technology, декабрь 2011.
6. Nystrom, "UEFI Networking and Pre-OS Security," in Intel Technology Journal – UEFI Today: Bootstrapping the Continuum, стр. 80-101, October 2011. URL: <http://noggin.intel.com>.
7. Richard Wilkins, Brian Richardson. UEFI secure boot in modern computer security solutions. September 2013, стр. 10. URL: www.uefi.org.
8. Sherri Sparks, Shawn Embleton. SMM Rootkits: A new Dreed of OS Independent Malware. URL: <http://www.eecs.ucf.edu>.
9. Вареница В.В., Вылегжанин В.В., Марков А.С., Никулин М.Ю., Фадин А.А., Цирлов В.Л. Устройство для доверительной загрузки. Патент на полезную модель RUS 101555, 25.10.2010; 2010143450/08, 20.01.2011, Бюл. № 2. 2 с. URL: <http://elibrary.ru/item.asp?id=18646386>.
10. Веряев А.С., Вылегжанин В.В., Марков А.С., Рязанцев А.А., Фадин А.А., Цирлов В.Л. Способ доверенной загрузки в виртуализированных средах. Патент на изобретение RUS 2581552 24.03.2016; 2014136615; 2016. URL: <http://elibrary.ru/item.asp?id=25916898>.

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

The basic input-output system as the object of information security threats

Nadeina I.¹⁸⁵

The article discusses the relevance of questions of realization of the threats with considering structural and functional characteristics of the basic input / output system (BIOS) and security measures to neutralize these threats. For this purpose the analysis of threats are formed approaches for BIOS protection.

Keywords: BIOS, threats, vulnerability, information security measures.

¹⁸⁵ Nadeina Irina, Bauman Moscow State Technical University, Moscow, nadeina.irina2013@yandex.ru

Информационная безопасность облачных технологий

Назарова Е.К.¹⁸⁶

Продвижение облачных сервисов на рынке связано с их реальными преимуществами, и с успехами рекламы, зачастую представляющей услуги удаленных серверов как принципиально новую технологию. Данная статья посвящена анализу существующих решений в области обеспечения информационной безопасности облачных технологий. Перечислены основные преимущества удаленного обслуживания. Проведен сравнительный анализ внедрения облачных технологий за рубежом и в России.

Ключевые слова: Защита, удалённое обслуживание, услуги.

Введение

Распространение облачных технологий носит массовый, «взрывной» характер. Продвижение облачных сервисов на рынке связано и с их реальными преимуществами, и с успехами рекламы, зачастую представляющей услуги удаленных серверов как принципиально новую технологию.

На самом деле «облачные» технологии появились вместе с интернетом и даже немного раньше, во времена больших ЭВМ, к интеллекту которых обращались десятки пользователей со своих рабочих мест. Программы, базы данных находились в памяти большой машины, а пользователи имели дисплей, клавиатуру и средства подключения к общей сети.

Сейчас в роли «большой ЭВМ» выступает группа серверов, взаимосвязанных, обменивающихся данными, перераспределяющих ресурсы. Эта удаленная группа серверов работает как единая система, и невозможно определить, какой именно реальный компьютер обработает поступивший по сети запрос. Физически серверные вычислительные мощности могут быть размещены в разных зданиях, удаленно друг от друга; при обработке информации сигналы «летают» по непредсказуемым траекториям между жесткими дисками; отсюда возникло поэтичное название «облака».

Основные услуги, предоставляемые владельцами «облачных технологий»

Главное преимущество удаленного обслуживания – доступность информации из разных точек, удаленных на большие расстояния. Возможность командной работы большого числа людей, находящихся далеко друг от друга. Это особенность Интернета как такового, но при увеличении скорости и доступности связи появилась возможность выносить в Сеть бухгалтерские программы, графические и дизайнерские программы, платформы для разработки программ, обширные базы данных.

Самая простая и распространенная услуга – SaaS, программное обеспечение как услуга. Программа предоставляется удаленным пользователям для работы, при этом обслуживание программы, ее регулярное обновление, резервное копирование пользовательских баз данных выполняет организация, предоставляющая услугу. Например, фирма 1С предоставляет услуги «облачным» клиентам; они не покупают программу, не покупают ежеквартальные обновления, не заботятся о мощных серверах, их обслуживании, постоянном копировании и сохранении данных, а платят за аренду программы, за то или иное количество рабочих мест. Это выгодное и рациональное решение.

¹⁸⁶ Назарова Елена Константиновна, МГТУ им.Н.Э.Баумана, Москва, alenan95@mail.ru

Цена многих программных пакетов очень высока, а степень их полезности не всегда однозначно просчитывается; в таком случае заплатить доступную цену за вход в «облачную версию» и поработать там – прекрасный вариант.

Технически сетевое использование бухгалтерской программы ничем не отличается от браузерной игры, отличие лишь в серьезном назначении программы и актуальности вопросов безопасности.

Технология PaaS – это «платформа как услуга». Пользователям предоставляется не программа, а средство для разработки программ и приложений.

IaaS – «инфраструктура как услуга». Пользователь получает не конкретные программные средства, а удаленные вычислительные мощности, виртуальную среду для размещения программ, средств разработки, хранилища данных. Выгода в этом случае заключается в том, что клиент избавлен от хлопот с «железом», ему не нужно заниматься сетевым администрированием, поддержанием должного микроклимата в серверной комнате.

Но сохраняет ли клиент, переносящий сервер в виртуальное пространство, полный контроль над информацией? Этот вопрос не имеет однозначного ответа на сегодняшний день, тем не менее, услуга востребована, и число пользователей стремительно растет.

Еще один облачный сервис называется «безопасность как услуга». Тот, кто предпочитает иметь собственный сервис, может получить облачного «ангела-хранителя», антивирусную программу для внешней защиты компьютера от вирусных атак. Дает ли этот способ стопроцентную гарантию защиты? Увы, не 100%, но все же активность троян-программ и пресекается весьма эффективно.

Итак, выгоды очевидны, риски присутствуют, технологии развиваются. Но не везде они развиваются одинаково энергично; специалисты считают, что Россия несколько отстает в освоении облаков.

Облачные технологии на западе и в России

Действительно, таких темпов ежегодного прироста пользователей «облачных» технологий, как на западе, в России не наблюдается. Рассмотрим объективные причины явления.

Успехи распространения товара напрямую связаны с рекламой. Энергичное продвижение облачных технологий в цивилизованном мире связаны как с реальными преимуществами, так и с талантом рекламодателей.

Большинство пользователей, перешедших на работу в облака, относятся к сфере малого и среднего бизнеса. Не потому, что большой бизнес игнорирует преимущества облачных технологий, а просто мелкого бизнеса там больше. Специфика России в том, что у нас пока малый и средний бизнес развиты недостаточно, многие малые фирмы скрываются в тени, а их владельцы предпочитают решать вопросы на уровне личных контактов.

Решая вопрос о подключении облачных технологий, люди нередко задаются вопросами: «если я перенесу информацию на удаленный сервер, останусь ли я единоличным владельцем информации? Утратив контроль над сохранностью данных, не лишусь ли их из-за чужой оплошности?». Рассмотрим возможные риски и способы защиты.

Актуальность вопросов безопасности

При передаче данных на удаленный сервер они, могут оказаться в большей безопасности, чем на личном компьютере. Это верно для тех пользователей, которые безопасности не уделяют должного внимания – по незнанию, легкомыслию, недостатку времени, низком приоритете вопросов безопасности и т.д.

Рассмотрим основные опасности для информации на личном компьютере.:

- Опасность физической утраты данных из-за аварии компьютера
- Повреждение информационных ресурсов вирусами
- Несанкционированный доступ к информации, разглашение секретных или конфиденциальных данных

Какие опасности подстерегают пользователей в «облаках»? Те же самые, что на личном компьютере, но их вероятность снижается.

Вывод

В результате были проанализированы существующие услуги, предоставляемые владельцами «облачных технологий». Главное преимущество удаленного обслуживания – это высокая доступность инфраструктуры из любых точек, удаленных на большие расстояния. Применение облачных технологий позволяет экономить на капитальных затратах.

Обеспечение целостности информации при переносе на сервер в виртуальное пространство остаётся одной из самых важных проблем информационной безопасности. На сегодняшний день, необходимо особое внимание уделять обеспечению целостности информации за пределами защищаемой территории.

Литература

1. Клементьев И.П., Устинов В.А. Введение в облачные вычисления//Интернет университет информационных технологий. URL: <http://www.intuit.ru/department/se/incloudc/> (дата обращения: 22.10.2016).
2. Коростелев В. К., Медведев Н. В. Обеспечение целостности информации в средах виртуализации данных // Математические методы и моделирование. Номер №11. М.:ФГБОУ ВПО МГТУ им. Н.Э. Баумана, 2016.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.:Логос, 2001. 256с.
4. Руководящий документ. Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. Режим доступа: <http://fstec.ru/component/attachments/download/294>

Научный руководитель: Медведев Николай Викторович, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, канд. техн. наук, доцент, medvedevnick54@yandex.ru

Information Security of Cloud Computing **Nazarova E.¹⁸⁷**

Advance of cloud services in the market is connected to their real advantages, and to progress of the advertizing often representing services of remote servers as essentially new technology. This article is devoted to the analysis of the existing decisions in the field of support of information security of cloud computing. Primary benefits of remote service are listed. The comparative analysis of implementation of cloud computing abroad and in Russia is carried out.

Keywords: Protection, remote service, services.

¹⁸⁷ Nazarova E.K., Bauman Moscow State Technical University, Moscow, alenan95@mail.ru

Способы статического и динамического анализа уязвимостей программного обеспечения

Полуэктов В.В.¹⁸⁸

В статье представлены результаты анализа существующих подходов защиты и идентификации дефектов (уязвимостей и ошибок) в исходном и бинарном кодах программ, проводимых на различных этапах их разработки, проектирования и эксплуатации. Обобщены наиболее распространенные дефекты кода и объекты воздействия, функциональные и эргономические требования, предъявляемые к современным системам анализа.

Ключевые слова: статический и динамический анализ, исходный и бинарный код, дефекты, требования, технологии защиты, объекты несанкционированных воздействий.

Высокая сложность современного программного обеспечения (ПО), обусловленная множеством факторов, является *фундаментальной проблемой*, вызванной текущим состоянием развития информационных технологий [1, 2].

Возможность изменения основных свойств защищенности информационных ресурсов и дестабилизации процессов функционирования информационно-вычислительных систем различного назначения посредством применения злоумышленниками несанкционированных воздействий деструктивного характера (атак) на уязвимости программно-аппаратных комплексов предопределяют острую потребность в своевременном обнаружении дефектов (уязвимостей и ошибок) на этапах жизненного цикла их разработки и проектирования, проверки соответствия их заявленной политики безопасности и реализации механизмов защиты [1, 3, 4].

Существующие подходы защиты и идентификации дефектов ПО

Технологии поиска дефектов (уязвимостей и ошибок) и защиты от них разрабатываются по трем основным направлениям. Во-первых, используются *системы автоматического поиска дефектов с помощью статического анализа исходного кода* программ, которые можно применять на самых ранних этапах разработки, что делает исправление дефектов максимально дешевым.

Во-вторых, применяются *системы динамического анализа бинарного кода* программ, позволяющие многократно запускать заданную программу на автоматически генерируемом наборе входных данных и отслеживать ситуации возникновения дефектов.

В-третьих, разрабатываются *технологии защиты программы и ее окружения* от эксплуатации имеющихся в ней уязвимостей во время работы программы (рис. 2).

Технологии поиска дефектов в исходном коде ПО

Поиск и устранение дефектов в ПО требует больших трудозатрат, при этом многие из них могут остаться незамеченными. Наибольшее распространение получили методы *статического анализа* исходного кода ПО, рассматривающие все возможные пути выполнения программы без ее фактического выполнения.

Существуют и другие классы систем обнаружения дефектов в исходном коде программ, однако точность и требуемые для использования ресурсы ограничивают их

¹⁸⁸ Полуэктов Вадим Валентинович, Военная академия войсковой противовоздушной обороны, Вооруженных Сил Российской Федерации, имени Маршала Советского Союза А.М.Василевского, г. Смоленск, poluektov.vadim@yandex.ru

область применения (рисунок 1). Данные системы не получили такого распространения, как упомянутые системы автоматического поиска дефектов на основе статического анализа.

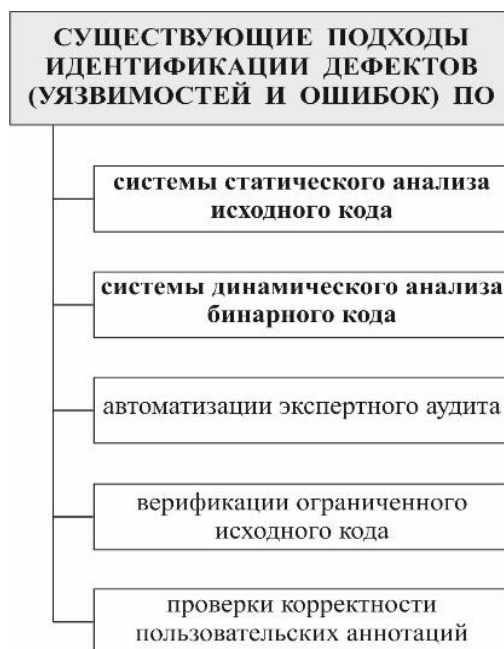


Рис. 1. Классы систем обнаружения дефектов в исходном коде программ

Технологии специализации систем автоматического поиска дефектов в исходном коде программ

Необходимо отметить, что эффективность систем автоматического поиска дефектов ПО зависит от того, на каком наборе тестовых программ нарабатывались эвристики этих систем. По умолчанию эвристики поиска ситуаций в исходном коде, ранжирования собранных данных по важности, параметры точности применяемых алгоритмов настроены на некоторое «среднее» значение поведения анализируемых программ. Так, если программист перед использованием некоторого указателя проверяет его значение на корректность во всех точках программы, кроме одной-двух, то велика вероятность, что и в этих точках программы значение указателя может быть некорректным, и требуется выдать предупреждение о возможном разыменовании нулевого указателя. Конечно, такая эвристика применяется лишь в том случае, если основные алгоритмы статического анализа не смогли с достаточной точностью установить значение указателя.

Следовательно, для специальных классов программ является возможной такая *доработка системы автоматического поиска*, что точность выполняемого системой анализа для этих классов программ повысится. При этом основные виды анализов, выполняемые системой, останутся неизменными.

Технологии динамического анализа бинарного кода ПО

Системы динамического анализа бинарного кода программ выполняют поиск дефектов (уязвимостей и некритических ошибок) путем генерации различных наборов данных и последующей передачей их на вход исследуемой программе. Основными задачами, которые решаются при динамическом анализе, являются: задача генерации наборов входных данных, покрывающих интересующие пути выполнения программы; запуск и трансляция программы; отслеживание возникающих уязвимостей [5].

Таким образом, системы динамического анализа представляют совокупность нескольких модулей-инструментов (зачастую, с открытым исходным кодом), решающих

основные сформулированные задачи анализа. Экспоненциальная сложность анализа и применения в случае нетривиальных алгоритмов обработки входных данных и/или модели исполнения (например, обратные вызовы процедур на мобильных платформах) преодолевается новыми эвристиками, позволяющими производить более глубокий анализ программы.

Объекты воздействия на систему при эксплуатации уязвимостей

Применение систем автоматического анализа дефектов (уязвимостей и не критических ошибок) в ПО на основе статического анализа не гарантирует полного их отсутствия. Поэтому требуются также технологии защиты программ и их окружения от эксплуатации имеющихся в программах уязвимостей (рисунок 2).

Как правило, большинство эксплуатируемых дефектов программ заключаются в неправильном использовании системных ресурсов напрямую или через интерфейсы ОС. Объектами воздействия при эксплуатации взлома, таким образом, являются разнообразные ресурсы ОС, при этом к взлому может приводить как ошибка в системных, так и в прикладных программах.

Соответственно, эффектом воздействия является либо гарантированный крах программы, либо несанкционированное изменение служебных данных системы, приводящее к эскалации прав атакующего, либо нарушение свойств защищенности информации, обрабатываемой программой.

Технологии защиты ПО от эксплуатации уязвимостей

Большинство технологий защиты ПО от эксплуатации уязвимостей направлены на защиту системных ресурсов, которые делают невозможным либо затрудненным их несанкционированное использование (рисунок 2).

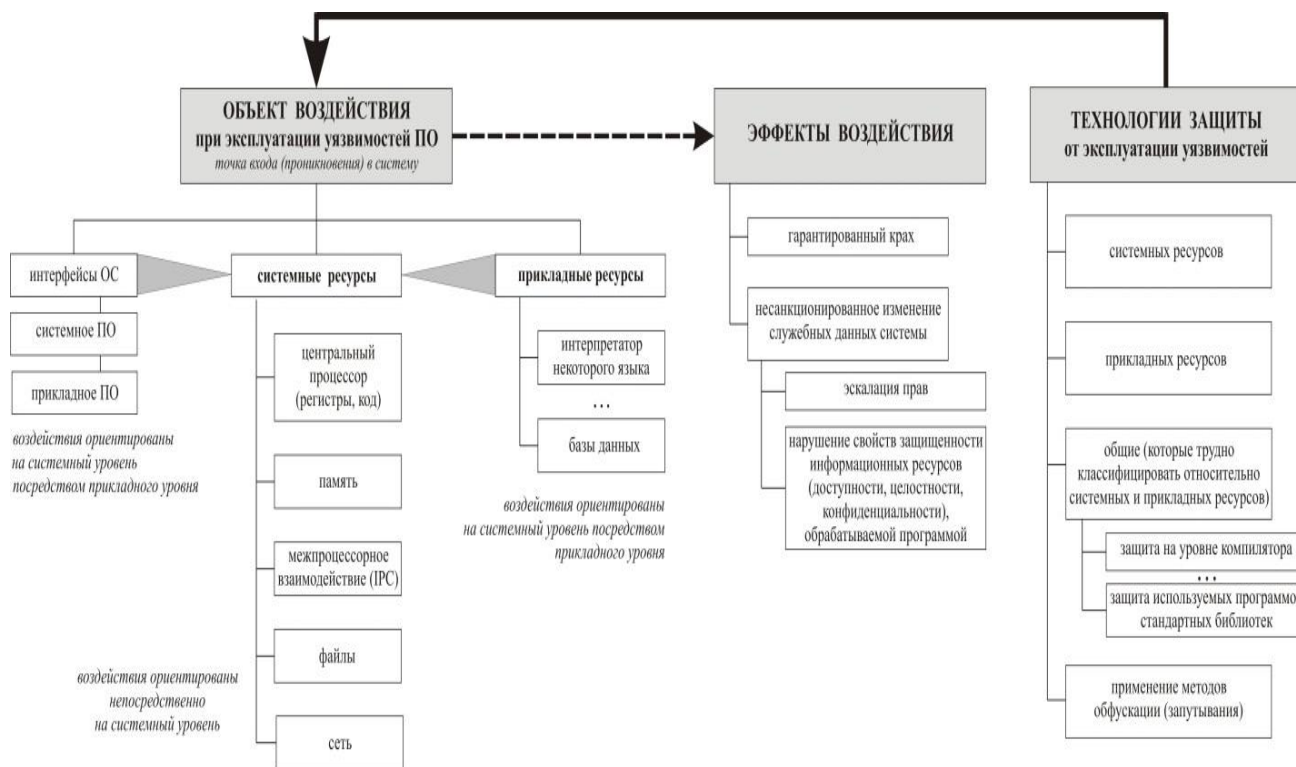


Рис. 2. Структурно-логическая схема «объект воздействия – эффекты воздействия – технологии защиты»

Таким образом, исходя из проведенного анализа существующих технологий минимизации дефектов программно-аппаратных комплексов, максимальный эффект достигается при комплексном использовании рассмотренных технологий анализа на этапах разработки, проектирования и эксплуатации.

Литература

1. Аветисян А. И. Современные методы статического и динамического анализа программ для решения приоритетных проблем программной инженерии: автореф. дис. ... д-ра физ.-мат. наук: 05.13.11/Аветисян Арутюн Ишханович. – М., 2011. – 36 с.
2. Марков А.С. Модели оценки и планирования испытаний программных средств по требованиям безопасности информации // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2011. № СПЕС. С. 90-103.
3. Чукляев И. И., Морозов А. В., Болотин И. Б. Теоретические основы построения адаптивных систем комплексной защиты информационных ресурсов распределенных информационно-вычислительных систем: монография / И. И. Чукляев, А. В. Морозов, И. Б. Болотин – Смоленск: ВА ВПВО ВС РФ, 2011. – 227 с.
4. Морозов А. В., Чукляев И. И. Информационная безопасность вычислительных систем боевого управления в аспекте информационного противоборства. Научно-практический журнал «Проблемы безопасности российского общества». М.: МГУПС. ISBN 2307-4396. Вып. № 2-3. 2013. С. 85-91.
5. С.П. Варганов, А.Ю. Герасимов. Динамический анализ программ с целью поиска ошибок и уязвимостей при помощи целенаправленной генерации входных данных. Труды ИСП РАН том 26 вып. 1, 2014. С. 375-394.

Научный руководитель: *Елисеев Андрей Николаевич, кандидат технических наук, заместитель начальника кафедры автоматизированных систем боевого управления, ВА ВПВО ВС РФ, г. Смоленск, badia67@mail.ru*

The Methods of Static and Dynamic Analyses Detecting Vulnerabilities of Software

Poluektov V.¹⁸⁹

Presented the results of analyses of the existing approaches securities and detecting defects (vulnerabilities and faults) in the source and binary code of software on the different stages of engineering and maintenance. The most common defects (vulnerabilities and faults) and objects of destructive programming attacks generalize, functional and ergonomic requirements of the modern program system of security and detecting vulnerabilities of software presented.

Keywords: *static and dynamic analyses, source and binary code, defects (vulnerabilities and faults), requirements, technologies of security, objects of destructive programming attacks.*

¹⁸⁹ Poluektov Vadim Valentinovich, Marshal of the Soviet Union A.M.Vasilevsky Army Air Defense Military Academy, Smolensk, poluektov.vadim@yandex.ru

Создание национальной системы раннего предупреждения о компьютерном нападении

Петренко С.А.¹⁹⁰

Исследована комплексная проблема раннего предупреждения о компьютерном нападении на ведомственные и корпоративные информационные ресурсы Российской Федерации. Предложен подход к созданию требуемых систем предупреждения на основе так называемого «вычислительного когнитивизма» – сравнительно нового научного направления исследований, в котором познание и когнитивные процессы являются разновидностью символического вычисления. Показано, что когнитивный подход позволяет создавать системы, принципиально отличающиеся от традиционных систем обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) уникальной способностью к самостоятельному ассоциированию и синтезу новых знаний о качественных характеристиках и количественных закономерностях информационного противоборства. Предложена возможная архитектура когнитивной системы раннего предупреждения о компьютерном нападении на информационные ресурсы Российской Федерации на основе конвергентных нано-, био-, инфо-, когнитивных технологий, NBIC-технологий.

Ключевые слова: когнитивная система, вычислительный когнитивизм, конвергентные NBIC-технологии, технологии Big Data, раннее предупреждение о компьютерном нападении.

Научный задел для решения задачи.

Предпосылками современного когнитивного подхода послужили фундаментальные результаты:

- математической логики (от Аристотеля до А.Н. Колмогорова);
- математической теории вычислимости (от А. Тьюринга до А.И. Мальцева);
- теории вычислительных машин архитектуры Дж. фон Неймана;
- теории порождающих грамматик Н. Хомского;
- теории вычислительной нейробиологии Дж. Марра и пр.

В частности, А.Н. Колмогоровым был выдвинут важнейший методологический тезис искусственной жизни: «если свойство той или иной материальной системы «быть живой» или обладать способностью «мыслить» будет определено чисто функциональным образом (например, любая система, с которой можно обсуждать проблемы современной науки и литературы будет признаваться мыслящей), то придется признать в принципе вполне осуществимым искусственное создание живых и мыслящих существ» [12].

По мнению А.Н. Колмогорова переработка информации и процессы управления в живых организмах построены на сложном переплетении:

- а) дискретных (цифровых) и непрерывных механизмов;
- б) детерминистического и вероятностного принципов действия.

При этом дискретные механизмы являются ведущими: «Не существует состоятельных аргументов в пользу принципиальной ограниченности возможностей дискретных механизмов по сравнению с непрерывными. При анализе явлений жизни существенно не диалектика бесконечного, а диалектика большого (чисто арифметическая комбинация большого числа элементов создает и непрерывность, и новые качества)» [12].

¹⁹⁰ Петренко Сергей Анатольевич, д-р техн. наук, профессор, Казань, Центр ИБ Университет Иннополис, s.petrenko@rambler.ru

Современные исследования когнитивных систем проводятся на основе нейрофизиологических принципов построения нервной системы и когнитивных методов познавательной и мыслительной деятельности человека.

Технологический задел для решения задачи.

В качестве технологической основы для решения поставленной задачи предлагается рассмотреть современные программно-аппаратные комплексы анализа и обработки *событий* информационной безопасности [21]. В международной практике упомянутые комплексы развиваются в составе специализированных центров безопасности, известных как Computer Emergency Response Team (CERT) или Computer Security Incident Response Team (CSIRT) или Security Operation Center (SOC).

В Российской Федерации уже создан ряд государственных и корпоративных центров *обнаружения, предупреждения и ликвидации последствий компьютерных атак* или центров реагирования на инциденты компьютерной безопасности, которые по своей функциональности аналогичны зарубежным CERT/CSIRT/SOC. В отечественной практике они известны как СОПКА или СПОКА, например: GOV-CERT.RU (ФСБ России), СПОКА Минобороны, FinCERT (Банк России), CERT Ростехнологий, SOC Газпрома и пр.

Указом Президента РФ от 15.01.2013 №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» установлено, что ФСБ России разрабатывает методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации и организует работы по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА).

Концепцией государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы Российской Федерации, утвержденной Президентом РФ 12 декабря 2014 года № К 1274, определен системный облик государственной СОПКИ. Основу СОПКИ составляют специальные центры обнаружения, предупреждения и ликвидации последствий компьютерных атак, которые подразделяются на центры:

- ФСБ России, предназначенные для защиты информационных ресурсов органов государственной власти;
 - Государственных и коммерческих организаций, предназначенные для защиты собственных информационных ресурсов.
- При этом упомянутые центры координируются Национальным координационным центром по компьютерным преступлениям при ФСБ России.

Вместе с тем, на практике создание *когнитивной системы раннего предупреждения о компьютерном нападении на информационные ресурсы Российской Федерации* оказалось далеко не тривиальной задачей. Потребовалось провести соответствующие научные исследования и решить ряд сложных научно-технических задач.

Например, такие задачи, как *классификация входных данных, выявление первичных и вторичных признаков компьютерного нападения, раннее обнаружение кибератак, многофакторное прогнозирование компьютерного нападения, моделирование распространения кибератак, обучение, порождение новых знаний о количественных закономерностях информационного противоборства и пр.* не имели готовых стандартных решений.

Кроме того, нужно было обеспечить сбор, обработку, хранение и проведение аналитических вычислений на сверхбольших объемах структурированной и

неструктурированной информации от разнообразных источников Inernet/Intranet и IoT/IIoT (тематика *Big Data u Big Data Analytics*).

Возможные технологические решения для создания когнитивной системы раннего предупреждения о компьютерном нападении на информационные ресурсы Российской Федерации представлены в презентации к докладу.

Здесь достаточно важной задачей оказалась задача выбора и реализации компоненты потоковой обработки больших данных, Big data (см. табл.1)

Таблица 1. Известные решения потоковой и пакетной обработки данных

Решение	Разработчик	Тип	Описание
Storm	Twitter	Потоковая	Новое решение для потокового анализа больших данных Twitter
S4	Yahoo!	Потоковая	Распределенная платформа потоковой обработки Yahoo!
Hadoop	Apache	Пакетная	Первая реализация парадигмы MapReduce с открытым исходным кодом
Spark	UC Berkeley AMPLab	Пакетная	Новая аналитическая платформа, поддерживающая наборы данных в оперативной памяти. Оличается высокой отказоустойчивостью.
Disco	Nokia	Пакетная	Распределенная среда MapReduce Nokia
HPCC	LexisNexis	Пакетная	НПС-кластер для больших данных

Другой не менее важной задачей стала задача организации хранилища больших данных, Big Data. Дело в том, что на практике известные решения, например Cassandra или HBase, оказались мало пригодными из-за следующих ограничений:

- отсутствие компонент в базе данных для обеспечения эффективного хранения и поиска по временным рядам. При этом большинство известных решений не содержат средств интеграции по причине своей закрытости, а доступные открытые, например, *InfluxDB*, не отличаются высокой стабильностью работы;
- отсутствие логических связей между интерфейсами бизнес-логики и базы данных;
- дублирование функциональности системы в связи с разделением базы данных и логики обработки в гетерогенной среде решения;
- ограниченная производительность решения HBase, связанная с архитектурными особенностями решения.
- значительные накладные расходы Cassandra, связанные с синхронизацией данных на различных узлах и пр.

Возможная системная архитектура когнитивной системы раннего предупреждения о компьютерном нападении на информационные ресурсы Российской Федерации на основе рассмотренных выше *NBIC-технологий* представлена в презентации к докладу.

Заключение.

Полученный положительный опыт создания когнитивной системы раннего предупреждения о компьютерном нападении *ПАК «Предупреждение-2016»* свидетельствует о целесообразности поэтапного решения названной задачи.

Этап 1 – развитие технической компоненты традиционной СОПКИ на основе технологий больших данных, *Big Data* — создание высокопроизводительного корпоративного (ведомственного) сегмента обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Этап 2 - создание аналитической компоненты на основе «вычислительного когнитивизма» — реализация собственно когнитивной компоненты системы раннего предупреждения о компьютерном нападении, способной самостоятельно извлекать и порождать полезные знания из больших объемов структурированной и неструктурированной информации для операционной поддержки СОПКИ.

При этом упомянутую техническую компоненту *СОПКИ* на основе технологий *Big Data* целесообразно наделить функциями:

- сбора больших данных о состоянии информационной безопасности в контролируемых информационных ресурсах;
- обнаружения и ликвидации последствий компьютерных атак на информационные ресурсы;
- поддержки средств программно-технического мониторинга событий информационной безопасности;
- взаимодействия с центрами государственной СОПКИ;
- информирования по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и пр.

Упомянутую аналитическую компоненту на основе «вычислительного когнитивизма» целесообразно наделить функциями:

- раннего предупреждения о компьютерном нападении на информационные ресурсы;
- выявления и порождения новых полезных знаний о качественных характеристиках и количественных закономерностях информационного противоборства;
- прогнозирования инцидентов безопасности, вызванных известными и ранее не известными компьютерными атаками;
- подготовки сценариев сдерживания киберпротивника и планирования ответных действий, адекватных компьютерной агрессии;
- подготовки шаблонов методических документов по вопросам раннего предупреждения, пресечения и ликвидации последствий компьютерных атак и пр.

Литература

1. Петренко С.А., Петренко А.С. Новая Доктрина информационной безопасности Российской Федерации // Защита информации. Инсайд. 2017. №1 (73). С. 07-14.
2. Петренко С.А., Шамсутдинов Т.И., Петренко А.С. Научно-технические задачи развития ситуационных центров в Российской Федерации // Защита информации. Инсайд. 2016. №6 (72). С. 37-43.
3. Петренко А.С., Петренко С.А. Проектирование корпоративного сегмента СОПКА // Защита информации. Инсайд. 2016. №6 (72). С. 47-52.
4. Петренко А.С., Петренко С.А. Первые межгосударственные киберучения стран СНГ: «Кибер-Антитеррор-2016» // Защита информации. Инсайд. 2016. №5 (71). С. 57-63.
5. Петренко А.С., Петренко С.А. Технологии больших данных (BigData) в области информационной безопасности // Защита информации. Инсайд. 2016. №4 (70). С. 82-88.
6. 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.
7. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA// Вопросы кибербезопасности. 2015. №3(11). С. 2-14.
8. Петренко А.А., Петренко С.А. НИОКР агентства DARPA в области кибербезопасности // Вопросы кибербезопасности. 2015. №4 (12). С. 2-22.
9. Аналитический доклад. "Подходы к формированию и запуску новых отраслей промышленности в контексте Национальной технологической инициативы, на примере сферы "Технологии и системы цифровой реальности и перспективные "человеко-компьютерные" интерфейсы (в части нейроэлектроники)" М.: Агентство Стратегических Инициатив - АСИ, 2015. с. 79.
10. Аристотель. Сочинения. В 4 т. (Серия «Философское наследие»). М.: Мысль, 1975—1983.
11. Величковский Б.М. Когнитивные технические системы // Компьютеры, мозг, познание: успехи когнитивных наук / Отв. ред. Б.М. Величковский, В.Д. Соловьев. М.: Наука, 2008. С. 273–292.
12. Колмогоров А. Н. Автоматы и жизнь // В кн. «Кибернетика ожидаемая и кибернетика неожиданная», под редакцией А. И. Берга и Э. Кольмана. - Москва: Наука. - 1968. - С. 12 - 30.
13. Лейбниц Г.В. Сочинения в 4 т., - М.: Мысль, 1982.
14. Поспелов Д. А. Моделирование рассуждений. Опыт анализа мыслительных актов. — М.: Радио и связь, 1989.—184 с.
15. Редько В.Г. Эволюция, нейронные сети, интеллект. М.: Книжный дом «ЛИБРОКОМ» /URSS, 2013.
16. Станкевич Л.А. Искусственные когнитивные системы // Научная сессия НИЯУ МИФИ - 2010. XII Всероссийская научно-техническая конференция "Нейроинформатика-2010". Лекции. М.: НИЯУ МИФИ, 2010. С. 106-160.
17. Тарасов В.Б. От многоагентных систем к интеллектуальным организациям. Серия "Науки об искусственном", М.: Эдиториал УРСС, 2002. – 352 с.
18. Chomsky N. Syntactic Structures. — The Hague: Mouton, 1957. (Переиздание: Chomsky N. Syntactic Structures. — De Gruyter Mouton, 2002. — ISBN 3-11-017279-8..)
19. Marr D. Vision. An Informational Investigation into the Human Representation and Processing of Visual Information. Cambridge, Massachusetts, London, England: The MIT Press, 2010.
20. Neisser, U. (1967) Cognitive Psychology. Appleton-Century-Crofts New York.
21. Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80-81.

Establishment of a National Early Warning System for Computer Attacks
Petrenko S.A.¹⁹¹

The complex problem of early warning about a computer attack on departmental and corporate information resources of the Russian Federation was investigated. An approach is proposed to create the required warning systems is justified. The cognitive approach is It is shown. A possible architecture of a cognitive early warning system about a computer attack on the information resources of the Russian Federation is suggested.

Keywords: big data, information security, attack warning systems

¹⁹¹ Petrenko Sergei, Doctor of Technical Sciences, Professor, Kazan, IS Center University Innopolis, s.petrenko@rambler.ru

Обнаружение вторжений в компьютерные сети. технологии обнаружения аномальной активности

Родионов Д.Е.¹⁹², Рудакова Е.В.¹⁹³

Рассматривается система обнаружения вторжения, ориентированная на поиск аномалий взаимодействия контролируемых объектов

Ключевые слова: пороговые значения, СОА, меры и методы в обнаружении, аномальное поведение.

Система обнаружения атак (СОА), как и множество программных продуктов, должно удовлетворять ряду требований. Должны быть учтены современные технологии разработки, совместимость с другими программными продуктами и ориентировка на особенности современных информационных сетей.

Система обнаружения аномального поведения основана на том, что СОА известны некоторые признаки, характеризующие правильное или допустимое поведение объектов наблюдения. Под нормальным или правильным поведением понимаются действия, выполняемые объектом и не противоречащие политике безопасности.

Датчики-сенсоры аномалий идентифицируют необычное поведение, аномалии в функционировании отдельного объекта – трудности их применения на практике связаны с нестабильностью самих защищаемых объектов и взаимодействующих с ними внешних объектов.

В качестве объекта наблюдения может выступить сеть в целом, отдельный компьютер, сетевая служба (FTP-сервер), пользователь и прочее.

Датчики срабатывают при условии, что нападения отличаются от «обычной» (законной) деятельности. Здесь появляется еще одно слабое место, характерное в большей степени для конкретных реализаций, заключающееся в некорректности определения «дистанции» отклонения наблюдаемого поведения от штатного, принятого в системе, и определении «порога срабатывания» сенсора наблюдения.

Меры и методы используемые в обнаружении аномалии, включают в себя атрибуты:

- пороговое значение. Наблюдение за объектом выражаются в виде числовых интервалов. Выход за пределы этих интервалов считается аномальным поведением. В качестве наблюдаемых параметров могут быть, например, количество файлов, к которым обращается пользователь в данный период времени, число неудачных попыток входа в систему, загрузка центрального процессора и прочее. Пороги могут быть статическими и динамическими;
- статические меры. Решение о наличии атаки делается по большому количеству собранных данных путем их статистической предобработки;
- параметрические меры. Для выявления атак строиться специальный «профиль нормальной системы» на основе шаблонов;
- непараметрические меры. Здесь уже профиль строиться на основе наблюдения за объектом в период обучения;
- меры на основе правил (сигнатур). Они очень похожи на непараметрические статические меры. В период обучения составляется представление о нормальном

¹⁹² Родионов Д.Е., доцент, к.т.н, МГТУ им. Н. Э. Баумана., derodionov@yandex.ru

¹⁹³ Рудакова Е.В., МГТУ им.Н.Э.Баумана, Москва

поведении объекта, которое записывается в виде специальных «правил». Получаются сигнатуры «хорошего» поведения объекта;

- другие меры. Нейронные сети, генетические алгоритмы, позволяющие классифицировать некоторые наборы видимых сенсору-датчику признаков.

Следует отметить, что существует две крайности при использовании данной технологии:

- обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак (ошибки второго рода);
- пропуск атаки, которая не подпадает под определение аномального поведения (ошибка первого рода). Этот случай гораздо более опасен, чем ложное причисление аномального поведения к классу атак.

Поэтому при инсталляции и эксплуатации систем такой категории обычные пользователи и специалисты сталкиваются с двумя довольно нетривиальными задачами:

- построение профиля объекта – это трудно формализуемая и затратная по времени задача, требующая от специалиста по безопасности большой предварительной работы, высокой квалификации и опыта;
- определение граничных значений характеристик поведения субъекта для снижения вероятности появления одного из двух вышеназванных крайних случаев.

Обычно система обнаружения аномальной активности используют журналы регистрации и текущую деятельность пользователя в качестве источника данных для анализа. Достоинства системы обнаружения атак на основе технологии выявления аномального поведения можно оценить следующим образом:

- системы обнаружения аномалий способны обнаруживать новые типы атак, сигнатуры для которых еще не разработаны;
- обнаружения аномалий генерирует информацию, которая может быть использована в системах обнаружения злоумышленного поведения;
- не нуждается в обновлении сигнатур и правил обнаружения атак.

Недостатки систем на основе технологии обнаружения аномального поведения:

- системы требуют длительного и качественного обучения;
- системы генерируют много ошибок второго рода;
- системы обычно слишком медленные в работе и требуют большого количества вычислительных ресурсов.

Литература

1. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов - М.: Горячая линия-Телеком, 2016. – 220 с: ил.
2. Лукацкий А.В. Обнаружение атак – СПб: БХВ-Петербург, 2001. – 624 с.
3. Гамаюнов Д.Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов. Диссер. МГУ им. Ломоносова, 2007.
4. Шелухин О.И., Гармашев А.В. Обнаружение аномальных выбросов телекоммуникационного трафика методом дискретного вейвлет-анализа // Электронная волна и электронные системы. 2012. № 2. С. 15-26.
5. Люгер Д.Ф. Искусственный интеллект, стратегии и методы решения сложных проблем. 4-е изд. – М.: Вильямс, 2003. – 864 с.

Intrusion detection in computer networks. Technology to detect anomalous activity
Rodionov D.E., Rudakova E.V.¹⁹⁴

Abstract: Discusses the intrusion detection system focused on the anomaly detection of interaction of controlled objects.

Keywords: thresholds, the SOA, measures, and methods in the detection of anomalous behavior.

УДК 004.056.53

Исследование вопросов повышения эффективности анализа уязвимостей при проведении сертификационных испытаний программного обеспечения по требованиям безопасности информации

Полянский А.Ю.¹⁹⁵

Выполнено исследование существующих подходов к проведению анализа уязвимостей программного обеспечения в ходе сертификационных испытаний по требованиям безопасности информации. Рассмотрены особенности отечественной системы сертификации средств защиты информации по требованиям безопасности информации. В работе предложена модель программного средства, предназначенного для повышения эффективности анализа уязвимостей программного обеспечения при проведении сертификационных испытаний по требованиям безопасности информации.

Ключевые слова: информационная безопасность, сертификация программного обеспечения, анализ уязвимостей, тестирование на проникновение.

Введение

С бурным развитием информационных технологий проблеме информационной безопасности уделяется всё более пристальное внимание. Для повышения защищённости информации ограниченного доступа активно разрабатываются и используются различные средства защиты информации, которые, согласно Постановлению правительства Российской Федерации № 608, подлежат обязательной сертификации в рамках систем сертификации средств защиты информации. Сертификация – процедура независимого подтверждения соответствия изделия заявленным требованиям [1]. В рамках процедуры сертификации проводятся сертификационные испытания, одним из обязательных этапов которых в настоящее время является проведение анализа уязвимостей [2]. Могут быть выделены следующие особенности отечественной системы сертификации, связанные с процедурой анализа уязвимостей [3].

1. Отсутствие необходимого методического обеспечения. В настоящее время регулятором системы сертификации не выпущены типовые методики проведения анализа уязвимостей для конкретных типов объектов сертификации (например, веб-приложение или средство антивирусной защиты). Испытательные лаборатории вынуждены самостоятельно разрабатывать методики с учетом анализа общедоступных источников информации и своего опыта проведения испытаний, что ведет к увеличению времени сертификационных испытаний.

2. Наличие ограничений по времени сертификационных испытаний. Время, отводимое на проведение сертификационных испытаний в целом и анализа уязвимостей в частности, ограничено. Перед началом проведения сертификационных испытаний между заявителем на сертификацию и испытательной лабораторией, непосредственно проводящей работы, подписывается договор, в котором сторонами четко оговорены в том числе и сроки

¹⁹⁴ Rodionov D.E., Rudakova E.V., Bauman MSTU, Moscow

¹⁹⁵ Полянский Андрей Юрьевич, ЗАО «НПО «Эшелон», Москва, a.polyanskiy@npo-echelon.ru

проведения испытаний.

3. Широкий профиль специалистов испытательных лабораторий. Динамичность процесса сертификационных испытаний и номенклатуры типов объектов сертификации требуют от экспертов испытательных лабораторий быть специалистами практически во всех сферах, связанных с созданием тех или иных типов средств защиты информации. С другой стороны, это приводит к увеличению времени испытаний за счет времени «переключения» эксперта испытательной лаборатории с одного типа объекта на другой.

Все особенности, перечисленные выше, ведут к увеличению времени проведения сертификационных испытаний [4-8].

Таким образом, задача разработки и совершенствования методического обеспечения анализа уязвимостей, при проведении сертификационных испытаний по требованиям безопасности информации, в настоящее время является актуальной.

Цель исследования состояла в сокращении времени анализа уязвимостей при проведении сертификационных испытаний за счет разработки программного средства автоматизации деятельности экспертов испытательных лабораторий.

Типовая последовательность действий, выполняемых в ходе анализа уязвимостей программного обеспечения

Типовую методику проведения анализа уязвимостей можно в общем виде описать следующим образом [1, 4, 9]:

1. Идентификация объекта испытаний и оценка его готовности к проведению анализа уязвимостей. На данном шаге эксперт испытательной лаборатории определяет, соответствует ли испытательный стенд описанному в документации, а также исследует правильность его установки. По результатам выполнения шага в протоколе анализа уязвимостей отражается соответствие/несоответствие испытательного стенда указанному в документации.

2. Поиск потенциальных дефектов безопасности объекта испытаний в общей базе дефектов безопасности [10].

3. Поиск потенциальных шаблонов атаки на объект испытаний в общей базе шаблонов атак [11].

При выполнении шагов 2-3 критерием поиска являются:

- название разработчика программного обеспечения;
- название обеспечения;
- название обеспечения, аналогичного по функциям безопасности объекта испытаний;
- название класса продуктов, к которым относится объект испытаний (например, «межсетевой экран», «средство антивирусной защиты» или «система обнаружения вторжений»);
- название и версии модулей, разработанных сторонними разработчиками (это могут быть библиотеки, динамические библиотеки), которые входят в состав объекта исследований.

4. Сопоставление множества потенциальных дефектов безопасности множеству потенциальных атак [11]. На данном этапе анализируются взаимосвязи между найденным по результатам выполнения шага 2 множеством потенциальных дефектов и найденным по результатам выполнения шага 3 множеством потенциальных шаблонов атаки.

5. Фильтрация полученных взаимосвязей. На данном этапе из получившегося множества удаляются записи, которые неактуальны для оцениваемой конфигурации, а также объекта испытаний, а также записи, метод исследования которых не определен.

6. Разработка тестов на проникновение на основе получившегося множества пар «дефект безопасности» - «шаблон атаки».

7. Проведение тестирования на проникновение.

8. Оформление отчетных материалов. Занесение полученных в ходе предыдущего шага результатов в протокол анализа уязвимостей.

Предложения по повышению эффективности процесса анализа уязвимостей

Для решения задачи повышения показателей эффективности процесса анализа уязвимостей предлагается разработать программное средство автоматизации деятельности эксперта испытательной лаборатории. Разрабатываемое программное средство будет учитывать особенности отечественной системы сертификации и позволит повысить показатели эффективности за счет уменьшения времени проведения сертификационных испытаний (оптимизация анализа уязвимостей программного обеспечения по времени его проведения).

Входными данными программного средства будут являться следующие ключевые особенности объекта испытаний:

- название разработчика программного обеспечения;
- название программного обеспечения;
- название программного обеспечения, аналогичного по функциям безопасности объекта исследований;
- название класса продуктов, к которым относится объект испытаний (например, «межсетевой экран», «средство антивирусной защиты» или «система обнаружения вторжений»);
- название и версии модулей, разработанных сторонними разработчиками, которые входят в состав объекта испытаний;
- тип программного обеспечения (например, веб-приложение или другое прикладное программное обеспечение);
- архитектура программного обеспечения (клиент – сервер или автономное).

Предполагается, что данное программное средство будет являться экспертной системой, которая по введенным экспертом испытательной лаборатории входным данным будет производить анализ ключевых особенностей объекта испытаний. На выходе программного средства по результатам анализа входных данных эксперту будет предложен ряд тестов для дальнейшего проведения тестирования проникновения, которое будет выполняться экспертом для поиска уязвимостей объекта испытаний в рамках деятельности по анализу уязвимостей.

Выводы

По результатам проведенного исследования были обнаружены и описаны недостатки в существующем в настоящее время подходе к проведению анализа уязвимостей. Разработка описанного программного средства автоматизации позволит повысить эффективность анализа уязвимостей при проведении сертификационных испытаний по требованиям безопасности информации, поскольку в таком случае упрощается процедура подготовки эксперта к тестированию на проникновение. Поскольку подготовительный этап вместо эксперта теперь будет выполнять программное средство, его использование позволит уменьшить затрачиваемое экспертом на подготовительный этап время, а также уменьшить количество ошибок при проведении сертификационных испытаний, связанных с человеческим фактором.

Литература

1. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под ред. А.С. Маркова. М.: Радио и связь, 2012. 192 с.
2. Марков А.С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации // Оборонный комплекс - научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.
3. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls // Journal of Theoretical and Applied Information Technology. 2016. Т. 88. № 1. С. 77-88.
4. Барабанов А.В., Федичев А.В. Разработка типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации // Вопросы кибербезопасности. 2016. № 2 (15). С. 2-8.
5. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1 (2). С. 40-48.
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. Мельников П.В., Горюнов М.Н., Анисимов Д.В. Подход к проведению динамического анализа исходных текстов программ // Вопросы кибербезопасности. 2016. № 3 (16). С. 33-39.
8. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1 (2). С. 36-39.
9. Барабанов А.В., Евсеев А.Н. Вопросы повышения эффективности анализа уязвимостей при проведении сертификационных испытаний программного обеспечения по требованиям безопасности информации // Надежность и качество: труды Международного симпозиума. - Пенза, 2015. - С. 330-333.
10. Покрова С.В., Зганяйко Д.О. Автоматизация обнаружения и анализа различных классов уязвимостей программных продуктов. // Вісник СевНТУ. 2014. № 146. С. 193-196. URL: <http://elibrary.ru/download/58739144.pdf>
11. Скокова О.В., Киселёв А.А. Методика оценки информационной безопасности на основе перечня и классификации общеизвестных схем атак. // Современные проблемы телекоммуникаций. Материалы конференции. 2016. С. 190-200. URL: <http://elibrary.ru/item.asp?id=26404511>.

Научный руководитель: Барабанов Александр Владимирович, кандидат технических наук, директор департамента АО «НПО «Эшелон», ab@cnpo.ru.

The Research about Improving the Efficiency of Software Vulnerability Analysis During Security Evaluation Polyanskiy A.¹⁹⁶

Abstract. A research of the existing approaches to the vulnerability analysis during security evaluation was conducted. The specific features of the national certification system are described. A proposal how to raise efficiency of software vulnerability analysis during security evaluation.

Keywords: information security, security evaluation, vulnerability analysis, penetration testing

¹⁹⁶ Polyanskiy Andreiy, NPO Echelon, Moscow, a.polyanskiy@npo-echelon

Автоматическая идентификация личности по изображениям лиц с использованием сверточных нейронных сетей

Пугачев Д.А.¹⁹⁷

Задача автоматического распознавания личности по изображению лица является одной из актуальных задач машинного обучения. Получаемая таким образом информация может использоваться в системах безопасности, в интерфейсе человек-компьютер, в маркетинговых системах и в других целях, в том числе в составе систем компьютерного зрения. Рассматривается возможность и особенности использования для данной задачи сверточных нейронных сетей. Реализованная СНС показала достаточную точность и скорость работы при решении задачи распознавания личности.

Ключевые слова: простая СНС, распознавание образов, машинное обучение.

Введение

В настоящее время активно разрабатываются и используются системы идентификации личности по изображению лица. Одним из методов решения задачи идентификации личности по изображению лица является машинное обучение, одним из подходов к реализации которого является создание сверточных нейронных сетей [1]. Преимущества нейронных сетей - высокая точность распознавания и универсальность [2]. Их недостатками являются высокие требования к производительности вычислительной системы, следовательно - долгое время обучения, сложность создания архитектуры сети для конкретной задачи и высокие требования к подготовке обучения сети. В дополнение к названным свойствам сверточных нейронных сетей, необходимо отметить возможность использования сверточных нейронных сетей для решения побочных задач в процессе идентификации личности, а также возможность построения систем компьютерного зрения на их базе [3].

Особенности архитектуры сверточных нейронных сетей для классификации изображений

Проведена работа с простой сверточной нейронной сетью. Слои в ней находятся один за другим, цепочкой. Выбор сверточной нейронной сети обусловлен ее большей эффективностью при многократно меньших требованиях к вычислительной системе при решении задачи распознавания личности по изображению. Использование архитектуры простой СНС обусловлено раздельным решением задач обнаружения лица на изображении и идентификации личности по найденному изображению лица.

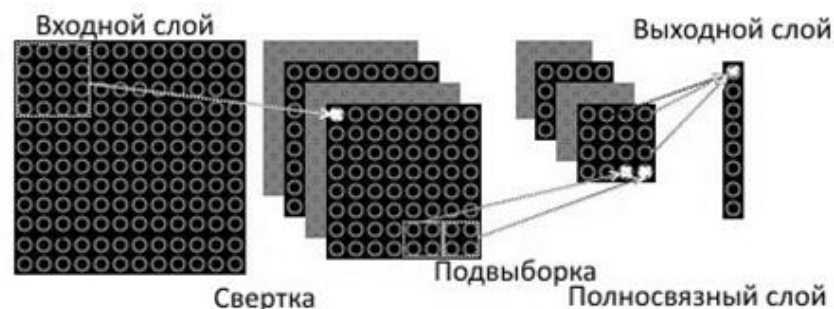


Рис.1. Обобщенная схема архитектуры простой нейронной сети

Представлена обобщенная архитектура простой сверточной нейронной сети (рис.1), слой свертки (с-слой, convolution) используется для получения карты признаков

¹⁹⁷ Пугачев Денис Александрович, Московский технический университет связи и информатики, г. Москва, 16den16@mail.ru

изображения, слой подвыборки (s-слой, subsampling, пространственное объединение) используется для снижения размерности вектора признаков, полносвязный слой используется для классификации [4].

Реализованная нейронная сеть производит распознавание идентификатора на закрытом множестве, то есть исходя из предположения, что идентифицируемый индивид точно присутствует в базе идентификаторов. При этом в качестве базы выступает сама СНС.

Для обнаружения лица использовалась полностью сверточная нейронная сеть, не имеющая полносвязного слоя. Подобная архитектура позволяет проводить обнаружение нескольких лиц на изображении и минимизировать количество ложных срабатываний на кадрах, в которых отсутствует изображение лица. Обнаружение лица проводилось отдельным шагом перед идентификацией для того, чтобы обнаруженные изображения лиц было легче масштабировать перед распознаванием.

Подготовка базы изображений

Для экспериментов использовались базы изображений Face Recognition Data, Georgia Tech Face Database и AT&T "The Database of Faces", находящиеся в открытом доступе, а также собственные изображения [5, 6, 7]. Используемые изображения имеют различный фон, освещение и другие условия съемки. Лица на них имеют различный масштаб, выражение, положение в кадре, поворот, детали и другие различия. Представлен пример изображений из созданной базы данных (рис.2).



Рис.2. Примеры изображений из базы

Локализация лица на изображении

Для локализации лица на изображении в разработанной программе используется алгоритм на базе полностью сверточной нейронной сети, в которой отсутствует полносвязный слой. Такая нейронная сеть позволяет достаточно точно проводить обнаружение одновременно нескольких изображений лиц в одном кадре. При этом если в кадре нет лица, то сеть ничего не отметит и не произойдет ошибочное срабатывание.

В ходе проверки работы модуля локализации лица на изображении было проведено его обучение и проверка на 250 тестовых изображениях, не участвовавших в обучении. Достаточную точность локализации модуль показал на 241 изображениях в тестовой выборке, что составляет 96 процентов тестовой выборки.

Эксперименты со сверточной нейронной сетью для классификации изображений

Вначале обучение разработанной сверточной нейронной сети проводилось на 3950 изображениях, по 10 на каждый идентификатор, 9 из которых использовались для обучения сети, а 1 для проверки во время обучения. В описываемом эксперименте обучение проходило в течение 67 эпох. Для проверки сети использовались 3950 изображений, не принимавших участие в обучении сети. Распознавание идентификатора происходит по характеристикам, получаемых при вычислении блоков СНС для конкретного изображения. В результате вычисления всех слоев СНС для тестового изображения получается массив характеристик, в котором каждое значение отражает совпадение исследуемого

изображения с записью в базе. Индексы этих характеристик соответствуют идентификаторам записи в базе. Показаны некоторые из полученных во время эксперимента на выходе СНС характеристик (рис.3).

1	2	3	4	5	6	7	8	9	10
24.4488	5.8379	-3.0543	-5.8088	-3.3286	-2.6204	1.5297	-2.9885	-13.6593	-0.7056

Рис.3. Пример получаемых на выходе сети характеристик

В качестве распознанного идентификатора принимается индекс максимального значения в массиве выходных характеристик. В результате описываемого эксперимента 3087 идентификаторов из 3950 было распознано верно, 863 ошибочно. Вероятность правильного распознавания составила 78.2% для изображений, не участвовавших в обучении сети. Также проводились эксперименты с наборами искаженных изображений. За основу были взяты изображения из базы FRD, не участвовавшие в обучении СНС. В различных экспериментах к ним применялись следующие искажения: поворот изображения на случайный угол до 1°, до 2°, до 3°, до 4°, до 5°, в случайном направлении по часовой или против часовой стрелки, изменение яркости изображения, искажение изображения гауссовским шумом. Вероятность правильного распознавания, полученная в этих экспериментах составила соответственно 77.6, 77.4, 76.9, 75.8, 72.3, 77.3, 74.2 процентов. Относительно малая точность распознавания обусловлена использованием изображений малого разрешения и сверточной нейронной сети с достаточно малым количеством слоев. Подобная конфигурация сети выбрана для повышения скорости работы, поскольку нейронная сеть с более сложной архитектурой будет иметь большие ограничения при практическом использовании из-за повышенных требований к производительности вычислительной системы и времени работы [8]. При этом большая часть некорректных срабатываний зафиксирована на изображениях, имеющих нехарактерный для использованных в обучении масштаб лица в кадре для данного идентификатора.

В дальнейшем проводилось обучение сверточной нейронной сети на 4000 изображений, по 10 на идентификатор, при этом использовались измененные изображения с более точно локализованными и масштабированными изображениями лиц. Сеть проходила обучение в течение 94 эпох. В ходе проверки использовались 4000 изображений, не присутствующих в обучающей выборке. На изображениях из тестовой выборки также проводилась локализация лица. Вероятность правильного распознавания идентификатора в данном эксперименте составила 91.6%.

Выводы

На основании полученных результатов сделан вывод о том, что разработанная сверточная нейронная сеть может быть обучена и использована для достаточно точного распознавания личности по изображению лица. В ходе экспериментов установлено, что данная сеть имеет достаточную устойчивость к изменениям освещения в кадре, различным частично перекрывающим изображение лица деталям, к изменениям выражений лица, к различиям в расположении лица в кадре и к искажению изображений. Также установлено, что данная сверточная нейронная сеть имеет малую устойчивость к изменению масштаба лица на изображении, что может быть преодолено за счет отдельного проведения шагов локализации лица на изображении и масштабирования.

Литература

1. Горемыкин И.В., Соловьев А.С., Бутенко Л.Н. Модели глубокого машинного обучения // Известия Волгоградского государственного технического университета. 2016. №3(182). С. 26-32.
2. Ефимов И.Н., Косолапов А.М. Методы автоматического распознавания лиц в системах безопасности // Перспективы развития информационных технологий. 2016. №28. С. 151-156.
3. Федотов Д.В., Попов Е.А., Охорзин В.А. Оптимизация структуры сверточной нейронной сети с помощью самоконфигурируемого эволюционного алгоритма в одной задаче идентификации // Вестник

Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2015. №4. С. 857-863.

4. Шелухин О.И., Пугачев Д.А. Автоматическая идентификация личности по изображениям лиц в видеопотоке с помощью сверточной нейронной сети // Спецтехника и связь. 2016. №3.

5. Face image database Face Recognition Data, University of Essex, UK [электронный ресурс]. 20.07.2008. URL: <http://cswww.essex.ac.uk/mv/allfaces/index.html> (дата обращения: 19.10.2016)

6. Face image database «Georgia Tech Face Database» [электронный ресурс]. 2005. URL: http://www.anefian.com/face_reco.htm (дата обращения: 19.10.2016)

7. Face image database AT&T "The Database of Faces" (formerly "The ORL Database of Faces") [электронный ресурс]. 2002. URL: <http://www.cl.cam.ac.uk/Research/DTG/attarchive/facedatabase.html> (дата обращения: 19.10.2016)

8. Дорогой Я.Ю. Архитектура обобщенных сверточных нейронных сетей // Вісник національного технічного університету України "Київський політехнічний інститут". серія: інформатика, управління та обчислювальна техніка. 2011. №54. С. 229-234.

Научный руководитель: Шелухин Олег Иванович, профессор, д-р техн. наук, Заведующий кафедрой «Информационная безопасность», Московский технический университет связи и информатики, г. Москва, ул. Авиамоторная, д. 8а, sheluhin@mail.ru

Automatic Person Identification for Face Images Using Convolutional Neural Networks

D. Pugachev¹⁹⁸

The problem of automatic recognition of the individual face image is one of the urgent tasks of machine learning. The resulting information can be used in security systems, the interface man-computer, marketing systems, and for other purposes, including the composition of computer vision systems. The possibility and peculiarities of usage for a given task convolutional neural networks are investigated. Implemented CNN showed sufficient accuracy and speed in solving the problem of identification.

Keywords: simple CNN, pattern recognition, machine learning.

¹⁹⁸ Denis A. Pugachev, Moscow Technical University of Communications and Informatics, Moscow, 16den16@mail.com

Сравнительный анализ систем управления информационной безопасностью и событиями безопасности

Самсонова В.Г.¹⁹⁹, Кулинич Р.С.²⁰⁰

В работе представлено сравнение зарубежных и отечественных систем управления информационной безопасностью и событиями безопасности, а также рассмотрена проблема обработки данных, собранных с нестандартных источников событий. Описаны положения законодательства РФ, касающиеся систем управления ИБ и событиями безопасности, и их влияние на проблему нормализации событий. На основании этого исследования произведено обоснование актуальности создания такой функциональной возможности SIEM-систем, как автоматическая генерация правил нормализации.

Ключевые слова: информационная безопасность, SIEM-системы, источники событий, законодательство, сертификация, средство защиты информации

Введение

В последние годы вслед за мировым трендом в Российской Федерации широкое применение в области обеспечения информационной безопасности на крупных предприятиях получили системы управления ИБ и событиями безопасности [1, 2]. В данный момент на российском рынке существует большой выбор систем этого класса – начиная от крупнейших мировых производителей программного обеспечения (ПО) и заканчивая небольшими отечественными фирмами.

В докладе будут рассмотрены три SIEM-системы (McAfee Security Information and Event Management, HP ArcSight ESM, IBM Security QRadar SIEM), которые по данным магического квадранта Gartner по системам управления ИБ и событиями безопасности за 2016 год занимали лидирующие позиции, и три SIEM-системы отечественного производства (KOMRAD Enterprise SIEM, MaxPatrol SIEM, SIEM «SECURITY CAPSULE»).

Сравнение систем управления ИБ и событиями безопасности

Основной задачей систем управления ИБ и событиями безопасности является анализ данных, поступающих от различных систем, поэтому SIEM – системы обычно включают в себя поддержку нескольких десятков типов источников журналов, таких как операционные системы (ОС), различные средства защиты информации (СЗИ), серверы приложений (например, веб-серверы, серверы электронной почты), и даже физические устройства контроля безопасности, такие как считыватели карт [2]. Для каждого поддерживаемого типа источника журнала SIEM – системы обеспечивают классификацию наиболее важных регистрируемых полей. Существует множество различных источников событий, и для понимания конкретного журнала событий используют специальные программные модули – коннекторы [3-7]. С помощью коннекторов происходит нормализация событий, т.е. их разбор (parsing). Описанное выше, визуально отображено на рисунке 1.

¹⁹⁹ Самсонова Вера Григорьевна, студентка, МГТУ им. Н.Э. Баумана, Москва, vgsamsonova@bk.ru

²⁰⁰ Кулинич Роман Сергеевич, МГТУ им. Н.Э. Баумана, Москва, kulinichrs@gmail.com

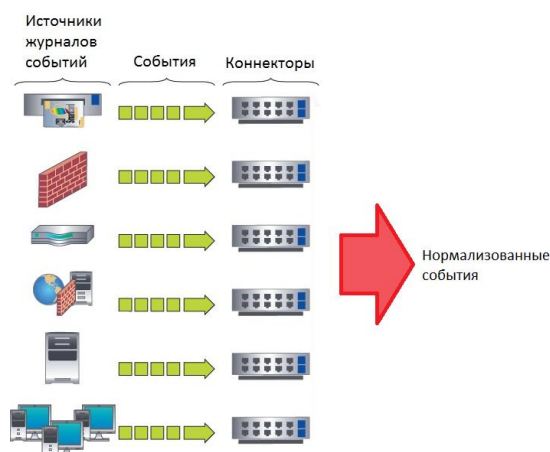


Рисунок 1. Уровень сбора данных

В ходе исследования были изучены основные характеристики SIEM-систем, которые производители указали на официальных сайтах продуктов. На основании полученной информации были сформированы критерии оценки: количество поддерживаемых источников событий, возможность подключения нестандартных источников, совместимость с отечественными СЗИ, поддерживаемые платформы, включение в реестр российского ПО²⁰¹, наличие сертификата соответствия²⁰² и цена.

Указанные выше критерии представлены в форме таблицы (таблица 1), из которой видно, что зарубежные SIEM-системы обладают внушительным набором поддерживаемых источников, так называемых «из коробки», отечественные – значительно отстают. Этот недостаток российского рынка SIEM - систем компенсируется поддержкой отечественных источников событий, таких как ОС Astra Linux, Антивирус Касперского и других [8-13]. Такие источники отсутствуют во всех западных конкурентах.

Кроме того, во многих компаниях используются программы собственной разработки, для которых не существует готовых коннекторов. Во всех рассматриваемых SIEM-системах есть возможность подключения нестандартных источников, которая осуществляется посредством встроенного редактора или возможностью запросить у разработчика создать готовый плагин. Первый метод имеет недостаток в том, что все-таки нужно разрабатывать, тестировать, а в дальнейшем и обслуживать этот коннектор самостоятельно. Второй – непосредственно влияет на цену SIEM-систем. К примеру, в состав ArcSight ESM входит СУБД Oracle, но даже ее стоимость оказывается незначительной, по сравнению с общей ценой решения [12]. В таблице приведены минимально возможные цены на SIEM-системы (с минимальной конфигурацией)²⁰³.

²⁰¹ Единый реестр российских программ для ЭВМ и БД. URL: <https://reestr.minsvyaz.ru/> (дата обращения: 30.10.2016).

²⁰² Государственный реестр сертифицированных СЗИ N РОСС RU.0001.01БИ00. URL: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi> (дата обращения: 30.10.2016).

²⁰³ Сравнение цены в данном случае является некорректным, так как конечная стоимость зависит от многих параметров, которые для различных производителей отличаются. Здесь приведен этот критерий сравнения лишь для того, чтобы показать, что SIEM-системы достаточно дорогие для внедрения.

Результаты аналитического обзора нормативных и методических документов, имеющих отношение к системам управления ИБ и событиями безопасности

После изучения информации о существующих SIEM-системах из открытых источников и составления таблицы, были проанализированы нормативные и методические документы, регламентирующие использование SIEM-систем в РФ. Изучены научные статьи, описывающие проблемы, возникающие при сертификации СЗИ, в т.ч. SIEM-систем, и, как результат, сделан вывод о возможном решении этих проблем.

Таблица 1.

Сравнение SIEM-систем

	McAfee Security Information and Event Management	HP ArcSight ESM	IBM Security QRadar SIEM	KOMRAD Enterprise SIEM	MaxPatrol SIEM	SIEM «SECURITY CAPSULE»
Количество поддерживаемых источников событий	Более 400	Более 350	Более 300	Более 180	Более 50	Более 15
Возможность подключения нестандартных источников	+	+	+	+	+	+
Совместимость с отечественными СЗИ	Возможность доработки	Возможность доработки	Возможность доработки	Комплекс "Рубикон", Форпост, Astra Linux, Сканер-BC 3.4 (3.5), SecretNet 3.5-3.7 (сервер управления), SolidWall WAF, БлокХост-Сеть, Efros Config Inspector, vGate R2, Jinn-Server, VIPNet IDS, АССОИ Матрица, SecretNet 7.6.604.0, InfoWatch 6.1, Kaspersky Endpoint Security 10, возможность доработки	Continent, SecretNet, vGate, PT AppSec, PT HoneyPot, PT MultiScanner, Kaspersky Security Center	eToken, ZlocK, Device Lock, Блок-Хост, Dallas Lock, Доктор WEB, NOD32, Антивирус Касперского, Аванпост, Falcongaze

	McAfee Security Information and Event Management	HP ArcSight ESM	IBM Security QRadar SIEM	KOMRAD Enterprise SIEM	MaxPatrol SIEM	SIEM «SECURITY CAPSULE»
Поддерживаемые платформы (рассматриваются только программные решения)	виртуальная машина для виртуальных сред VMware	Red Hat Enterprise Linux 6.4 и 6.5, SUSE 11 SP3, Windows Server 2012	виртуальная машина для виртуальных сред VMware	виртуальная машина для виртуальных сред VMware	OC Windows XP\7\8, OC Windows Server\2008\2010\2012	OC Microsoft Windows XP\7\8\10, Windows Sever 2010\2012, OC Linux
Включение в реестр российского ПО	-	-	-	+	+	+
Наличие сертификата соответствия	серия	300	серия	серия	-	-
Цена	От 3 млн. руб	от 4 млн. руб.	от 3 млн. руб.	От 300 тыс. руб	от 3 млн. руб.	от 200 тыс. руб.

В России вступили в силу положения законодательства об использовании российского программного обеспечения и запрет на закупки иностранного программного обеспечения при наличии российских аналогов, удовлетворяющих разумным требованиям государственных и муниципальных заказчиков. Программное обеспечение признается российским, если сведения о нем включены в единый реестр российских программ для электронных вычислительных машин и баз данных. То есть, в госорганах и муниципальных органах использование SIEM-систем, таких как McAfee Security Information and Event Management, HP ArcSight ESM, IBM Security QRadar SIEM, как правило запрещено, так как есть аналоги²⁰⁴ - KOMRAD Enterprise SIEM, MaxPatrol SIEM, SIEM «SECURITY CAPSULE» и другие. Но бывают исключения.

В соответствии с законодательством РФ (Приказ № 17 ФСТЭК России от 11 февраля 2013г. "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"²⁰⁵, Федеральный закон РФ от 27 июля 2006 г. N 152-ФЗ " О персональных данных"²⁰⁶, Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"²⁰⁷), для государственных организации, негосударственных организации, работающих со служебной информацией государственных органов, и организации, работающих с персональными данными,

²⁰⁴ Аналоги в следующих классах: «Системы мониторинга и управления», «Средства обеспечения информационной безопасности», «Серверное и связующее программное обеспечение», «Системы сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных».

²⁰⁵ "Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании"..."

²⁰⁶ «Обеспечение безопасности персональных данных достигается, в частности: ...

... 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации"

²⁰⁷ "Меры по обеспечению безопасности персональных данных реализуются, в том числе, посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных."

использование сертифицированных программных продуктов является обязательным. McAfee Security Information and Event Management, HP ArcSight ESM, IBM Security QRadar SIEM и KOMRAD Enterprise SIEM имеют сертификаты соответствия в системе сертификации ФСТЭК России. SIEM от McAfee и KOMRAD от Эшелона имеют сертификаты по 4 уровню РД НДВ и ТУ, ArcSight и QRadar – только на соответствие ТУ. Так же KOMRAD Enterprise SIEM имеет сертификат на соответствие требованиям Минобороны России. Сертификат по 4 уровню контроля РД НДВ означает, что СЗИ можно использовать при защите конфиденциальной информации. Что касается соответствия техническим условиям, ни для одной из рассматриваемых SIEM-систем ТУ не доступны в открытом доступе, поэтому сложно сказать, какие характеристики проверялись. В технических условиях обычно указаны ограничения, накладываемые на использование ПО, например, операционная система. То есть для сертифицированных SIEM – систем при добавлении нового коннектора, необходимо проводить инспекционный контроль, что вводит дополнительные финансовые и временные затраты.

Вывод

На основании изложенного можно сделать вывод о том, что существует проблема совместимости SIEM-систем с источниками событий. Невозможно предусмотреть все возможные варианты источников событий, особенно на мировом уровне. Поэтому стоит потребовать в том, чтобы помимо большого встроенного числа коннекторов, было какое-то универсальное средство, которое могло бы автоматически генерировать правила нормализации. Такое решение позволило бы снизить стоимость SIEM-систем и позволило бы избежать процедуры инспекционного контроля при подключении нового нестандартного источника.

Литература

1. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности российской федерации в 2014 г // Вопросы кибербезопасности. 2013. №1. С.61-64.
2. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности // Мониторинг правоприменения. 2017. № 1 (22). С. 53-61.
3. Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80-81.
4. Кузнецов А.В., Ненашев С.М. Способ определения регистрируемых событий // Вопросы кибербезопасности. 2015. № 5 (13). С. 23-25.
5. Фадин А.А. На пути к развертыванию центра управления информационной безопасностью предприятия // Connect! Мир связи: наука. Бизнес. Управление. 2013. №4. С.57-60.
6. Фадин А.А., Авезова Я.Э. SIEM-решения по управлению и консолидации средств защиты информации // Автоматика. Информатика. 2015. № 1(36). С. 27-31.
7. КОМРАД // Разработки ЗАО "НПО "ЭШЕЛОН" URL: <https://npo-echelon.ru/production/65/9855> (дата обращения: 30.10.2016).
8. SIEM СИСТЕМА ПАКАБ «SECURITY CAPSULE» // SIEM Analytics URL: https://www.itb.spb.ru/3_2_2.php (дата обращения: 30.10.2016).
9. MaxPatrol SIEM // Positive Technologies URL: <https://www.ptsecurity.com/ru-ru/products/mpsiem/> (дата обращения: 30.10.2016).
10. IBM Security QRadar SIEM // IBM URL: <http://www-03.ibm.com/software/products/ru/qradar-siem> (дата обращения: 30.10.2016).
11. ArcSight ESM // Hewlett-Packard Enterprise URL: <http://www8.hp.com/ru/ru/software-solutions/siem-security-information-event-management/> (дата обращения: 30.10.2016).
12. Информационная Безопасность и Управление Событиями // Intel Security URL: <http://www.mcafee.com/ru/products/siem/index.aspx> (дата обращения: 30.10.2016).
13. Устройство корреляции событий информационной безопасности / Марков А.С., Цирлов В.Л., Фадин А.А., Титов А.В., Марков Г.А. // Патент на полезную модель RUS 166348 01.08.2016. 2016.

Научный руководитель: Цирлов Валентин Леонидович, кандидат технических наук, генеральный директор ЗАО «НПО «Эшелон», v.tsirlov@npo-echelon.ru.

Comparative Analysis of the Security Information and Event Management Systems

V.G. Samsonova²⁰⁸, R.S. Kulinich²⁰⁹

The paper presents a comparison of foreign and domestic security information and event management products, and the problem of data collected from unusual event sources is examined. The position of the Russian Federation legislation, concerning SIEM and their impact on problem of log normalization, is described. On the basis of this research the rationalization of relevance of invention of such a functionality of SIEM as automatic generation of normalization rules is produced.

Keywords: information security, SIEM-systems, event sources, legislation, certification, information security tool

УДК 621.396.6

Экспериментальные исследования алгоритма распознавания образов на основе SURF

Сараева Е.С.²¹⁰

В публикации приведены результаты численных экспериментов, проведенных с помощью разработанного автором программного обеспечения автоматизированного рабочего места (АРМ) для распознавания образов в условиях искажений и сложной фоновой обстановки. Приведены результаты анализа областей применимости метода SURF. Показано, что сочетание детерминированного подхода с применением матрицы дескрипторов рационально применение эвристик, основанных на нечеткой логике Заде.

Ключевые слова: Автоматизированное рабочее место, алгоритм, нечеткая логика распознавание.

Введение.

Анализ доступных публикаций [1-4], показывает, что задача идентификации людей по их биометрическим данным (СИЛ) является актуальной задачей в области разработки средств обеспечения информационной безопасности. Результаты известных работ остаются несистематизированными, что не позволяет создать единую научно-обоснованную технологию для создания СИЛ [4]. Задачу распознавания в общем случае не решают ввиду ее сложности, поэтому для каждого случая ищется новое решение. Создание АРМ для экспериментальных исследований и практической доработки СИЛ представляется актуальной задачей.

1. Постановка решаемых задач

Математическая постановка задачи. Пусть Ω – множество объектов распознавания (пространство образов); $\omega : \tilde{\omega} \in \Omega$ Ω – объект распознавания (образ). $g(\omega) : \Omega \rightarrow M$, $M = \{1, 2, \dots, m\}$ – индикаторная функция, разбивающая пространство образов на Ω на m непересекающихся классов $\Omega^1, \Omega^2, \dots, \Omega^n$. Индикаторная функция неизвестна наблюдателю. X – пространство наблюдений, воспринимаемых наблюдателем (пространство признаков).

²⁰⁸ V.G. Samsonova, Bauman University, vgsamsonova@bk.ru

²⁰⁹ R.S. Kulinich, Bauman University, kulinichrs@gmail.com

²¹⁰ Сараева Екатерина Станиславовна. МГТУ им.Н.Э.Баумана, katyasaraeva95@mail.ru

$x(\omega): \Omega \rightarrow X$ – функция, ставящая в соответствие каждому объекту Ω точку $x(\omega)$ в пространстве признаков. Вектор $x(\omega)$ – это образ объекта, воспринимаемый наблюдателем. В пространстве признаков определены непересекающиеся множества точек $K_i \in X$, $i = 1, 2, \dots, m$, соответствующих образам одного класса; $\hat{g}(x): C \rightarrow M$ – решающее правило – оценка для $g(\omega)$ на основании $x(\omega)$, т.е. $\hat{g}(x) = \hat{g}(x(\omega))$.

Пусть $x_j = x(\omega_j)$, где $j = 1, 2, \dots, N$ – доступные наблюдателю данные о функциях $\hat{g}(\omega)$ и $x(\omega)$, но сами эти функции наблюдателю неизвестны.

Тогда g_j, x_j , где $j = 1, 2, \dots, N$ – есть множество прецедентов. Задача заключается в построении такого решающего правила $\hat{g}(x)$, чтобы распознавание проводилось с минимальным числом ошибок. Пространство признаков можно считать евклидовым, т.е. $C = [R^n]$. Качество решающего правила измеряют частотой появления правильных решений. Обычно его оценивают, наделяя множество объектов Ω некоторой вероятностной мерой. Таким образом, оно записывается в виде $\min P \{ \hat{g}(x(\omega)) \neq g(\omega) \}$.

Классификация производится на основе сравнения с эталоном. В качестве эталона рассматривается силуэт объекта на сцене. Ориентация и положение объекта заранее не известны. Пространство признаков формируется с помощью матрицы Гессе. Факт присутствия эталона на сцене является случайным событием.

2. Описание предлагаемого технического решения

Решение поставленной задачи производилось с помощью ПО MATLAB и встроенного набора инструментов Image Processing Toolbox. Схема распознавания эталона на изображении приведена на Рис1.



Рисунок 1. Укрупненная схема распознавания эталона на изображении.

Блок 1. Получение входных данных. В реализованной версии программы под входными данными понимается два изображения в формате .jpg, одно из которых является эталонным, т.е. содержит объект для поиска. Второе изображение образует поле признаков.

Блок 2. Первичная обработка. Приведение изображений к черно-белому виду.

Блок 3. Выделение SURF-признаков. Поиск особых точек производится с помощью матрицы Гессе. Известно, что гессиан достигает экстремума в точках максимального изменения яркости. Матрица образуется вторыми частными производными функции. Если все производные существуют, матрица принимает следующий вид:

$$H(f) = \begin{bmatrix} \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} & \dots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \frac{\partial^2 f}{\partial x_2 \partial x_1} & \frac{\partial^2 f}{\partial x_2^2} & \dots & \frac{\partial^2 f}{\partial x_2 \partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \frac{\partial^2 f}{\partial x_n \partial x_2} & \dots & \frac{\partial^2 f}{\partial x_n^2} \end{bmatrix} \quad (1)$$

Детерминант матрицы
Гессе для двумерного случая:

$$\det(H) = \frac{\partial^2 y}{\partial x^2} * \frac{\partial^2 x}{\partial y^2} - \left(\frac{\partial^2 f}{\partial x \partial y} \right)^2 \quad (2)$$

Критические точки:

$\det(H) > 0 \Rightarrow x_0$ – точка локального минимума для функции f

$\det(H) < 0 \Rightarrow x_0$ – точка локального максимума для функции f

$\det(H) \geq 0 \cup \det(H) \neq 0 \Rightarrow x_0$ – точка локального минимума для функции f

Гессиан инвариантен относительно поворота и неинвариантен относительно масштабирования. Поэтому размер фильтра берется равным $4s$, где s – масштаб ключевой точки.

Блок 4. Модуль дескрипторного анализа. На вход блока поступают два массива дескрипторов, сформированных блоком 3. Назначением этого блока является непосредственное сопоставление массивов с целью поиска общих точек, которые могли бы указывать на нахождение объекта на сцене. При проведении численных экспериментальных исследований применен гистограммный метод для выбора наилучшей пары. Пример анализа сцены (Рис.2) приведен на Рис.3.



Множество тюльпанов



Эталон для поиска

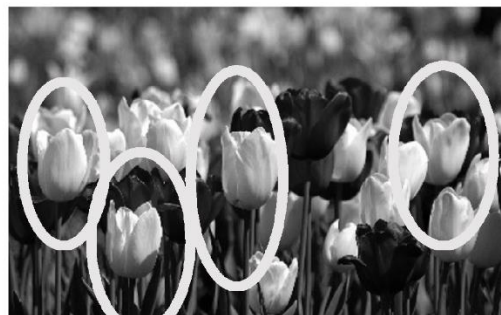


Рис.2. Изображения поля поиска и эталонов для поиска.

Метод основан на построении гистограммы областей и выборе наилучшего совпадения. На Рис. 3 приведены гистограммы изображений четырех объектов из предыдущего примера.

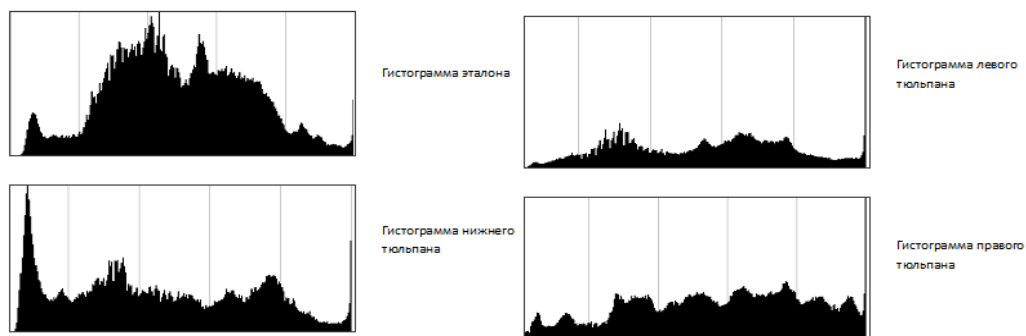


Рис. 3. Гистограммы изображений тюльпанов

Однако гистограммный метод не избавляет массив дескрипторов от «ложных» находений пар. Для исключения выбросов использовался алгоритм RANSAC, на вход которому подаются уже сформированные и обработанные массивы дескрипторов. Главным преимуществом является способность дать надежную оценку модели даже в случае большого количества ложных срабатываний.

3. Основные результаты численных экспериментов.

Программная реализация приведенного алгоритма была протестирована на трех выборках изображений различных размеров. Каждая выборка содержала 100 «сцен», которой ставилось в соответствие 100 эталонов. На рис.5 приведены графики времени работы алгоритма для каждой выборки и процент успешных распознаваний. Интересно, что для каждой группы изображений число ложных срабатываний, которые отсеиваются методом RANSAC, варьируется от 0 до 60. Начальное количество дескрипторов в среднем в 40 раз больше.



Рис.5. Графики времени работы и процента успешных распознаваний

В ходе работы были также проведены успешные тесты на выборках размытых изображений и для случаев, когда эталон является полупрозрачным.

Заключение. Экспериментальные исследования подтвердили работоспособность программного комплекса. Совместно с видеосистемами комплекс применим в области идентификации личности человека по его лицу или совокупности биометрических характеристик. На основе экспериментального анализа сделан вывод о возможности и целесообразности дополнения SURF эвристическими методами и алгоритмами.

Литература

1. А. Потапов. Системы компьютерного зрения: современные подходы и задачи. – Электронный журнал: Control Engineering Россия, 2014, февраль. <http://controleng.ru>
2. Мишунина Н.О. Разработка системы идентификации объекта по его изображению. – Журнал: Путь науки, 2015, 5(15). <http://elibrary.ru>
3. Спиридонов И.Н. Биометрические технологии в интегрированных автоматизированных системах безопасности государства. – Вестник МГТУ: приборостроение, 2015, S. <http://elibrary.ru>
4. Маркелов К.С. Идентификация и верификация личности – комплексная биометрическая информационная технология. - International Journal of Open Information Technologies, 2015, 3(5), 12-19. <http://elibrary.ru>

Научный руководитель: Чичварин Н.В., к.т.н, доцент МГТУ им. Н.Э. Баумана,
e-mail: genrih.gertz@gmail.com

Algorithm has been Tested Recognition on the Basis of Surf Saraeva.E.

Abstract: The publication presents the results of the numerical experiments conducted by the author with the developed software workstation for recognition in terms of distortion and difficult background conditions. It shows results of the application areas analysis for SURF method. It shows that the combination of a deterministic approach with the use of descriptors matrix rational use of heuristics based on fuzzy logic Zadeh.

Key words: workstation, algorithm, fuzzy logic, recognition.

Анализ социальных сетей и выявление сообществ Русских А.Н., Басараб М.А.²¹¹

Анализ социальных сетей и их математическое представление необходимы для выявления связей и нахождения внутренних закономерностей. В данной статье рассмотрены вопросы анализа социальных сетей на основе аппарата теории графов. Так как многие сети содержат в себе сообщества, то одна из задач – нахождение сообществ в сетях и выявление их участников. Показано, как представить социальную сеть в виде графа, выявить сообщества, рассмотрено свойство транзитивности применительно к анализу социальных сетей.

Ключевые слова: анализ социальных сетей, граф, сообщество.

Введение

Анализ социальных сетей (Social Network Analysis, SNA) подразумевает изучение взаимодействия между индивидуальными сущностями и группами. Обычно, отношения между индивидуальными сущностями, например, дружеские, можно представить в виде сети (графа), вершины которого – индивидуальные сущности, а дуги – взаимодействия между ними. Такой тип представления данных является преобладающим в традиционном анализе «больших» социальных сетей.

С развитием глобальных социальных сетей и сервисов пользователям стало намного проще установить связь друг с другом. Эта возможность позволила увеличить масштаб исследований и проводить анализ миллионов и более индивидуальных сущностей. Для примера можно взять сети адресов электронной почты [1], мгновенных сообщений, социальные сети [2], сети в биологии и т.п. Такие масштабные сети и огромные объемы данных, как правило, требуют особых подходов и больших вычислительных мощностей.

Одними из основных задач SNA являются следующие:

- анализ и нахождение центральной индивидуальной сущности в социальной сети;
- обнаружение сообществ на основе изучения сетевых структур и топологий;
- анализ позиции/роли, принадлежащей индивидуальной сущности во время взаимодействий в сети;
- классификация сетей и раннее обнаружение подозрительных сообществ.

Представление социальных сетей

Социальные сети представляются в виде графа $G(V, E)$, где V – вершины (индивидуальные сущности), E – дуги (связи). Связи удобно представлять в виде матрицы A , где элемент $A_{ij} \neq 0$ соответствует $(v_i, v_j) \in E$, а $A_{ij} = 0$ – случаю $(v_i, v_j) \notin E$. Степень вершины v_i обозначим как d_i . Для ориентированных графов выделяют входящую и исходящую степени: d_i^- и d_i^+ . Количество вершин и дуг в графе: $|V| = n$ и $|E| = m$ соответственно. Кратчайший путь между парой вершин v_i и v_j называется «геодезическим» и обозначается как $d(i, j)$. Связи вершины v обозначаются как $N(v)$. В ориентированном графе связи до и от вершины v обозначаются как $N^-(v)$ и $N^+(v)$ соответственно.

Структуры сообществ

Сообщество – это группа людей, члены которой имеют свойство взаимодействовать друг с другом больше, чем с индивидуальными сущностями за пределами группы [3]. Измерение эффекта сообщества связано с понятием транзитивности («друзья моего друга – мои друзья»).

²¹¹ Русских А.Н., МГТУ им.Н.Э.Баумана, Москва, russkikh.a@gmail.com; Басараб М.А., д-р физ.-мат. наук, профессор, МГТУ им.Н.Э.Баумана, Москва, m.basarab@bmstu.net

Для измерения транзитивности можно использовать коэффициент кластеризации. Пусть вершина v_i имеет d_i соседей и среди этих соседей существует k_i дуг. Тогда коэффициент кластеризации будет равен

$$C_i = \begin{cases} \frac{k_i}{d_i(d_i-1)/2}, & d_i > 1 \\ 0, & d_i = 0 \text{ или } 1 \end{cases} \quad (1)$$

Здесь знаменатель обозначает максимально возможное число дуг между соседями. Для сети, изображенной на рис. 1, коэффициент кластеризации вершины v_1 равен $C_1 = \frac{3}{10}$.

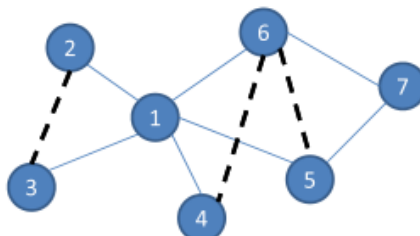


Рис. 1. Социальная сеть, визуализированная неориентированным графом

Рассмотрим еще один способ вычисления коэффициента кластеризации

$$C_i = \frac{\text{число треугольников соединенных с узлом } v_i}{\text{число связанных с вершиной } v_i \text{ треугольников}}, \quad (2)$$

где треугольник – это кортеж вида $(v_i \{v_j, v_k\})$, такой что $(v_i, v_j) \in E$ и $(v_i, v_k) \in E$, и вершины v_j и v_k не упорядочены. Например, треугольники $(v_1 \{v_3, v_6\})$ и $(v_1 \{v_6, v_3\})$ имеют одинаковый центр в вершине v_1 (см. рис. 1). Всего таких треугольников 10. Треугольники обозначают неупорядоченный набор трех вершин, таким образом, что каждые две имеют связи. Треугольники, имеющие связи с вершиной v_1 – это $\{v_1, v_2, v_3\}, \{v_1, v_4, v_6\}, \{v_1, v_5, v_6\}$, таким образом опять $C_1 = \frac{3}{10}$.

Для измерения структуры сообщества сети в целом используются следующие формулы «глобального» коэффициента кластеризации:

$$C = \sum_{i=1}^n \frac{C_i}{n}, \quad (3)$$

$$C = \frac{\sum_{i=1}^n \text{число треугольников соединенных с вершиной } v_i}{\sum_{i=1}^n \text{число связанных с вершиной } v_i \text{ троек}}, \quad (4)$$

$$C = \frac{3 * \text{количество треугольников в сети}}{\text{количество связанных троек с вершиной}}. \quad (5)$$

Вычисление глобального коэффициента кластеризации зависит от точности подсчёта треугольников в сети. Одним из методов подсчета является алгоритм подсчёта вершин (дуг), который проходит все вершины (дуги) для подсчета количества треугольников, соединенных с каждой вершиной (дугой). Следует отметить, однако, что это не самый оптимальный алгоритм, требующий большого количества памяти.

Коэффициент кластеризации и транзитивность более характерны для небольших сообществ, но в больших сетях можно выделить множество маленьких, «обособленных» сообществ, которые имеют связь со всей сетью посредством нескольких дуг. Такие сообщества сливаются с основной сетью и незаметны, если не рассматривать сеть более детально [5].

Выводы

Рассмотрен и описан минимально необходимый математический аппарат, используемый для анализа и визуализации социальных сетей с целью выявления сообществ. Можно отметить следующие перспективные направления дальнейших исследований:

- исследование развития сообществ с учетом развития и расширения сетей с течением времени;
- изучение неоднородных сетей с разными отношениями между индивидуальными сущностями (дружеские, партнерские, рабочие);
- выявление новых шаблонов для анализа сетей и нахождения сообществ; выявление признаков и свойств, по которым можно классифицировать индивидуальные сущности;
- разработка и совершенствование новых методов и алгоритмов визуализации для выявления шаблонов связей между различными группами, иерархическая визуализация, выявление наиболее важных сообществ.

Литература

1. Xiaoyan Fum Seok-Hee Hong, Nikola S. Nikolov, Xiaobin Shen, Yingxin Wu, Kai Xu. Vusialisation and Analysis of Email Networks.
2. A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee. Measurement and analysis of online social networks. In *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 29–42, New York, NY, USA, 2007. ACM.
3. J. Leskovec, K. J. Lang, A. Dasgupta, and M. W. Mahoney. Statistical properties of community structure in large social and information networks. In *WWW '08: Proceeding of the 17th international conference on World Wide Web*, pages 695–704, New York, NY, USA, 2008. ACM.
4. M. Newman, A.-L. Barabasi, and D. J. Watts, editors. *The Structure and Dynamics of Networks*. 2006.
5. Mohammad Ali Abbasi, Sun-Ki Chai, Huan Liu, and Kiran. Sagoo, *Real-world behavior analysis through a social media lens.*, Social Computing, Behavioral-Cultural Modeling and Prediction, Springer, 2012, pp. 18–26.
6. N. Agarwal, H. Liu, L. Tang, and P.S. Yu, *Identifying the influential bloggers in a community*, Proceedings of the International Conference on Web Search and Web Data Mining, ACM, 2008, pp. 207–218.

Social Network Analysis and Community Detection **Russkikh A., Basarab M.²¹²**

Abstract: social network analysis and mathematical describing is necessary for connections and pattern finding. In this article authors explain «graph» - basic mathematical apparatus for networks understanding. As far as authors concerned, many networks include communities, thereby one of the problem is community detection and community participants disclosure. Was shown, how to represented network as a graph, find communities and what is transitivity in case of social network.

Keywords: Social network analysis, Graphs, Community

²¹² Russkikh A., Bauman Moscow State Technical University, Moscow, russkikh.a@gmail.com; Basarab M., Dr. Sc., Professor, Bauman Moscow State Technical University, Moscow, m.basarab@bmstu.net

Создание приложения для работы со Smart-картой

Смолянинова К.А.²¹³

Доклад посвящен проблеме защиты данных пациента при использовании электронных историй болезни. Предложено применение Smart-карты для хранения идентификатора пациента, по которому он однозначно идентифицируется в базе электронных документов. Сформулированы требования к структуре данных, хранящихся на карте. Приведены блок-схема разработанного приложения, а также его особенности. Создано программное обеспечение для работы со Smart-картой.

Ключевые слова: ключевая пара, электронная история болезни, электронная подпись, Smart-карта пациента

Введение

В настоящее время в медицине распространен переход на электронный документооборот[1-3]. В частности, широкую популярность приобрела электронная регистратура, но истории болезней в большинстве медицинских учреждений по-прежнему хранятся на бумажных носителях. При переезде человека в другой район или город ему заводят новую медицинскую карту, и вся история о его прежних заболеваниях теряется.

В некоторых организациях уже начинается переход на системы электронных историй болезней (ЭИБ). Недостаток современных систем заключается в том, что доступ к истории болезни пациента может получить любой сотрудник, имеющий доступ к системе, без ведома пациента. Они позволяют внести, удалить или изменить любую информацию. Такие системы не являются безопасными, так как в них нарушаются принципы конфиденциальности и целостности информации и они не являются безопасными. Системы, которые оперируют такими важными данными, как информация о здоровье человека, должны быть надежно защищены.

Определяющую роль в этом процессе играет безопасный доступ к информации, а также обеспечение защиты при передаче данных и использовании электронных подписей [4-6].

Решением этих проблем является использование Smart-карты, которая хранится у пациента и позволяет однозначно идентифицировать его в единой базе электронных медицинских карт [7, 8].

Защита данных пациента при работе с системой ЭИБ

Рассмотрим особенности приема врача при использовании Smart-карт (рис. 1). Каждый участник процесса имеет личную Smart-карту, на которую записана его персональная информация.

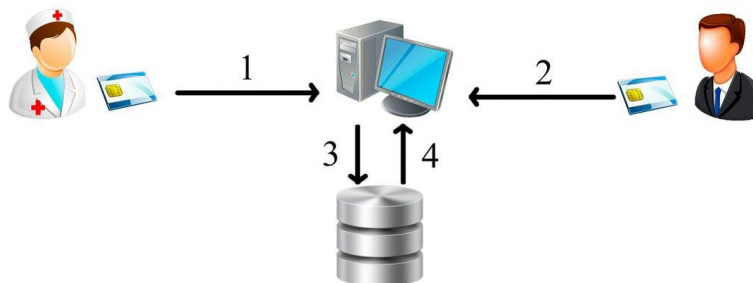


Рис. 1. Описание приема врача

²¹³ Смолянинова Кристина Александровна, МГТУ им. Н.Э. Баумана, Москва, kriszzztina@yandex.ru

В начале приема врач авторизуется с помощью своей смарт-карты (1) для получения доступа к системе ЭИБ. Приходя в медицинское учреждение, пациент предоставляет карту и вводит свой PIN-код (2). После этой процедуры, медицинский сотрудник, авторизованный в системе, получает доступ к идентификатору пациента, хранящемуся на карте. По этому идентификатору в базе данных (БД) производится поиск ЭИБ пациента (3), после чего она предоставляется медицинскому сотруднику (4). Далее он может создавать электронные персональные медицинские записи, после чего в соответствии с ГОСТ Р 52636-2006 обязан их подписать квалифицированной электронной подписью. Изменение записей может производиться только до момента подписания. После этого изменение или удаление записей из базы данных производится в особом порядке, прописанном в политике безопасности медицинской организации. Таким образом, медицинский сотрудник несет ответственность за подписанные им электронные документы. Для обеспечения целостности и достоверности информации в системе должен использоваться сервер доверенного времени.

Требования к структуре данных, хранящихся на карте

Данные, хранящиеся на карте, подразделяются на открытые и закрытые. В табл. 1 приведены данные, которые должны храниться на карте, их формат и размер занимаемой памяти.

Таблица 1.

Данные, хранящиеся на карте

Наименование элементов	Список допустимых значений	Размер занимаемой памяти, байт
Идентификатор пациента	12-значный номер	12
PIN-код	8-значный номер.	8
Идентификатор ЭМА	4-значный номер	4
Персональные данные (ФИО)	Строка, не более 50 символов	50
Группа крови и резус фактор	3 символа: (0+, 0-, A+, A-, B+, B-, AB+, AB-)	3
Сахарный диабет	1 символ	1
ВИЧ-статус	Один символ (+, -)	1
Гепатит	Один символ (0 – нет гепатита, A, B, C, D, E, F, G)	1
Хронические заболевания	Строка, 5 символов	10
Непереносимость лекарственных препаратов	Строка, 5 символов	10
Сертификат открытого ключа	Открытый ключ	64
Дайджест	Хэш всех данных карты	64

Описание работы приложения

Приложение предусматривает работу с двумя Smart-картами: картой врача и картой пациента. На карте врача хранится идентификатор и ключевая пара. На карте пациента хранятся следующие данные: идентификатор, фамилия, имя, отчество, базовая информация, подпись врача, сертификат открытого ключа.

Блок-схема работы приложения представлена на рис. 2.

При запуске программы и на протяжении ее работы происходит проверка наличия подключенной карты врача. Если при запуске программы карта отсутствует, появляется сообщение с просьбой подключить карту. После подключения происходит авторизация. Врачу предлагается ввести PIN-код карты. Если PIN-код верный, то происходит проверка подлинности карты методом Challenge-Response. Суть данного метода заключается в следующем. На карте врача хранится идентификатор. По этому идентификатору в базе данных выбирается открытый ключ, соответствующий врачу, для проверки подписи.

Приложение генерирует случайное число, хэширует его алгоритмом ГОСТ34.11-94. Затем хэша аппаратно подписывается картой по алгоритму ГОСТ34.10-2001. После этого с помощью открытого ключа из базы данных подпись проверяется. Если подпись верная, то врачу предоставляется доступ к системе. Для того чтобы продолжить работу с приложением, необходимо подключить вторую карту.

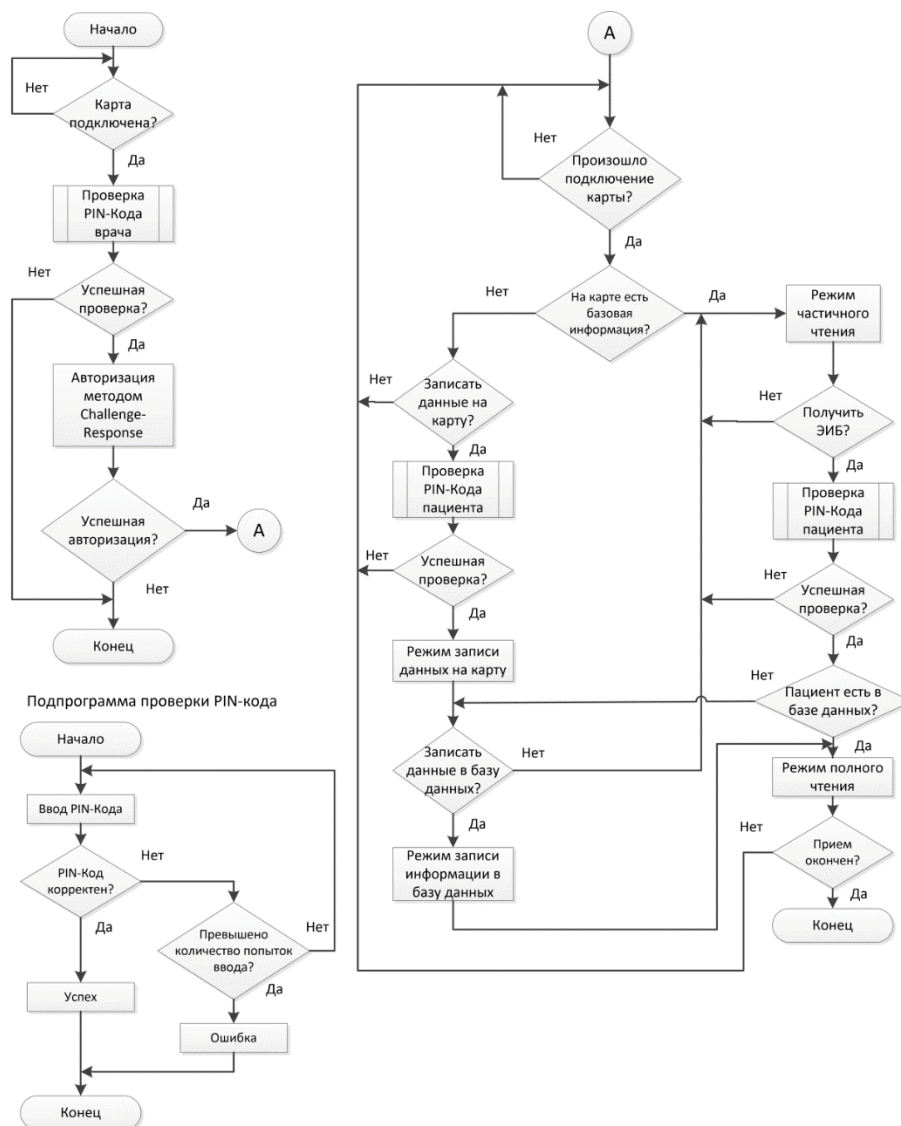


Рис.2. Блок-схема работы приложения

После подключения второй карты приложение предоставляет врачу три режима работы с картой пациента: «Режим записи», «Режим частичного чтения», «Режим полного чтения». Режимы записи и полного чтения доступны только после ввода PIN-кода пациентом. Режим частичного чтения доступен сразу после подключения карты пациента.

Программное обеспечение, которое осуществляет доступ к карте, разработано на языке программирования C++ в среде разработки QtCreator.

Выводы

В ходе выполнения работы было разработано программное обеспечение с пользовательским интерфейсом для работы со Smart-картой пациента. Реализованное приложение позволит повысить эффективность работы медицинского персонала, а также

обеспечить надежное хранение медицинских данных пациентов.

Литература

1. Хавкина Е.Ю., Уйба В.В., Олесов Е.Е., Макеев А.А., Максюков С.Ю., Аксаментов А.Д., Хавкин В.А. Недостатки заполнения медицинской документации как предпосылка для перехода к электронным историям болезни // Российский стоматологический журнал. 2010. № 5. С.45.
2. Ланцберг А.В., Тройч К., Булдакова Т.И. Развитие системы электронных услуг муниципальной поликлиники (на основе анализа зарубежных web-ресурсов) // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2011. № 4. С. 1-7.
3. Ланцберг А.В., Тройч К., Булдакова Т.И. Особенности оценки качества медицинской электронной услуги // Информационное общество. 2011. № 4. С. 28-37.
4. Грачева Т.Ю. Электронная история болезни: защита медицинской информации: М. Компания Спутник, 2005. 266С.
5. Монич В.А., Кушников О.И., Алакаев Р.Р., Косоногов А.Я., Коротин Д.П., Медоваров Е.В. Электронная история болезни - важнейшее звено медицинских информационных систем // Современные технологии в медицине. 2010. № 3. С.73-74.
6. Булдакова Т.И., Суятинов С.И., Миков Д.А. Анализ информационных рисков виртуальных инфраструктур здравоохранения // Информационное общество. 2013. №4. С. 6.
7. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. Под. ред. А.С.Маркова. - М.: Радио и связь, 2012. 192 с.
8. Встраивание устройств Рутокен через PKCS#11 [Электронный ресурс]. Режим доступа: <http://dev.rutoken.ru/pages/viewpage.action?pageId=13795364> (дата обращения 20.10.2016).

Научный руководитель: Булдакова Татьяна Ивановна, доктор технических наук, профессор, МГТУ им. Н.Э. Баумана, buldakova@bmstu.ru

Development of Software Application for Working with Smart-Card Smolyaninova K.A.²¹⁴

At present it is common to use digital document management in medicine. Digital desk became very popular, but in most clinics clinical records are still stored on paper. Paper clinical records are often getting lost. Restore them is almost impossible. Also possible is a situation that the person has moved to another district, or even the city. In order to get medical help, the one must attach to medical organization first. After that the patient gets a new clinical record and all information about his previous diseases gets lost. The solution is to use the Smart-card that patient have and that can uniquely identify him in the unified digital clinical records database. The application for working with a Smart-card was developed in this work.

Keyword: *keypair, digital clinic record, digital signature, patient Smart-card*

²¹⁴ Smolyaninova K.A., Bauman Moscow State Technical University, Moscow, kriszzztina@yandex.ru

Обзор методов и средств оценки рисков информационной безопасности Скворцов М.А.²¹⁵, Шахалов И.Ю.²¹⁶

В статье детально рассмотрен процесс оценки рисков информационной безопасности. Представлен обзор наиболее распространенных методов их оценки. Проанализированы их достоинства и недостатки. Предложены возможные пути дальнейшего развития методик.

Ключевые слова: информационная безопасность, оценка информационных рисков, факторы риска, этапы оценки, симплекс-метод, интеллектуальный анализ данных

Введение

Для реализации информационных сервисов в современных банковской и финансовой сферах, в сфере государственного управления и промышленного производства широко применяются информационные системы (ИС), обладающие сложной, зачастую распределенной инфраструктурой. Качество реализации сервисов неразрывно связано с вопросами обеспечения безопасности при использовании системы защиты информации.

Международные и национальные стандарты в области информационной безопасности (ИБ) декларируют необходимость управления рисками, не предлагая какой-либо методологии. Основопологающим этапом управления рисками нарушения ИБ является их оценка; значение уровня риска определяется как функция вероятностей реализации угроз защищенности информации и ее ценности с точки зрения последствий для бизнеса [1-5]. Программные продукты, автоматизирующие процесс оценивания риска, не в полной мере позволяют достоверно оценить уровень риска конкретного объекта защиты. Это связано с определением в них значений вероятностей угроз экспертным путем на основании статистических данных об инцидентах в области ИБ, с отсутствием возможности учесть специфику объекта защиты: особенности топологии сети и технологий обработки информации, сведения об используемых или планируемых средствах защиты информации, оценить эффективность конкретного набора средств. Как следствие, эти программные продукты могут быть использованы только на этапе эксплуатации, а не при проектировании.

На сегодняшний день практически отсутствуют методы, которые можно использовать при проектировании системы защиты информации, адекватность которых не зависит от наличия или отсутствия статистических данных в области инцидентов ИБ, экспертные знания в которых сведены к минимуму или основываются на объективных данных об объекте защиты. Таким образом, разработка методики оценки рисков информационной безопасности, максимально учитывающей обозначенные выше аспекты, является актуальной задачей.

Основные этапы оценки рисков

В соответствии с ГОСТ Р ИСО/МЭК 27005-2010, риск информационной безопасности – это возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесёт ущерб организации [6]. Он измеряется исходя из комбинации вероятности события и его последствия²¹⁷ [7].

Таким образом, риск информационной безопасности необходимо рассматривать как комплексную величину, а деятельность по его оценке – представить в виде алгоритма, учитывающего несколько факторов, представленных на схеме рис. 1.

²¹⁵ Скворцов Михаил Алексеевич, МГТУ им. Н.Э. Баумана г. Москва, SkvortsovM@rambler.ru

²¹⁶ Шахалов Игорь Юрьевич, ЗАО «НПО «Эшелон», Москва, is@cnpo.ru

²¹⁷ ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»

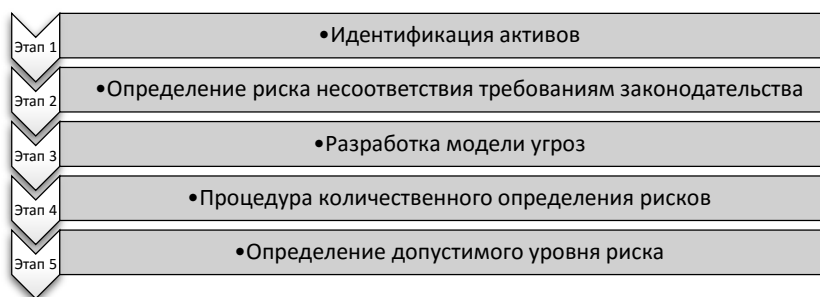


Рис. 1. Основные этапы оценки информационных рисков

Используя математический аппарат проиллюстрируем вычисление риска с помощью формулы (1):

$$Riskvalue = R(A, T, V) = R(L(T, V), F(C_A, V_A)) \quad (1)$$

где: R – функция вычисления риска от переменных

A – активы, T – угрозы, V – уязвимости, L – возможность угрозы привести к инцидентам с помощью уязвимостей, F – потери, вызванные событиями безопасности, V_A – степень уязвимости, C_A – стоимость активов.

Определение значения риска неразрывно связано с результатами оценки риска и выработкой мер по его контролю. В целях предотвращения несанкционированного доступа организации используют различные контрмеры для защиты своих активов, но даже применение контрмер и управление информационной безопасностью не дает абсолютной уверенности в защите активов ввиду недостатка контроля. Поэтому в данной работе к факторам риска отнесены и контрмеры (M) (табл. 1). В целом вероятность наступления неблагоприятного события характеризует сумма факторов $T+V+M$.

Таблица 1

Факторы риска и их составляющие

Факторы риска	Составляющие
Угрозы (T)	Естественные угрозы (T_1)
	Антропогенные угрозы (T_2)
Ущерб (F)	Ущерб конфиденциальности (F_1)
	Ущерб целостности (F_2)
	Ущерб доступности (F_3)
Уязвимости (V)	Технические уязвимости (V_1)
	Уязвимости в управлении (V_2)
Контрмеры (M)	Существующие контрмеры (M_1)
	Необходимые контрмеры (M_2)

Основные элементы системы оценки информационных рисков могут быть представлены в виде схемы на рис. 2. Данный процесс и его этапы аналогичны для любых организаций, независимо от сферы их деятельности, масштабов, уровня организационной зрелости [8]. Однако на практике оценка рисков информационной безопасности является сложным процессом, в котором необходимо учитывать неопределенности и специфику деятельности организации, для которой разрабатывается система управления рисками.

Идентификация активов. Активы системы информационных технологий являются компонентом или частью общей системы, в которую предприятие напрямую вкладывает средства и которые, соответственно, требуют защиты со стороны предприятия. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только аппаратные средства, но и программное обеспечение. Описание информационных активов должно быть наглядным и удобным для анализа.

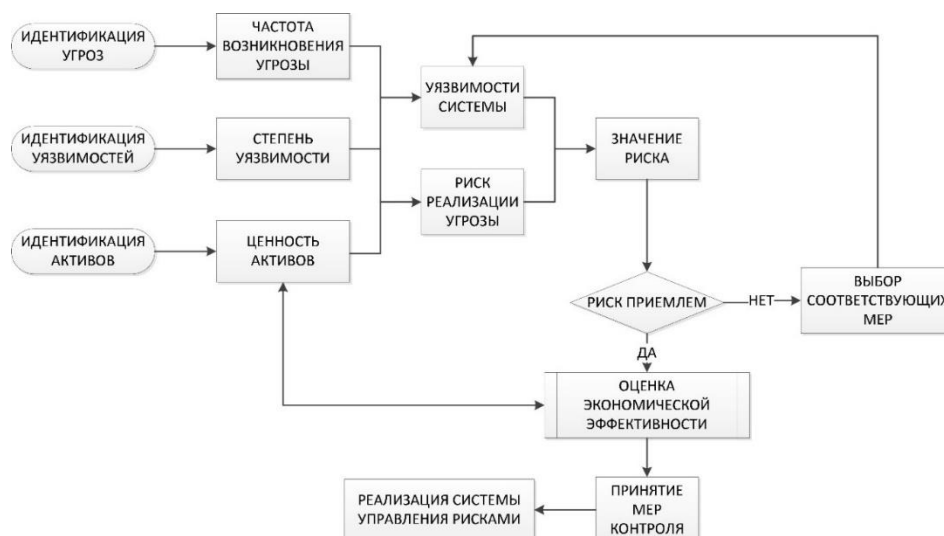


Рис. 2. Основные элементы системы оценки угроз ИБ

Таковыми свойствами обладают функциональные модели, строящиеся с помощью методов структурного анализа в графической форме с содержательным описанием, позволяющим анализировать диаграммы. Например, решения с использованием схем IDEF0 предложены авторами работ [3, 9].

Разработка модели угроз. В методике с целью максимально точного определения риска ИБ необходимо разработать частную модель угроз ИБ предприятия. Определение вероятности наступления неблагоприятных событий определяется экспертным методом. Экспертным методом определяется и актуальность угроз ИБ.

После завершения оценки угроз составляют перечень актуальных идентифицированных угроз на каждый идентифицированный актив или групп активов, подверженных этим угрозам, а также определяют вероятность реализации угроз. Для точного расчета

В зависимости от выбора шкалы измерений можно выделить **два основных направления оценки рисков:** количественная и качественная.

Для достижения приемлемой точности количественный расчет величин рисков требует значительного объема статистических данных о вероятности реализации той или иной угрозы. В результате наибольшее распространение получила качественная оценка информационных рисков. Однако обладая простотой, такая оценка не позволяет выразить вероятности с помощью числовых коэффициентов и имеет приближенный характер.

Свести перечисленные недостатки к минимуму позволяет комбинация количественных и качественных методов – использование шкалы числовых коэффициентов совместно с лингвистическим описанием ее уровней. Комбинированные методы целесообразно применять также и при оценке существующих мер безопасности. Сложность на этом этапе может представлять то, что оценить факторы риска можно только экспертно, а значит, результаты оценки напрямую зависят от опыта выполняющего оценку эксперта. Особенно это касается экономической оценки потенциального ущерба, при оценке значения которого обязательно должен выполняться принцип «разумной достаточности»: затраты на обеспечение ИБ должны быть сопоставимы с величиной потенциального ущерба. При оценке остальных факторов в качестве вспомогательной информации эксперты могут использовать результаты анализа потоков данных в информационной системе и накопленные статистические данные об угрозах, уязвимостях и эффективности существующих мер безопасности. Также существует необходимость обеспечения адекватности и согласованности экспертных мнений. В работе [10] проведён

сравнительный анализ экспертных методов. Для этого предлагается использовать решение задачи линейного программирования симплекс-методом, где вероятности реализации угрозы информационной безопасности (x_1), нанесения наивысшего возможного ущерба (x_2) и использования уязвимости информационной системы (x_3) должны быть в интервале $[0, 1]$ (2):

$$\begin{cases} 0 \leq x_1 \leq 1 \\ 0 \leq x_2 \leq 1 \\ 0 \leq x_3 \leq 1 \end{cases} \quad (2)$$

Итоговая система уравнений выглядит следующим образом (3):

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \leq b_1, \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \leq b_2, \\ \dots \\ a_{n1}x_1 + a_{n2}x_2 + a_{n3}x_3 \leq b_n, \end{cases} \quad (3)$$

$a_{ij} \in [0, 10]$; $b_i \in [0, 30]$; $i \in 1, 2, \dots, n$; $j \in 1, 2, 3$

a_{i1} – экспертные оценки мощности угрозы; a_{i2} – экспертные оценки величины ущерба; a_{i3} – экспертные оценки степени уязвимости; b_i – оценки риска; n – число экспертов. После того, как была проведена оценка принятых мер безопасности, должна быть проведена оценка остаточного уровня риска. Одних статистических данных тут недостаточно. Необходимо математически оценить данные о факторах риска, выявленных ранее. Такими возможностями обладают методы, использующие элементы искусственного интеллекта [11]. При этом наибольшей эффективностью в оценке информационных рисков обладают гибридные модели, учитывающие как числовые значения факторов риска, так и качественные данные, получаемые от экспертов. Например, в работе [12] представлен модуль нечёткого вывода на основе нейронных сетей, а в работе [10] приведён опыт применения нечетких когнитивных карт. Этап оценки риска повторяется до тех пор, пока уровень остаточного риска, сниженного в результате внедрения контрмер, не будет приемлемым.

Выводы

Выполнен сравнительный анализ существующих методов оценки рисков. Для того чтобы решить проблему оценки рисков информационной безопасности целесообразно применять не один универсальный метод, основанный только на количественной или качественной их оценке, а комбинировать методы и средства на разных этапах процесса управления рисками.

Литература

1. Басараб М.А., Бельфер Р.А., Соцкий В.В. Расчет риска безопасности атак DOS сборных сенсорных узлов на базе метода Fuzzy-АНР для определения архитектуры взаимодействия между наземными сенсорными сетями и Fanet в летающей сенсорной сети // Вопросы кибербезопасности. 2015. № 5 (13). С. 16-22.
2. Бельфер Р.А., Калюжный Д.А., Тарасова Д.В. Анализ зависимости уровня риска информационной безопасности сетей связи от экспертных данных при расчетах с использованием модели нечетких множеств // Вопросы кибербезопасности. 2014. № 2 (3). С. 33-39.
3. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде Matlab // Вопросы кибербезопасности. 2015. № 4 (12). С. 53-61.
4. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. № 2 (3). С. 66-73.
5. Калашников А.О. Управление информационными рисками объектов критической информационной инфраструктуры российской федерации // Вопросы кибербезопасности. 2014. № 3 (4). С. 35-41.
6. Марков А.С., Цирлов В.Л. Управление рисками - нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. №8. С. 63-67.

7. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. Под. ред. А.С.Маркова. - М.: Радио и связь, 2012. 192 с.
8. Fu S, Xiao Y. (2012), «Strengthening the research for Information security risk assessment». International Conference on Biological and Biomedical Science Advanced in Biomedical Engineering, Vol.9; pp.386-392.
9. Анализ информационных рисков виртуальных инфраструктур здравоохранения / Т. И. Булдакова, С. И. Суятинов, Д. А. Миков // Информационное общество. 2013. №4. С. 6.
10. Степанова Е.С. Модели и методы оценки рисков информационной безопасности с использованием нечетких когнитивных карт // Автореферат дисс. на соискание уч. степени канд. техн. наук. Уфа, 2013.
11. Information Security Risk Analysis Methods and Research Trends: ANP and Fuzzy Comprehensive Method / MingChang Lee // International Journal of Computer Science & Information Technology (IJCSIT). 2014. Vol 6. No1. Pp. 29-45.
12. Атаманов А. Н. Модуль нечеткого вывода на основе нейронных сетей для динамического итеративного анализа рисков информационной безопасности // Безопасность информационных технологий. 2011. № 1. С. 7.

Рецензент: Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, v.tsirlov@bmstu.ru

A Survey of Information Security Risks Assessment Tools and Methods

Skvortsov M.A.²¹⁸, Shakhlov I.Yu.²¹⁹

A survey presents the process of information security risk assessment, its methods and tools. An overview of the most common and actual methods is given in detail. Their highs and lows, as well as most perspective ways of further evolution are discussed.

Keywords: *information security, threat, damage, vulnerability, countermeasure, information security risk assessment, AI, expert assessments, fuzzy sets, neural networks, learning vector, soft-computing, hybrid models.*

²¹⁸ Skvortsov Mikhail, Bauman Moscow State Technical University, Moscow
e-mail: SkvortsovM@rambler.ru

²¹⁹ Shakhlov Igor, NPO Echelon, is@cnpo.ru

Опыт использования технологий нейронных сетей для обнаружения низкоинтенсивных DDoS-атак

Тарасов Я.В.²²⁰

Представлен прототип системы обнаружения атак, методика формирования обучающей выборки, механизм обучения, ход экспериментов и топология экспериментального стенда. Показаны результаты эксперимента.

Ключевые слова: обнаружение атак, гибридная нейронная сеть

Введение

С развитием возможностей вычислительной базы использование аппарата искусственных нейронных сетей в области информационной безопасности приобретает широкий характер [1-6]. Что касается кибербезопасности, то в первую очередь интересны изыскания, касающиеся выявления сложных атак.

В работе [7, 8] представлены модели низкоинтенсивных DDoS-атак. В данной работе показаны результаты эксперимента по выявлению LR DOS-атак.

Моделирование на основе аппарата нейронных сетей.

Основное преимущество систем обнаружения атак (СОА), использующих нейронные сети, в том, что нейросеть не ограничена знаниями, которые заложил в неё разработчик. Они имеют возможность учиться на предшествующих событиях - как на аномальном, так и на нормальном трафике. За счёт этого достигается высокая эффективность и адаптивность СОА.

Существуют различные варианты применения нейросетевых систем обнаружения атак (НСОА) - анализ всего сетевого трафика в защищаемом сегменте сети, анализ команд, вводимых пользователем, анализ переходов состояний и др. В настоящей статье предлагается метод обнаружения и архитектура СОА, основанная на использовании гибридной нейронной сети в качестве анализатора трафика.

В работе [9] показана возможность использования многослойного персептрона в качестве решающего блока в СОА, анализирующей последовательно приходящие сетевые пакеты. Предлагаемый в статье подход предполагает использование нейросети для выявления злоупотреблений, распределённых во времени и основанных на совместном создании искусственного (аномального) потока данных несколькими источниками.

Идея метода состоит в разделении и последовательном анализе отдельных частей непрерывного потока данных. Поток разделяется на наборы по 150 пакетов, причём кроме данных из заголовков пакетов сетевого и транспортного уровней, как предлагается в работе [9], учитываются также и первые 50 символов полезной нагрузки прикладного уровня (в ASCII-коде). Кроме этого, проводится нормализация представления значений порта назначения для уточнения используемого прикладного протокола (http, ftp и т.д.). Схожий метод анализа исходных данных был описан в [10].

Как правило, ни одно событие, составляющее трафик DoS-атаки, по отдельности не выглядит подозрительно. Кроме того, даже два или три события не являются чем-то необычным. Тем не менее, взятые вместе, в определенной последовательности, повторяемые в определённое время, эти события являются указанием на то, что осуществляется атака. Дальнейшее осложнение обнаружения состоит в том, что эти

²²⁰ Тарасов Ярослав Викторович, ЗАО «Инфосистемы Джет», г. Москва, info@jet.msk.su

события, хотя и в определенной последовательности, могут поступать из различных источников и чередоваться с другими, нормальными событиями.

Для обработки аномального трафика предлагается применять гибридную нейронную сеть, состоящую из самоорганизующейся сети Коханена (self-organizing map, SOM) и многослойного персептрона. Архитектура прототипа предлагаемой системы обнаружения атак представлена на рисунке 1.

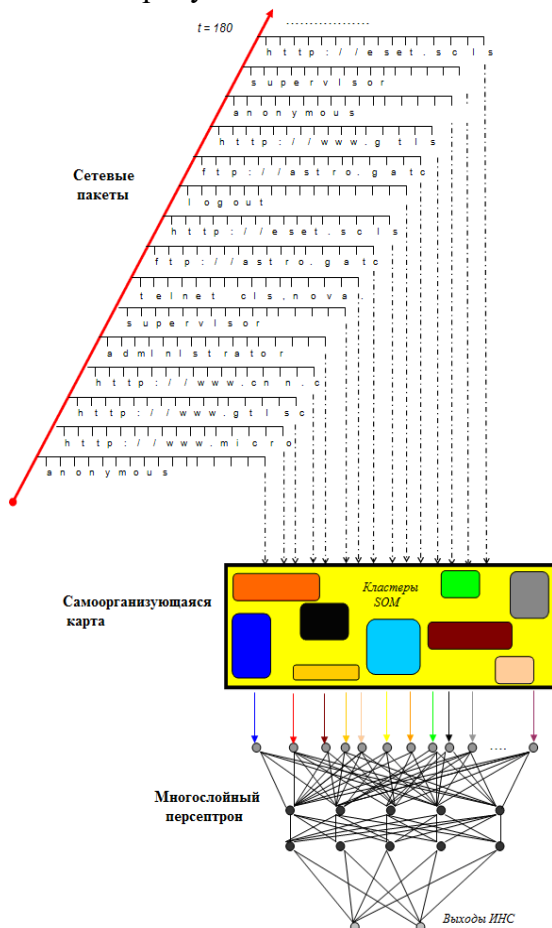


Рисунок 1 – Архитектура предлагаемой системы обнаружения атак

SOM используется для выделения групп (наборов) событий, а персептрон - собственно для классификации нормальных или аномальных наборов.

При помощи применения карты Коханена происходит кластеризация 50-символьных событий в узлы матрицы, в которых будут сгруппированы события аналогичных числовых символов. Фактически, отдельные узлы будут представлять собой определённые сценарии атак.

Входной вектор для SOM содержит следующие компоненты:

- 1-4 - байты, составляющие адрес пакета (для протокола IPv4), приведённые в диапазон 0-1;
- 5 - порт пакета, приведённый в диапазон 0-1;
- 6-55 - первые 50 байтов данных пакета, приведённые в диапазон 0-1.

После этого данные заголовков пакетов и информация о группировке подаются на вход многослойного персептрона, обученного распознавать аномальный трафик, но уже с учётом информации о событии, т.е. принадлежности пакета той или иной группе-сценарию. Это позволяет не только обнаруживать аномалии в единичных пакетах, но и выявлять принадлежность пакета к распределённой по времени атаке.

Входная выборка для персептрона разбивается на непересекающиеся части длиной 150 пакетов. Все пакеты проходят через сеть Кохонена. Пакету ставится в соответствие номер кластера (номер нейрона-победителя).

Кластеры укрупняются - 5 соседних объединяются воедино. Получается 100 укрупнённых кластеров.

По укрупнённым кластерам считается гистограмма для представления трафика. Т.е., первый компонент вектора входного вектора для FF-сети - это число пакетов, попавших в первый укрупнённый кластер (кластеры 1-5), и так далее. Гистограмма нормируется, компоненты приводятся к диапазону 0-1. После этого вычисляется дельта между соседними векторами.

В предлагаемом методе учитывается два типа активности трафика. При анализе отдельных узлов кластера выявляются отдельные сценарии атак. Кроме того, анализируются резкие перепады мощности сетевого потока для выявления всплесков нагрузки. Совместный анализ этих двух типов событий позволяет более точно реагировать на появление DoS-трафика, при этом снижая число ложных срабатываний, связанных с легальным возрастанием использования полосы пропускания.

Для обучения искусственной нейронной сети моделировались два типа сетевого трафика – нормальный и аномальный. Первый содержал пакеты, появляющиеся в сети при обычной работе, а второй имитировал распределённую атаку.

Перед обучением сохранённые пакеты классифицируются экспертом как нормальные или атакующие. Затем на первом этапе обучения сеть Кохонена обучается без учителя для кластеризации данных, на втором этапе обучения многослойный персептрон обучается с учителем методом Левенберга-Маркуорта для классификации наборов пакетов на нормальные и атакующие. Входными данными для сети Кохонена служат сетевые пакеты, представленные следующим образом – один входной вектор соответствует одному сетевому пакету, первый компонент вектора – номер порта, остальные 50 компонент – первые 50 байтов данных пакета. Компоненты вектора нормированы в диапазоне [0,1]. Входными данными для персептрона являются результаты распознавания группы из 150 пакетов сетью Кохонена. Каждый компонент вектора соответствует кластеру сети Кохонена, а его значение – число пакетов, принадлежащих данному кластеру. Компоненты вектора также нормированы в диапазоне [0,1]. Выходной вектор имеет вид $\langle u_n, u_a \rangle$, где u_n – близость к нормальному поведению, u_a – близость к атакующему поведению.

Обучение и тестирование ИНС проводилось на непересекающихся окнах, поскольку при использовании скользящих окон при тестировании ухудшается возможность контроля за степенью использования полосы пропускания сетевого канала.

ИНС, используемые для построения указанных классификаторов, являются большими и сверхбольшими, то есть имеют несколько слоев и множество нейронов в каждом из них [11].

Результаты обучения такой сети с применением известных градиентных методов поиска точки экстремума, как правило, показывает неудовлетворительные временные значения. Минимизация времени обучения возможна за счет модификации алгоритма обучения.

Имитация отжига (ИО) является одной из наиболее известных и широко применяемых для решения подобных задач метаэвристических методов поиска. Если, однако, рассматривать ИО в аспекте ее использования в системах реального времени, то следует отметить, что основным недостатком ИО считается ее медленная сходимость к глобальному минимуму [12] в связи с чем к настоящему моменту времени разработаны и используются методы улучшения как скоростных характеристик ИО (например, различные

температурные схемы «тушения»), так и методы улучшения результата на ограниченном количестве итераций (достигается за счет распараллеливания ИО) [13].

Выводы

Анализ механизма реализации Low-rate DDoS-атак на примере атаки slowloris показал, что этот тип атак может быть организован с минимальным соотношением необходимой мощности/канала атакующего компьютера (компьютеров) и атакуемого сервера, недостижимым раньше. Со стороны сервера зачастую сложно выявить атаку, поскольку трафик не превышает нормальных значений.

После проведения экспериментов стало ясно, что для успешной атаки такого рода требуется хорошо скоординированный сценарий атаки и ошибки конфигурирования на целевой системе.

Предлагаемый метод обнаружения низкоинтенсивных атак позволяет эффективно выявлять принадлежность трафика к распределённой по времени и источникам атаке.

В результате тестирования прототипа системы обнаружения атак были получены следующие результаты:

- величина ошибки первого рода (ложное срабатывание) составила 3,16%;
- величина ошибки второго рода (пропуск атаки) составила 1,23%.

Литература

1. Басараб М.А., Вельц С.В. Иерархическое представление компьютерной сети на основе нейронной сети Хопфилда // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2013. № 9. С. 335-348.
2. Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2013. № 11. С. 295-310.
3. Качайкин Е.И., Иванов А.И. Идентификация авторства рукописных образов с использованием нейросетевого эмулятора квадратичных форм высокой размерности // Вопросы кибербезопасности. 2015. № 4 (12). С. 42-47.
4. Качайкин Е.И., Иванов А.И., Безяев А.В., Перфилов К.А. Оценка достоверности нейросетевой автоматизированной экспертизы авторства рукописного почерка // Вопросы кибербезопасности. 2015. № 2 (10). С. 43-48.
5. Марков Г.А. Эксперимент по использованию нейросетевых технологий для проведения испытаний открытого программного обеспечения // Вопросы кибербезопасности. 2013. № 2. С. 47-52. 0
6. Рыжков А.П., Катков О.Н., Морозов С.В. Нейросетевые технологии при решении задач разграничения доступа // Вопросы кибербезопасности. 2016. № 3 (16). С. 69-76.
7. Тарасов Я.В. Метод обнаружения низкоинтенсивных DDoS-атак на основе гибридной нейронной сети // Известия ЮФУ. Технические науки. – 2014. - № 8. – С. 47-58.
8. Тарасов Я.В., Макаревич О.Б. Моделирование и исследование низкоинтенсивных dos-атак на bgr-инфраструктуру // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 101-111.
9. James Cannady, The Application of Artificial Neural Networks to Misuse Detection. 2001.
10. Абрамов Е.С., Сидоров И.Д. Метод обнаружения распределенных информационных воздействий на основе гибридной нейронной сети // Изв. ЮФУ. Технические науки. – 2009. - № 11. – С. 154-164.
11. Осовский С. Нейронные сети для обработки информации / Пер. с польского И.Д. Рудинского. М.: Финансы и статистика, 2002. 44 с.
12. Тихомиров А.С. О быстрых вариантах алгоритма отжига. (<http://www.math.spbu.ru/user/gran/soi5/Tikhomirov5.pdf>).
13. Лопатин А. С. Метод отжига // Стохастическая оптимизация в информатике. СПб.:Изд-во СПбГУ, 2005. Вып. 1. С. 133–149.

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

Using Artificial Neural Networks to Detect Low-Intensity DDoS-Attacks Tarasov Y.²²¹

The prototype intrusion detection systems, methods of forming training sample, training mechanism, the course of experiments and experimental stand topology is presented. The results of the experiment are Shown.

Keywords: intrusion detection, hybrid neural network

УДК 004.056

Исследование алгоритма дешифрования полностью гомоморфных шифров Султанов Д.Р.²²²

Обоснована невозможность использования алгоритма дешифрования, предложенного А. Малинским в 2013 году, на любой полностью гомоморфной криптосистеме. Рассмотрены существующие алгоритмы гомоморфного шифрования. Разработана программа дешифрования методом А. Малинского. Результаты исследования опровергают возможность дешифрования полностью гомоморфной криптосистемы за полиномиальное время. В области криптографии данное исследование опровергает способ дешифровки криптографически преобразованного текста за полиномиальное время.

Ключевые слова: криптография, гомоморфное шифрование, дешифровка, оценка алгоритма.

Введение

В 2009 году в мире криптографии был сделан первый шаг в сторону создания практически применимой полностью гомоморфной криптосистемы. В кандидатской диссертации Крейга Джентри [1] была предложена первая гомоморфная криптосистема, поддерживающая неограниченное количество операций сложения и умножения над зашифрованными данными.

Вслед за публикацией диссертации Крейга последовало множество публикаций, улучшающих схему [2]. Несмотря на растущий интерес в данной области криптографии, на текущий момент не было предложено эффективной системы полностью гомоморфного шифрования (ПГШ). Некоторые системы ПГШ рассмотрены в статье [3-6].

Ученые изучали не только достоинства данного вида шифрования, но и недостатки, анализировали криптостойкость, искали уязвимости к разного рода атакам [7-8]. До 2013 года не существовало алгоритма, доказывающего слабую криптостойкость полностью гомоморфных шифров.

В 2013 году студентом МГТУ им. Баумана в научной статье [9] был предложен метод дешифрования любого полностью гомоморфного шифра без знания ключа в лучшем случае за полиномиальное время. Если данный метод даст возможность быстрой дешифровки сообщений, то про алгоритмы полностью гомоморфного шифрования можно забыть, и использовать только ограниченные схемы гомоморфного шифрования.

Определение полностью и ограничено гомоморфных криптосистем

В статье Малинского А.Е. «Оценка криптостойкости полностью гомоморфных систем» дается определение.

Пусть $\lambda(x_1, x_2, \dots, x_i)$ — произвольная функция от i переменных, где $x_i \in X$, $\lambda(x_1, x_2, \dots, x_i) \in X$. Тогда полностью гомоморфное шифрование (ПГШ) — это пара отображений

²²¹ Tarasov Yaroslav, Jet Infosystems Moscow, Russia, info@jet.msk.su

²²² Султанов Денис Радикович, МГТУ им. Н.Э. Баумана, г. Москва, sultanov-57@mail.ru

$$f : X \xrightarrow{f} Y, \quad y = f(x) \quad (1)$$

$$f^{-1} : Y \xrightarrow{f^{-1}} X, \quad x = f^{-1}(y), \quad (2)$$

таких что $\forall \lambda(x_1, x_2, \dots, x_i)$, выполняются следующие условия:

$$f^{-1}(f(\lambda(x_1, x_2, \dots, x_i))) \equiv \lambda(x_1, x_2, \dots, x_i) \quad (3)$$

$$\exists \lambda_f(y_1, y_2, \dots, y_i) : \lambda(x_1, x_2, \dots, x_i) \equiv f^{-1}(\lambda_f(y_1, y_2, \dots, y_i)) \quad (4)$$

Уравнение (3) гарантирует, что при шифровании значения произвольной функции и последующем расшифровании результат останется неизменным. Уравнение (4) позволяет отображать произвольную операцию над множеством X в операцию над множеством Y .

Частично гомоморфным шифрованием, в данном случае, называется шифрование, где функция $\lambda(x_1, x_2, \dots, x_i)$ не является произвольной, а набор функций, которые можно осуществлять над зашифрованными данными, не должен позволять выразить произвольную функцию. В этом случае, частично (ограниченно) гомоморфная система может быть построена под конкретную задачу, а общий подход, описанный Малинским, к атаке на данную систему становится невозможен.

В диссертации Крейга Джентри [1], а также в ряде научных статей [10,13] дается иное определение ПГШ.

Полностью гомоморфным шифрованием называют функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо операций над открытыми текстами. В отличие от частично (ограниченно) гомоморфного шифрования, которое позволяет производить гомоморфные вычисления относительно лишь одной операции открытого текста, полностью гомоморфное шифрование обеспечивает гомоморфизм обеих операций (как сложения, так и умножения) [10].

Существующие полностью гомоморфные криптографические системы

На данный момент существует множество разработанных схем полностью гомоморфного шифрования, некоторые из них приведены ниже.

1. Крейг Джентри (2009 г., на основе идеальных решеток);
2. М. ван Дейк, К. Джентри, Ш. Халеви, В. Вайкунтанатан (2010 г., на основе колец вычетов);
3. З. Бракерски, В. Вайкунтанатан (2011 г., на основе задачи LWE в решетках);
4. З. Бракерски, К. Джентри, В. Вайкунтанатан (2011 г., BGV);
5. К. Джентри, С. Хелави, Н. Смарт (2011 г., GHS - модификация BGV);
6. А. Ростовцев, А. Богданов (2011 г., полиномиальные схемы);
7. К. Джентри, А. Сахоу, Б. Вотерс (2013 г., матричные схемы на основе LWE);
8. С. Кренделев, А. Жиров (2013 г., полиномиальные схемы в классах вычетов);
9. Ф. Буртыка, О. Макаревич (2014 г., матричные полиномы);

Анализ возможности применения алгоритма дешифрования А.Е. Малинского

Согласно определению в статье Малинского и описанию алгоритма, данная атака может сработать только на криптосистему гомоморфную относительно полной системы булевых функций.

В настоящее время нет ни одной криптографической системы, обладающей возможностью производить любую алгебраическую операцию над зашифрованными данными. Все схемы, приведенные в прошлом пункте, могут выполнять над зашифрованными данными лишь операции сложения и умножения.

В случае если подходящая система будет разработана, то алгоритм дешифрования Малинского к данному шифру применить будет возможно. Но возникает сложность использования алгоритма, основанная на особенностях всех существующих схем ПГШ. Сложность заключается в том, что размер шифртекста возрастает при умножении его на

другой шифртекст. Согласно алгоритму в этом случае скорость дешифровки будет экспоненциальной относительно константы k , $O(n \cdot 2^k)$, где k – количество перехваченных шифртекстов.

Автор не оценил k , несмотря на то, что от её величины зависит возможность реализации данной атаки до момента, пока данные не потеряют актуальность.

Описанная константа определяет количество возможных прообразов каждого образа и её минимальное значение можно свести к разнице в длине вектора открытого текста и длине вектора шифртекста. То есть, если шифртекст длиннее открытого текста на 256 бит, то алгоритм дешифрования на достаточно производительном ЭВМ, способном осуществлять $\sim 10^9$ операций в секунду, будет работать более 10^{60} лет.

Реализация схемы дешифрования, предложенной А.Е. Малинским

Написанная на C++ программа, реализует дешифрование по известному шифртексту, опираясь на формулы в анализируемой статье. Текст программы включен в приложение к статье.

```
Input length vector open text 5
Input binary vector open text 10100

The values of the function at points 2^i
f<2^0> = 00001
f<2^1> = 00010
f<2^2> = 00100
f<2^3> = 01000
f<2^4> = 10000

Decrypted open text: 10100
Для продолжения нажмите любую клавишу . . .
```

Рис 1. Результат работы программы для шифртекста (10100)

Создание таблицы шифрования с помощью алгоритма А.Е. Малинского

Опираясь на результаты работы программы составлена таблица (табл.1) соответствия векторов открытых текстов векторам шифртекстов для длины вектора равной 3.

Таблица 1.

Соответствие векторов открытых текстов и шифртекстов

№ п/п	Шифртекст	Открытый (дешифрованный) текст
1	000	000
2	001	001
3	010	010
4	011	011
5	100	100
6	101	101
7	110	110
8	111	111

После анализа формул в статье Малинского был сделан вывод, что им предложена примитивная полностью гомоморфная система, соответствующая функции $ENC(x) = x$, где ENC – функция шифрования.

Данная функция соответствует требуемым характеристикам гомоморфности, но не является криптографической.

Выводы

Обоснованная в статье невозможность дешифровки данных с использованием алгоритма Малинского подтверждается на практике. Алгоритм ПГШ Крейга Джентри, обладающий возможностью совершать операции сложения и умножения над зашифрованными данными, не обладает нужными характеристиками для дешифрования его с помощью предложенного алгоритма.

Это было подтверждено как теоретически в статье, так и на практике. С помощью ЭВМ и языка программирования C++ была написана программа, реализующая схему дешифрования. В результате была получена примитивная функция.

Хотя алгоритм дешифрования и не применим для всех схем ПГШ, но проблемы у данного вида шифров остаются. [5-6] Сам Крейг Джентри отмечает главную проблему гомоморфного шифрования – производительность. По его словам производительность одного поискового запроса в Google с зашифрованным словом потребует увеличения времени вычислений в триллион раз.

Сложности реализации гомоморфного шифрования стоят всех потраченных усилий, так как появляется возможность изменить представления о защите данных внутри облачных инфраструктур [10-13], разработать идеальный программный обфускатор [10], произвести полностью анонимную систему голосования.

Литература

1. Gentry, C. *A fully homomorphic encryption scheme* / C. Gentry. – Stanford University, Ph.D. thesis, 2009. URL: <https://crypto.stanford.edu/craig/craig-thesis.pdf>.
2. Smart, N.P., Vercauteren, F. *Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes*. In: Ngyuen, P.Q., Pointchevar, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 420-443. Springer, Heidelberg (2010). URL: <http://www.cs.au.dk/~stm/local-cache/smarthomo.pdf>.
3. Stehlé D., Steinfeld R. *Faster fully homomorphic encryption* // Advances in Cryptology ASIACRYPT 2010. – Springer Berlin Heidelberg, 2010. – P. 377-394. URL: <http://perso.ens-lyon.fr/damien.stehle/downloads/FFHE.pdf>.
4. Буртыка Ф. Б. Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов // Труды Института системного программирования РАН. 2014. Т. 26. № 5. С. 99–116. DOI: 10.15514/ISPRAS-2014-26(5)-5.
5. Варновский Н. П., Шокуров А. В. Гомоморфное шифрование // Труды Института системного программирования РАН. 2007. № 12. С. 27–36. URL: http://www.ispras.ru/proceedings/docs/2007/12/isp_12_2007_27.pdf.
6. Шокуров А.В., Сергеев К. В. Об одном методе построения схемы полного гомоморфного шифрования // Труды Института системного программирования РАН. 2012. Т. 23. URL: http://www.ispras.ru/proceedings/docs/2012/23/isp_23_2012_427.pdf.
7. Трепачева, А.В. Дерандомизационная криптостойкость гомоморфного шифрования // Труды Института системного программирования РАН, 2015 - №6 (27), выпуск 6. - С. 381-394. DOI: 10.15514/ISPRAS-2015-27(6)-24.
8. Трепачева А.В. Криптоанализ симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел // Известия ЮФУ. Технические науки. 2015. № 5 (166). С. 89–102, URL: <http://izv-tn.tti.sfedu.ru/wp-content/uploads/2015/5/9.pdf>.
9. Малинский А.Е. Оценка криптостойкости полностью гомоморфных систем. // *Инженерный журнал: наука и инновации*, 2013, вып. 11. URL: <http://engjournal.ru/articles/995/995.pdf>.
10. Бабенко Л. К., Буртыка Ф. Б., Макаревич О. Б., Трепачева А. В. Методы полностью гомоморфного шифрования на основе матричных полиномов // Вопросы кибербезопасности. 2015. № 1 (9). С. 14–25.
11. Варновский Н. П., Мартишин С. А., Храпченко М. В., Шокуров А. В. Пороговые системы гомоморфного шифрования и защита информации в облачных вычислениях // Программирование. 2015. № 4. С. 47–51. URL: http://www.ispras.ru/proceedings/docs/2014/26/2/isp_26_2014_2_269.pdf.
12. Червяков Н. И., Кучеров Н. Н. Исследование методов обеспечения конфиденциальности вычислений в облачной среде на основе китайской теоремы об остатках // Сборник научных трудов ВНИИ ОиК. 2015. Т. 1. № 8. С. 633–635.
13. Жиров А.О., Жирова А.О., Кренделев С.Ф. Безопасные облачные вычисления с помощью гомоморфной криптографии // Безопасность информационных технологий. 2013. №. 1. С. 6-12. URL: http://bit.mephi.ru/wp-content/uploads/2013/2013_1/part_1.pdf.

Научный руководитель: Лебедев Анатолий Николаевич, доцент, кандидат физико-математических наук, МГТУ им Н.Э. Баумана, lan@lancrypto.com.

Research of Algorithms Decryption Fully Homomorphic Ciphers **Sultanov D.R.²²³**

The impossibility of using the decryption algorithm on any fully homomorphic cryptosystem proposed by A. Malinskiy in 2013 is substantiated. The existing homomorphic encryption algorithms are considered. The decryption program by A. Malinskiy is developed. The results of the research disprove the possibility of decrypting fully homomorphic cryptosystem in polynomial time. In the field of cryptography, the study refutes the way to decrypt the cryptographically transformed text in polynomial time.

Keywords: cryptography, homomorphic encryption, decryption, algorithm evaluation.

²²³ Denis Sultanov, Bauman Moscow State Technical University, Moscow, sultanov-57@mail.ru

Анализ защищенности биометрических иммобилайзеров Соколов М.Н.²²⁴

Доклад посвящен проблеме недостаточной защищенности современных биометрических иммобилайзеров, и, как следствие, роста количества угонов. Проанализирована статистика угонов автомобилей в России и во всем мире за определенные периоды времени. Приведена краткая характеристика существующих противоугонных систем. Рассмотрены современные методы биометрической аутентификации и предложено применение сканера вен руки для разработки иммобилайзера.

Ключевые слова: противоугонная система, транспортное средство, биометрическая аутентификация.

Введение

В настоящее время автомобильная промышленность развивается очень быстро. Вместе с этим также растет количество злоумышленников, которые угоняют автомобили. Чем больше электроники используется в транспортных средствах, тем изощренней становятся пути взлома и, следовательно, методы защиты.

Существующие средства защиты в основном связаны с отпугиванием, отслеживанием и привлечением внимания, а средства блокировки автомобиля обходятся путем прописывания поддельных ключей в центральный блок управления. Таким образом, необходимы дополнительные средства защиты для предотвращения угонов.

Статистика угонов автомобилей в России и в мире

Общая статистика угонов легковых транспортных средств за 2015 год [3] на всей территории России составила 36323 автомобиля (рис.1). Это немногим меньше, чем в 2014 году (39253 машин). Проанализировав статистику по маркам угоняемых автомобилей (рис. 2), можно сделать вывод, что почти треть угонов приходится на отечественный автопром.



Рис.1. – Общая статистика угонов автомобилей в России

²²⁴ Соколов М.Н., МГТУ им. Н.Э. Баумана, Москва, mike.sv@mail.ru

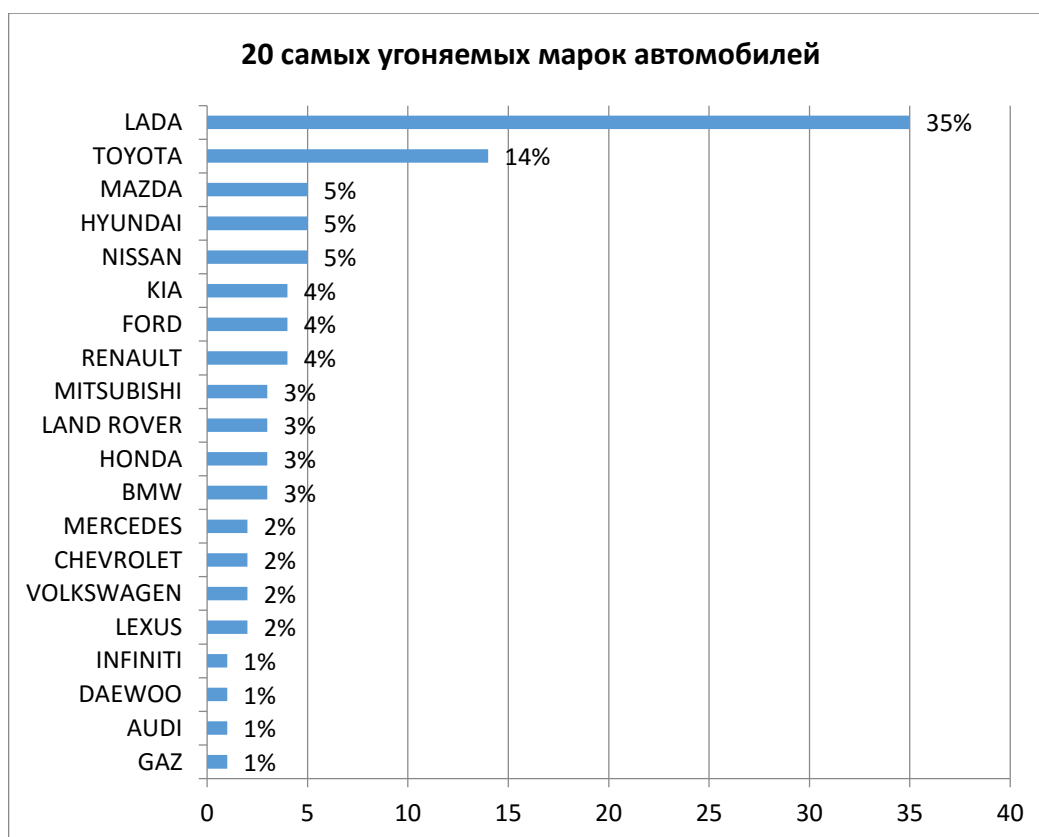


Рис.2. – Статистика угонов по маркам угоняемых автомобилей

Таким образом, отмечается значительное увеличение удельного числа угонов на всей территории России, то есть количество угнанных машин относительно проданных. Рост угонов относительно рынка вызван увеличением стоимости запасных частей, в связи с резким ростом курса доллара. В следствии этого происходит увеличение числа угонов автомобилей "под разбор".

Статистика угонов автомобилей по всему миру представлена на рис.3. Диаграмма показывает, что в 2015 году было осуществлено самое большое количество угонов (7.411.706) за последние девять лет. Это число значительно превышает количество угонов в 2014 году (6.892.161).



Рис.3. – Общая статистика угонов автомобилей в мире

Приведенная статистика показывает, что существующие средства защиты автомобилей не обеспечивают должной безопасности. Следовательно, нужно искать новые пути решения этой проблемы.

Анализ биометрических методов аутентификации

Наиболее часто встречающиеся методы биометрической аутентификации приведены

в таблице 1.

Таблица 1

Сравнительная характеристика основных методов биометрической аутентификации [5]

Метод аутентификации	Уровень защиты	Цена	Скрытность характеристики	Размер устройства
Метод распознавания по венам пальца руки	Высокий	Средняя	Очень скрытая	От небольшого до среднего
Метод распознавания по венам кисти руки	Высокий	Средняя	Очень скрытая	Средний
Метод распознавания по отпечатку пальца	Средний	Низкая	Не скрытая	Небольшой
Метод распознавания по контуру, расположению и форме глаз и носа	Низкий	Средняя	Не скрытая	От среднего до большого
Метод распознавания по радужной оболочке	Высокий	От средней до высокой	Средне скрытая	Большой

Анализ существующих противоугонных систем и предложения по устранению недостатков

В настоящее время на рынке противоугонных средств существует большое количество различных устройств, предназначенных для защиты автомобилей. Помимо стандартных сигнализаций и иммобилайзеров, использующих пароли и метки, появляются системы с биометрическими методами аутентификации [2]. Но увеличение числа угонов с каждым годом свидетельствует о том, что существующие противоугонные системы не обеспечивают должной защиты транспортных средств.

Современные биометрические иммобилайзеры [4], например WooDoo WD-800W, распознают владельца автомобиля по отпечатку пальца. Данный метод аутентификации имеет среднюю эффективность и, следовательно, не может гарантировать высокую степень защиты транспортного средства. Он имеет ряд недостатков:

1. Папиллярный узор отпечатка пальца очень легко повреждается мелкими царапинами, порезами.
2. Недостаточная защищённость от подделки изображения отпечатка.
3. Для людей с «неподходящими» пальцами (особенности температуры тела, влажности) вероятность отказа в доступе может достигать 100%.

Защита от угона в такой системе реализована посредством использования дистанционно управляемого реле блокировки Wait Up.

Wait Up – противоугонная технология, обеспечивающая блокировку двигателя в момент начала несанкционированного движения автомобиля. На неподвижном автомобиле, оснащённом данным реле, все электрические цепи замкнуты. Блокирующее реле разомкнет электрическую цепь только тогда, когда угоняемая машина тронется с места. Как только она остановится, имитируя неисправность, контакты вновь замкнутся, и отыскать блокировку будет гораздо сложнее даже при помощи специального диагностического оборудования.

Сигналом для срабатывания иммобилайзера служит перемещение автомобиля в пространстве. Датчик движения находится непосредственно в корпусе противоугонного устройства. Благодаря этому, решение о блокировке Wait Up принимает самостоятельно, без участия центрального блока противоугонной системы.

Более эффективным методом будет являться использование биометрического иммобилайзера на основе сканера вен кисти руки [1,3]. Данный метод аутентификации является новой технологией в сфере биометрии. Инфракрасная камера делает снимки

внешней или внутренней стороны руки. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК излучение. В результате, степень отражения уменьшается, и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку. Не требуется контакта человека со сканирующим устройством.

Технология сравнима по надёжности с распознаванием по радужной оболочке глаза, в чём-то превосходя её, а в чём-то уступая.

Преимущества метода:

1. Отсутствие необходимости контактировать со сканирующим устройством.
2. Высокая достоверность — статистические показатели метода сравнимы с показателями радужной оболочки.
3. Скрытость характеристики.

Недостатком метода является недопустимость засветки сканера солнечными лучами и лучами галогенных ламп.

Учитывая специфику применения сканера, а также все преимущества, недостатками можно пренебречь.

Выводы

В докладе приведена сравнительная характеристика биометрических методов аутентификации, рассмотрены современные противоугонные средства и применение в них данных методов. На основании этого сделаны выводы о недостаточной эффективности существующих средств защиты и предложено использование в иммобилайзерах сканеров вен кисти руки.

Литература

1. Глинская Е.В., Биометрическая технология васкулярной идентификации личности. / Е.В. Глинская // Инженерный вестник. – 2013. – №5. – С. 5
2. Татарченко Н. В., Тимошенко С. В. Биометрическая идентификация в интегрированных системах безопасности // Специальная техника. № 2, 2012.
3. Кузнецов В.А., Автомобильные иммобилайзеры - инновационный подход к проектированию / В.А. Кузнецов // Журнал научных публикаций аспирантов и докторантов. – 2010. – №6 (48). – С. 143-145
4. Кяриямов Р.В., Анализ информационной безопасности иммобилайзеров / Р.В. Кяриямов, Н.В. Царев // Молодой ученый. – 2016. – №5 (109). – С. 45-48
5. Богословская Е.С., Биометрические системы и средства защиты информации / Е.С. Богословская // Сборник студенческих научных работ. – 2015. – №5 (45). – С. 299-303

Научный руководитель: Родионов Дмитрий Евгеньевич, кандидат технических наук, доцент, МГТУ им. Н.Э. Баумана, derodionov@yandex.ru

Biometric Immobilizers Security Analysis

Sokolov M.N.²²⁵

This article is focused on the problem of lack security in modern biometric immobilizers and as a result the growth of the car thefts. The theft statistics in Russia and around the world is analyzed. A brief description of the existing anti-theft systems is shown. Modern methods of biometric authentication is considered and using palm vein scanner for immobilizer development is offered.

Keywords: anti-theft system, vehicle, biometric authentication

²²⁵ Sokolov M.N., Bauman Moscow State University, Moscow, mike.sv@mail.ru

Анализ процесса оценки защищенности веб-приложений

Фокин М.С.²²⁶

В ходе изучения и сравнения приказов № 17, 21 и 31 ФСТЭК России и Стандарта Подтверждения Безопасности Приложений OWASP (ASVS) было предложено применение ASVS в качестве основы для составления программы и методик подтверждения безопасности веб-приложений. Также была обоснована актуальность проблемы отсутствия программы и методик по тестированию веб-приложений. Было установлено, что создание программы и методик на основе данного стандарта существенно облегчит работу экспертам испытательных лабораторий при функциональном тестировании веб-приложений, что сможет значительно сократить время, затраченное на проверку, а, следовательно, оптимизировать сроки, необходимые для проведения сертификационных испытаний данных приложений.

Ключевые слова: веб-приложение, стандарт подтверждения безопасности приложений OWASP, ФСТЭК, СЗИ, ИТ, разработчик, эксперты испытательных лабораторий, обеспечение безопасности.

Введение

Веб-приложение - это клиент-серверное приложение, в котором клиентом выступает браузер, а сервером - веб-сервер. Логика веб-приложения распределена между сервером и клиентом, хранение данных осуществляется, преимущественно, на сервере, обмен информацией происходит по сети. Одним из преимуществ такого подхода является тот факт, что клиенты не зависят от конкретной операционной системы пользователя, поэтому веб-приложения являются кроссплатформенными сервисами. Веб-приложения стали широко популярными в конце 1990-х — начале 2000-х годов.

Информация, содержащаяся в веб-приложениях, является критическим ресурсом, позволяющим организациям успешно решать свои задачи. Кроме того, частные лица вправе ожидать, что их персональная информация, будучи размещенной в данных приложениях, останется приватной, доступной им по мере необходимости и не сможет быть подвергнута несанкционированной модификации. При выполнении продуктами или системами информационных технологий (ИТ) их функций следует осуществлять надлежащий контроль информации, что обеспечило бы ее защиту от опасностей типа нежелательного или неоправданного распространения, изменения или потери [1-6]. Термин "безопасность ИТ" охватывает предотвращение и уменьшение этих и подобных опасностей [7].

Многие потребители ИТ из-за недостатка знаний, компетентности или ресурсов не будут уверены в безопасности применяемых продуктов и систем ИТ, и, возможно, не захотят полагаться исключительно на заверения разработчиков. Чтобы повысить свою уверенность в мерах безопасности веб-приложений, потребители могут заказать проведение анализа безопасности этого продукта или системы (т.е. оценку безопасности) [8-11]. Для проведения данного анализа экспертам испытательных лабораторий (ИЛ) будут необходимы программы и методики (ПиМ), которых на данный момент не существует в открытом доступе.

Анализ существующих стандартов подтверждения безопасности веб-приложений на территории Российской Федерации

На территории РФ нет открытых стандартов для подтверждения безопасности веб-приложений. Однако существуют приказы № 17, 21 и 31 ФСТЭК России, которые могут быть использованы для проведения тестирования веб-приложений.

²²⁶ Фокин М.С., НПО «Эшелон», m.fokin@npo-echelon.ru

Наиболее подходящим для разработки программы и методик подтверждения безопасности веб-приложений является 21-й приказ ФСТЭК России, поэтому для исследования в рамках данной статьи возьмем именно его.

Приказ № 21 ФСТЭК России направлен на обеспечение безопасности персональных данных при их обработке в информационных системах. Данный приказ не предназначен конкретно для подтверждения безопасности веб-приложений, но его меры по обеспечению безопасности персональных данных могут использоваться для функционального тестирования данных приложений.

Описание недостатков существующих стандартов

Рассмотрим, какие меры по обеспечению безопасности веб-приложений может предложить 21-й приказ.

В таблице 1 приведены меры для обеспечения безопасности идентификации и аутентификации субъектов и объектов доступа из приказа № 21.

Таблица 1 – Меры обеспечения безопасности из приказа № 21

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

Из таблицы 1 видно, что главным минусом данного приказа является нехватка необходимой информации для составления ПИМ. В нем описана сама задача, решение которой необходимо для подтверждения безопасности веб-приложений, но методов решения этой задачи не приводится. Приказ № 21 предлагает лишь общее понятие того, что должно выполняться в приложении, для подтверждения его безопасности. В свою очередь это заметно увеличивает время поиска методики проверки для обеспечения данных мер.

Анализ зарубежных стандартов подтверждения безопасности веб-приложений

Одним из наиболее распространенных и полных по требованиям к проверкам безопасности веб-приложений в США является Стандарт Подтверждения Безопасности Приложений OWASP (OWASP Application Security Verification Standard - ASVS). Он может использоваться для выбора приемлемых мер проведения проверок уровня безопасности веб-приложений. В нем содержится список требований безопасности к приложениям или тестам, которые могут быть использованы архитекторами систем информационной безопасности, разработчиками, специалистами по информационной безопасности, а также потребителями, для определения уровня надежности приложения.

Обоснование выбора ASVS при разработке ПИМ

Рассмотрим, что может предложить Стандарт Подтверждения Безопасности Приложений OWASP. В таблице 2 приведены некоторые пункты проверок из ASVS для подтверждения безопасности процедуры аутентификации веб-приложений.

Таблица 2

№	Описание	Уровни проверки безопасности		
		1	2	3
2.9.	Проверить, что функционал по изменению пароля включает в себя старый пароль, новый пароль и подтверждение пароля	✓	✓	✓
2.13	Проверить, что все пароли защищены достаточной степенью шифрования и что они могут противостоять методу перебора паролей		✓	✓
2.17	Проверить, что функция «забыл пароль» и другие пути восстановления пароля не отображают текущий пароль и что новый пароль не отображается пользователю в виде чистого текста	✓	✓	✓
2.19	Проверить, что самим приложением или компонентами приложения не используются стандартные пароли (такие как «admin/password»)	✓	✓	✓
2.25	Проверить, что систему можно настроить на запрет использования определенного количества ранее существовавших паролей		✓	✓
2.27	Проверить, что существуют меры по запрещению использования часто используемых или слабых паролей	✓	✓	✓
2.28	Проверить, что все запросы на аутентификацию, исполненные или нет, должны выполняться в среднее время на отклик			✓

Из таблицы 2 видно, что ASVS предлагает тестировщику не только перечень того, что должно быть реализовано в приложении, но и список проверок, благодаря которым можно наиболее полно оценить реальную безопасность процедуры аутентификации веб-приложений.

На основе данных, приведенных в таблицах 1 и 2, можно сделать вывод, что по сравнению с 21-ым приказом ФСТЭК России в ASVS указаны конкретные пункты проверок, необходимые для подтверждения безопасности веб-приложения. Данный Стандарт охватывает обширную область тестирования и предлагает новейшие методы проверок для подтверждения обеспечения приложением безопасности персональных данных пользователя.

В связи с этим за основу при разработке программы и методик для подтверждения безопасности веб-приложений предлагается взять ASVS, что позволит сократить время их разработки за счет полноты информации, представленной в ASVS [6].

Выводы

В заключении хотелось бы добавить, что на сегодняшний день «Стандарт Подтверждения Безопасности Приложений» - OWASP является одним из наиболее полных по списку требований к обеспечению безопасности веб-приложений. В нем рассмотрены часто встречающиеся проблемы, связанные с работой приложений и методы проверок, для их решения. Используя данный стандарт в качестве основы для составления требований к функциональному тестированию веб-приложений в системе сертификации СЗИ ФСТЭК России, мы сможем обеспечить более полную защиту информации конечного пользователя. Создание программы и методик на основе данного стандарта существенно облегчит работу экспертам испытательных лабораторий при функциональном тестировании веб-приложений, что сможет значительно сократить время, затраченное на проверку, а, следовательно, оптимизировать сроки, необходимые для проведения сертификационных испытаний данных приложений.

Литература

1. Барабанов А.В., Федичев А.В. Разработка типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации // Вопросы кибербезопасности. 2016. № 2 (15). С. 2-8.
2. Волкович Е.К., Мессерле А.А. Защита от вредоносных междоменных запросов // Вопросы кибербезопасности. 2013. № 3. С. 8-11.
3. Волосенков В.О., Андреева О.Н. Анализ способов обеспечения информационной безопасности веб-приложений // Вестник МГТУ МИРЭА. 2015. Т. 2. № 3 (8). С. 247-252.
4. Волосенков В.О., Лупорев С.Н. Способы обеспечения информационной безопасности веб-приложений // Проблемы безопасности российского общества. 2015. № 1. С. 80-85.
5. Сафин Л.К., Чернов А.В., Александров Я.А., Трошина К.Н. Исследование информационной защищенности мобильных приложений // Вопросы кибербезопасности. 2015. № 4 (12). С. 28-37.
6. Фокин М.С. Стандартизация процесса оценки защищенности веб-приложений. 6-я Всероссийская научно-техническая конференция «Безопасные информационные технологии – 2015», 2015 г.
7. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под ред. А.С. Маркова. М.: Радио и связь, 2012. 192 с.
8. Медведев Н.В., Марков А.С., Фадин А.А. Применение метода статического сигнатурного анализа для выявления дефектов безопасности веб-приложений // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2012. № 9. С. 21.
9. Markov, A.S., Fadin, A.A., Tsirlov, V.L. Multilevel metamodel for heuristic search of vulnerabilities in the software source code // International Journal of Control Theory and Applications, 2016, 9 (30), pp. 313-320.
10. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls // Journal of Theoretical and Applied Information Technology. 2016. V. 88. № 1. P. 77-88.
11. Бирюков А.А. Информационная безопасность: защита и нападение // М.: ДМК Пресс, 2012. – 474 с.

Научный руководитель: Цирлов Валентин Леонидович, кандидат технических наук, генеральный директор ЗАО «НПО «Эшелон», v.tsirlov@npo-echelon.ru.

Evaluation process analysis of web applications security

Fokin M.S.²²⁷

Abstract. Orders No. 17, 21 and 31 of FSTEC of Russia and OWASP application security verification standard (ASVS) are examined. The usage of ASVS as a basis document for testing procedures of web applications security is proposed. The lack of testing procedures documents is justified as an urgent problem. It is found that the usage of ASVS-based testing procedures documents will simplify the work of the testing laboratory experts in functional testing of web applications and significantly reduce the time spent verifying and, hence, optimize the time required for testing.

Keywords: web application, OWASP application security verification standard, ASVS, FSTEC of Russia, IT, developer, testing laboratory experts, security assurance.

²²⁷ Fokin M.S. NPO Echelon, Moscow, m.fokin@npo-echelon.ru

Применение метода k-ближайших соседей для распознавания дискретного сигнала в аддитивном шуме для двух каналов передачи информации при наличии общего шума

Троицкий И. И., Якубов Р. Ж.²²⁸

В данной статье приводятся результаты анализа метода k ближайших соседей при распознавании дискретного сигнала в аддитивном шуме. В ходе работы был проведен ряд вычислительных экспериментов, направленных на оценку качества работы метода k ближайших соседей. Кроме того, полученные данные позволяют оценить влияние параметров модели каналов передачи на распознавание сигнала. Результаты работы могут быть применены при организации передачи данных по различным каналам связи.

Ключевые слова: отношение сигнал/шум, вероятность распознавания, коэффициент корреляции, компьютерное моделирование, статистика.

Введение

Для решения задачи распознавания дискретного сигнала в аддитивном шуме может быть применен целый ряд методов, в том числе параметрические и непараметрические методы (к которым относится метод k ближайших соседей), быстрое преобразование Фурье, вейвлет-преобразования и т.д. [1-9].

В представленной работе ведется распознавание дискретного сигнала, передаваемого по двум каналам передачи, причем между шумами в них имеется статистическая взаимосвязь. Будем считать, что первом канале содержится полезный сигнал и аддитивный шум, а во втором только шум. Если второй канал передачи информации отсутствует, то в ряде случаев его можно искусственно ввести.

Математическое представление исследуемой модели

В связи с простотой реализации и наличием опыта проведенных исследований [10] для решения задачи классификации полученных данных в работе был использован метод k ближайших соседей [11].

Данный метод является одним из наиболее простых алгоритмов классификации. Классифицируемому объекту s присваивается тот класс S_i ($i = 1 \dots l$, где l – количество классов), к которому относится большинство из k ближайших элементов обучающей выборки.

Оценка успешного распознавания бинарного сигнала в канале представляется в виде величины

$$P^* = \frac{m}{N}, \text{ где} \quad (1)$$

m – количество успешно определенных классов сообщения,
 N – общая длина выборки.

Исходная модель:

$$\begin{cases} y = \frac{a}{2}\eta + \varepsilon + \xi \\ x = \delta + h \cdot \xi \end{cases} \quad (2)$$

где

$\varepsilon, \eta, \delta, \xi$ – случайные величины,

²²⁸ Троицкий И. И., канд. техн. наук, доцент, МГТУ им. Н.Э. Баумана, Москва, iitroickiy@mail.ru, Якубов Р. Ж., МГТУ им. Н.Э. Баумана, Москва, yakubov_rustam@inbox.ru

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

$\varepsilon \sim N(0, \sigma_\varepsilon^2)$ – шум в первом канале, $\delta \sim N(0, \sigma_\delta^2)$ – шум во втором канале, ε и δ статистически взаимосвязаны, $r_{\varepsilon, \delta}$ – их коэффициент корреляции;

$\xi \sim N(0, \sigma_\xi^2)$ – общий шум в каналах, h – константа;

η и ξ – случайные величины, независимые от ε и δ , и от друг друга;

ε и δ – естественные шумы, присутствующие в каналах передачи данных,

ξ – шум, появляющийся в каналах передачи данных при определенных технических условиях;

$a = |m_1 - m_{-1}|$ – дискретный сигнал;

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

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

Данная модель используется для определения вероятности распознавания сигнала методом k ближайших соседей. Отметим, что модель, рассматриваемая в работах [10] и [12], отличалась отсутствием шума ξ .

Эксперименты

Для исследования метода k ближайших соседей был проведен ряд экспериментов, позволяющих выявить влияние различных факторов на распознавание сигналов. Целью экспериментов являлось выявление зависимости вероятности распознавания передаваемого дискретного сигнала от изменения коэффициента корреляции шумов ε и δ , а также влияние на качество распознавания сигнала коэффициента h .

При исследовании коэффициент корреляции ε и δ принимал значения от -1 до 1 с шагом 0.1. Был проведен ряд экспериментов с разными значениями коэффициента h . Среднеквадратичное отклонение величины ξ значительно больше среднеквадратичного отклонения ε и δ . Кроме того, отношение сигнал/шум модели (2) $\ll 1$.

На (рис.1) представлены результаты исследований, направленных на нахождение оптимального значения параметра k . Оптимальным значением в данном случае считается то, при котором достигается максимальная вероятность распознавания сигнала.

Исходя из полученных результатов, можно отметить, что распознавание сигнала наименее эффективно при значении $k = 1$. Постепенное увеличение данного параметра позволяет достичь более высокой вероятности распознавания, причем при $k \geq 25$ результаты перестают улучшаться, в то время как вычислительная сложность растет. Соответственно, при проведении дальнейших вычислений, целесообразно принять $k = 25$.

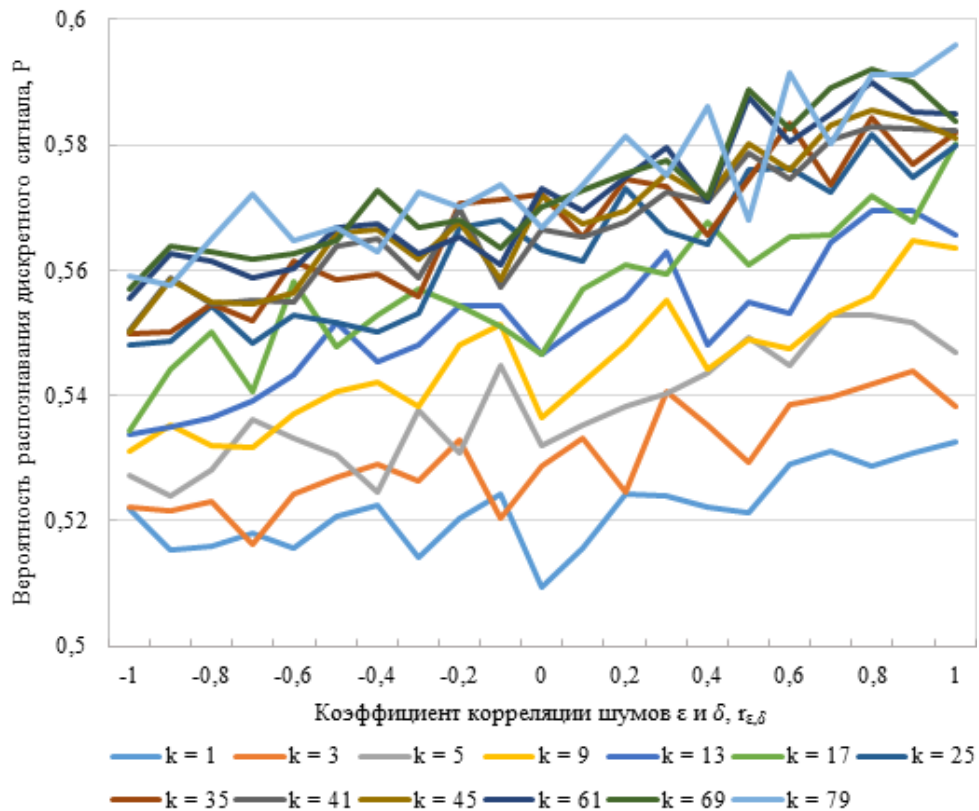


Рис.1 Зависимость вероятности распознавания P от значения параметра k

На (рис.2) и (рис.3) представлены результаты распознавания сигнала при разных значениях параметра h . По оси ординат откладываются значения вероятности распознавания P двумерного дискретного сигнала методом k ближайших значений. По оси абсцисс – значения коэффициента корреляции шумов ϵ и δ , $r_{\epsilon, \delta}$, принимающего значения от -1 до 1 с шагом 0,1. На (рис.2) представлены результаты эксперимента для значений $h \leq 0$. На (рис. 3) - для $h \geq 0$. Кроме того, в качестве эталона на каждом графике присутствуют результаты распознавания при значении $\xi = 0$, т.е. в каналах присутствуют только статистически связанные шумы ϵ и δ . Значение $k = 25$.

Результаты, полученные в ходе работы, позволяют сделать следующие выводы. Как и следовало ожидать, наличие в каналах шума ξ значительно снижает распознавание сигнала (на (рис.2) и (рис.3) представлены результаты для модели (2) без общего шума (случай $\xi = 0$) – они несколько выше, чем в других случаях). При изменении коэффициента h наблюдается следующая динамика. Его постепенно увеличение позволяет вплотную приблизиться к результатам, полученным для модели с отсутствием шума ξ (случаи $h = 5, h = -5, h = 15, h = -15$). При этом дальнейшее увеличение модуля данного параметра приводит к уменьшению вероятности распознавания сигнала, но она не падает до критического значения (критическим считается значение $P=0.5$).

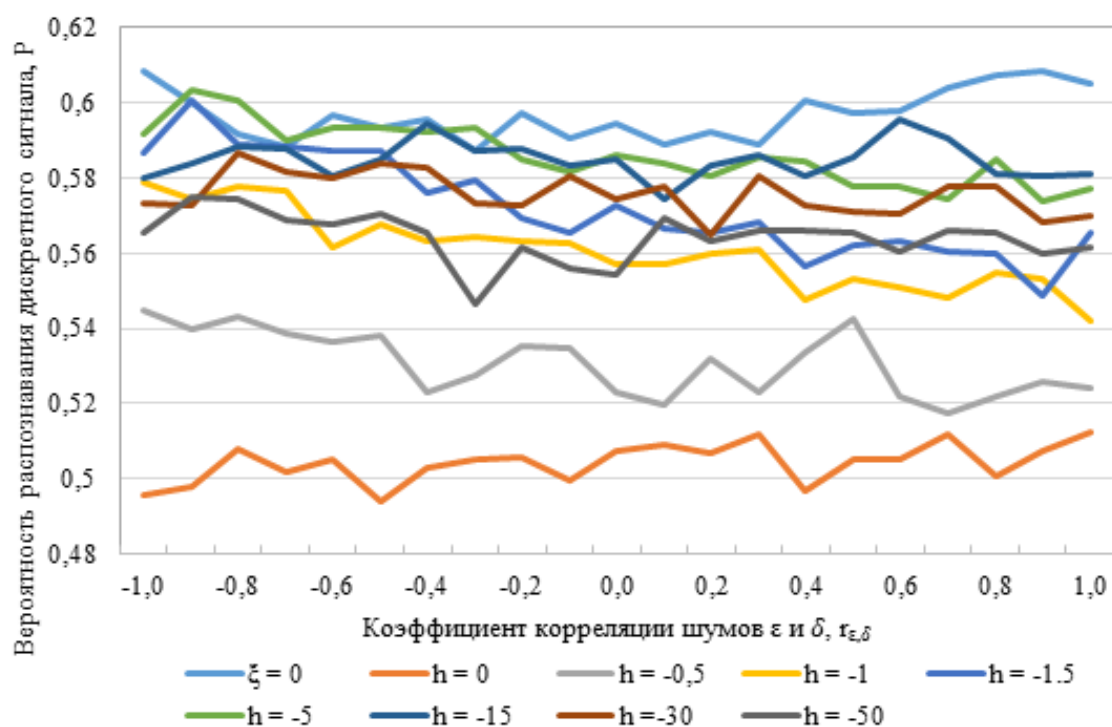


Рис. 2. Влияние шума ξ на распознавание сигнала в каналах X и Y методом k ближайших соседей, $h \leq 0$

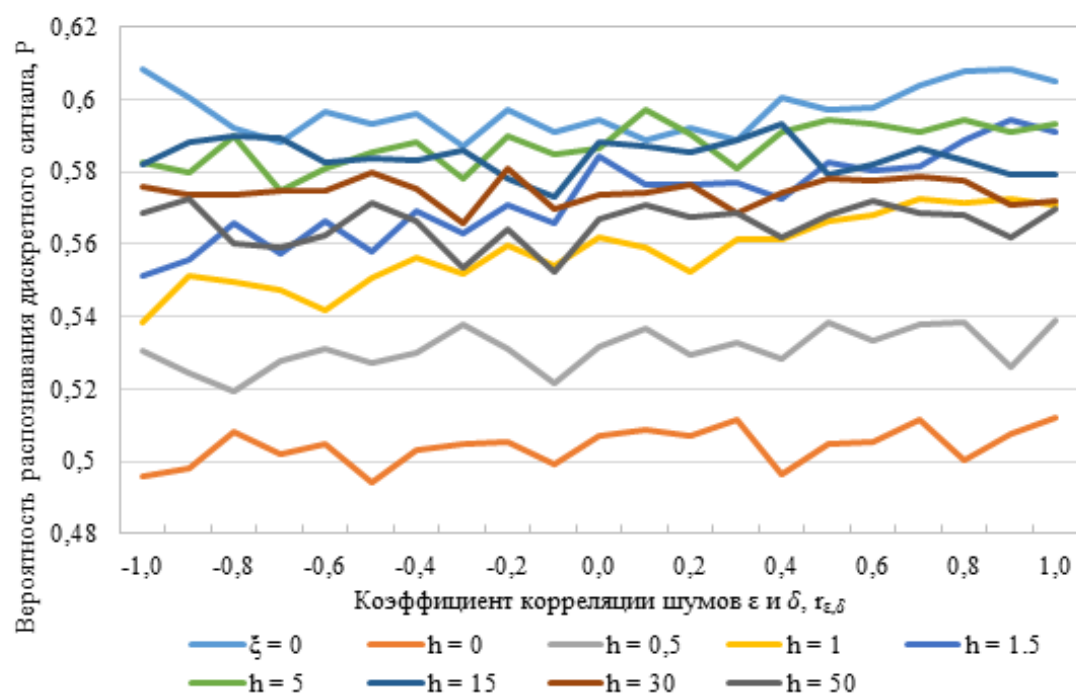


Рис. 3. Влияние шума ξ на распознавание сигнала в каналах X и Y методом k ближайших соседей, $h \geq 0$

Проведенные эксперименты позволили выявить ряд закономерностей, проявляемых при распознавании дискретного сигнала в модели (2) с использованием метода k ближайших соседей. Учитывая простоту реализации данного алгоритма, а также возможность выбора параметра k , позволяющего подобрать оптимальное соотношение вычислительной сложности к точности исследований, можно сказать, что метод k ближайших соседей оптимально подходит для решения задачи распознавания дискретного сигнала.

Выводы

В ходе данной работы была проанализирована возможность использования метода k ближайших соседей для распознавания двумерного дискретного сигнала. Проведен ряд вычислительных экспериментов, позволивших на практике убедиться в высокой точности данного метода, а также оценить вероятность распознавания сигнала при изменении некоторых параметров модели (2). Результаты исследований позволяют заявить об эффективности распознавания сигнала, передаваемого по двум каналам связи, при наличии в них статистически связанных шумов, а также о высокой эффективности применения метода k ближайших соседей для решения данной задачи. Полученные данные позволяют заложить основу для дальнейших исследований в области передачи данных с использованием инструментов математического моделирования и статистики.

Литература

1. Горелик А. Л., Скрыпник В. А. Методы распознавания. М.: Высшая школа, 1989. 232 с.
2. Даджион Д., Мерсеро Р. Цифровая обработка многомерных сигналов. М.: Мир, 1988. 488 с.
3. Малла С. Вейвлеты в обработке сигналов. М: Мир, 2005. 672 с.
4. Афонский А. А., Дьяконов В. П. Цифровые анализаторы спектра, сигналов и логики. М: Солон – Пресс, 2005. 576 с.
5. Сергеенко А. Б. Цифровая обработка сигналов. 2-е изд. СПб: Питер, 2006. 751 с.
6. Шахтарин Б. И. Случайные процессы в радиотехнике. Т.1. Линейные преобразования. М.: Горячая линия — Телеком, 2010. 520 с.
7. Тихонов В. И., Шахтарин Б. И., Сизых В. В. Случайные процессы. Примеры и задачи. Т.5. Оценка сигналов, их параметров и спектров. Основы теории информации. М.: Горячая линия — Телеком, 2014. 400 с.
8. Перов А. И. Статистическая теория радиотехнических систем. М: Радиотехника, 2003. 400 с.
9. Джиган В. И. Адаптивная фильтрация сигналов. Теория и алгоритмы. М: Техносфера, 2013. 528 с.
10. Якубов Р. Ж. Двумерное распознавание сигнала на основе метода k ближайших соседей // Молодежный научно-технический вестник, 2015. № 7. с. 40-46. URL: http://sntbul.bmstu.ru/file/791148.html?__s=1
11. Дуда Р., Харт П. Распознавание образов и анализ сцен. М.: Мир, 1976. 510 с.
12. 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

Application of the K-nearest Neighbors Algorithm for Recognition of a Discrete Signal in Additive Noise for Two Channels of Communication with General Noise **Troitskij I. I., Yakubov R. Zh.²²⁹**

In this article are analyzed results of a k-nearest neighbors algorithm in case of recognition of the discrete signal in an additive noise. A row of the computing experiments directed to assessment of quality of operation of a k-nearest neighbors algorithm was carried out. Besides, results allow to estimate influence of model parameters of transmission channels on recognition of a signal. Results of operation can be applied in case of the organization of data transmitting for different communication links.

Keywords: signal-to-noise ratio, integral of probability of recognition, correlation coefficient, computer modeling, statistics.

УДК 004.056.53; ГРНТИ 49.33.35; ВАК 05.13.19

К вопросу о централизации управления информационной безопасностью корпоративной сети

Фадин А.А.²³⁰, Цирлов В.Л.²³¹

Аннотация: Показана роль SIEM-систем в структуре управления информационной безопасностью корпоративной сети. Выделены основные компоненты SIEM-системы. Обоснованы показатели выбора SIEM-системы. Сделан обзор российского и международного рынка SIEM-решений. Типовая архитектура и принципы функционирования рассмотрены на примере программного комплекса «KOMRAD Enterprise SIEM». Рассмотрены проблемные вопросы внедрения SIEM-систем. Представлен опыт разработки и внедрения отечественной SIEM.

Ключевые слова: события информационной безопасности, мониторинг, управление безопасностью, анализ данных, правила корреляции

Введение. В настоящее время основной тенденцией построения систем защиты информации является комплексный подход. Инфраструктура крупных организаций становится настолько многоуровневой и в целом сложной, что уследить за огромным потоком сведений о нарушениях информационной безопасности и оценить значимость каждого из них бывает чрезвычайно сложно [1-4]. Это приводит к росту требований к квалификации и качеству работы персонала автоматизированной системы. Решение обозначенных выше проблем появилось почти 10 лет назад, но особенно востребованным оно стало только в последние годы. В 2005 году аналитическое агентство Gartner объединило термины Security Information Management (SIM) и Security Event Management (SEM). Так появилось понятие Security Information and Event Management (SIEM) - система, предназначенная для анализа информации, поступающей от различных систем [5, 6].

SIEM можно определить как класс решений в области информационной безопасности, ориентированных на поддержку процессов управления как безопасностью, так и всей ИТ-инфраструктурой предприятия. Решение SIEM позволяет проводить:

- централизованный сбор и анализ данных журналов событий СЗИ, АРМ, серверов и сетевого оборудования;
- удаленный контроль параметров конфигурации и работы автоматизированных

²²⁹ Troitskij Igor, Ph.D, Associate Professor, Bauman Moscow State Technical University, Moscow, e-mail: iitroickiy@mail.ru; Yakubov Rustam, Bauman Moscow State Technical University, Moscow, e-mail: yakubov_rustam@inbox.ru

²³⁰ Фадин Андрей Анатольевич, ЗАО «НПО «Эшелон», af@снро.ру

²³¹ Цирлов Валентин Леонидович, канд. техн. наук, МГТУ им.Н.Э.Баумана, v.tsirlov@bmstu.ru

рабочих мест с помощью установленного программного агента;

- оперативное оповещение и реагирование на внутренние и внешние угрозы безопасности автоматизированной системы;

- контроль выполнения заданных требований по безопасности информации, сбор статистики и построение отчетов по защищенности АС в любые моменты времени.

Важнейшей особенностью SIEM-решений является возможность выявления неизвестных компьютерных атак, т.е. атак, не выявляемых сигнатурными методами.

SIEM представляет собой распределенную систему, включающую в себя сервер, выполняющий основные работы по агрегации и корреляции событий, и сенсоры, собирающие информацию, передаваемую из различных компонентов АС. В крупных системах отдельным модулем иногда реализуют компонент хранения журналов событий, как правило, на базе быстрых систем хранения данных. Сенсоры, как правило, располагаются в каждом сегменте (и даже узле сети). Центр управления и хранилище журналов событий чаще всего находятся в контролируемой зоне, рядом либо с АРМ администратора безопасности, либо с АРМ системного администратора АС. Сенсоры должны поддерживать различные протоколы взаимодействия и иметь возможность настройки новых протоколов и входных форматов. Наиболее популярными протоколами передачи журнальных данных являются Syslog, FTP, ODBC и SNMP. Кроме того, важно не только поддерживать транспортный протокол, но и распознавать формат и семантику содержимого журнала. Для этих целей имеются форматы Syslog, CLF, SCAP, CIM и CEF, предлагаемые для его использования различными поставщиками продуктов в области безопасности.

Рассмотрим компоненты типовой архитектуры SIEM на примере программного комплекса «KOMRAD Enterprise SIEM» производства АО «НПО «Эшелон» [7-12]. Рассматриваемое решение содержит:

- источники событий - объекты ИТ-инфраструктуры (конечные устройства и системы, такие как серверы, активное сетевое оборудование, базы данных, средства защиты информации), мониторинг безопасности которых является основной задачей «KOMRAD Enterprise SIEM»;

- журналы событий объектов ИТ-инфраструктуры;

- средства сбора и передачи информации - агенты, собственные средства конечных устройств и систем или запросы от сенсора, передающие данные о событиях ИБ от источников событий в ядро системы;

- rsyslog - средство приёма данных о событиях ИБ и их агрегации в журналах;

- журналы данных о событиях информационной безопасности, поступивших от конечных устройств и систем;

- плагин - набор инструкций, в соответствии с которыми сенсор обрабатывает данные из журналов;

- сенсор - программный модуль, нормализующий и передающий данные в базу данных (БД) «KOMRAD Enterprise SIEM»;

- база данных, в которой хранятся архивы событий ИБ, данные об инцидентах ИБ и информация о настройках системы;

- модуль корреляции - модуль анализа данных, с помощью которого выявляются инциденты ИБ;

- веб-интерфейс - средство взаимодействия администратора безопасности с системой;

- ядро - совокупность программных модулей «KOMRAD Enterprise SIEM».

При возникновении событий ИБ на конечных устройствах или системах данные об этом записываются в журналы состояния соответствующих объектов ИТ-инфраструктуры и в режиме времени, близком к реальному, отправляются на сервер «KOMRAD Enterprise

SIEM» агентами, собственными средствами конечных устройств и систем или по запросу от сенсора к БД (MySQL, MSSQL). Сервер «KOMRAD Enterprise SIEM» принимает данные, агрегирует и записывает их в журналы в соответствии с типом источника событий с помощью утилиты rsyslog. Сенсор обрабатывает журналы в соответствии с логикой плагинов, обеспечивающих поддержку работы с конечными устройствами и системами различных типов, после чего нормализованные данные поступают в БД «KOMRAD Enterprise SIEM», где каждому событию ИБ присваивается уникальный персональный идентификатор. После этого выполняется обработка данных модулем корреляции в соответствии с заранее определёнными правилами корреляции и политиками, на основании которых выявляются инциденты ИБ [12].

Заключение. Дальнейший рост эффективности систем безопасности связан прежде всего с качеством их взаимной интеграции, одним из столпов этого объединения являются SIEM-системы, решающие различные задачи поддержки процессов управления как безопасностью, так и всей IT-инфраструктурой предприятия.

Литература

1. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности // Мониторинг правоприменения. 2017. № 1 (22). С. 53-61.
2. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г // Вопросы кибербезопасности. 2013. №1. С.61-64.
3. Петренко А.С., Петренко С.А. Проектирование корпоративного сегмента СОПКА // Защита информации. Инсайд. 2016. №6 (72). С. 47-52.
4. Петренко С.А., Шамсутдинов Т.И., Петренко А.С. Научно-технические задачи развития ситуационных центров в Российской Федерации // Защита информации. Инсайд. 2016. №6 (72). С. 37-43.
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. Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80-81.
7. Клянчин А.И., Марков А.С., Фадин А.А., Илюхин М.В. SIEM-технология как основа построения защищенных систем. В сборнике: Информатизация и информационная безопасность правоохранительных органов XXII Всероссийская научная конференция. 2013. С. 270-273.
8. Марков А.С., Фадин А.А., Рауткин Ю.В. Корпоративные информационные системы управления событиями информационной безопасности. В сборнике: Информационные и математические технологии в науке и управлении. Труды XVIII Байкальской Всероссийской конференции «Информационные и математические технологии в науке и управлении». Отв. ред.: д-р техн. наук Л.В. Массель, ИСЭМ СО РАН. 2013. С. 162-166.
9. Марков А.С., Фадин А.А., Цирлов В.Л., Рауткин Ю.В. О централизации управления информационной безопасностью предприятия. В сборнике: Региональная информатика и информационная безопасность сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2015. С. 345-347.
10. Фадин А.А. На пути к развертыванию центра управления информационной безопасностью предприятия // Connect! Мир связи: наука. Бизнес. Управление. 2013. №4. С.57-60.
11. Фадин А.А., Авезова Я.Э. SIEM-решения по управлению и консолидации средств защиты информации // Автоматика. Информатика. 2015. № 1(36). С. 27-31.
12. КОМРАД // Разработки АО "НПО "ЭШЕЛОН" URL: <https://npo-echelon.ru/production/65/9855> (дата обращения: 1.01.2017).
13. Марков А.С., Цирлов В.Л., Фадин А.А., Титов А.В., Марков Г.А. Устройство корреляции событий информационной безопасности // Патент на полезную модель. 2916. RUS 166348 01.08.2016.

Centralizing of Information Security Control

A. Fadin²³², V. Tsirlov²³³

The role of SIEM-systems in the management structure of the enterprise information security is shown. The basic components of SIEM-system are obtained. Based indicators for SIEM-selection system are substantiated. The review of the Russian and international market is done. Typical architecture and operating principles are considered by the example of KOMRAD Enterprise SIEM. The issues of implementing SIEM-systems are considered. The experience in the development and implementation of national SIEM is presented.

Keywords: information security events, monitoring, SIEM, data analysis, correlation rules

УДК 621.0+681.5

Программное обеспечение АРМ проектирования средств сканирования в FSO

Чичварин Н.В., Бушуев В.В., Иванников П.В., Сосенко А.С.²³⁴

В публикации приведены результаты исследований, позволившие разработать программный комплекс для проектирования устройств, входящих в состав средств пространственной стабилизации защищенных атмосферных линий связи (FSO). Рассмотрены нестандартные методы сканирования в оптико-электронных, лазерных, акустоэлектронных и радиолокационных системах. Предлагается методика и универсальный алгоритм моделирования сканирующего устройства с произвольным законом развертки. Появляется возможность синтезировать произвольный закон сканирования при проектировании сканирующих устройств.

Ключевые слова: Автоматизированное рабочее место, алгоритм, анализ, модель, прибор с зарядовой связью.

Введение. Целью работы было создание ПО АРМ для решения задач анализа и синтеза СУ с произвольным законом сканирования, с учетом помех и противодействия. Предложенная методика позволяет синтезировать различные траектории развертки в различных СУ, в особенности систем локации, систем технического зрения и дистанционного зондирования. К ним относятся: акустоэлектронные системы, оптико-электронные системы, радиоэлектронные системы.

Таким образом, разработанное ПО позволяет анализировать распределение облученности в пространстве анализа сканирующих систем локации и обнаружения. Характерной особенностью ПО является возможность учета различного рода атак на систему. Это, в свою очередь, позволяет дополнять АРМ соответствующих САПР АЭС, РЭС и ОЭС и проектировать различные системы с учетом требований ИБ.

Описание выбранного метода моделирования.

При разработке программного комплекса учтены требования обеспечения максимального быстродействия. Выбран полу частотный метод моделирования процесса анализа изображения СУ[1]. Отметим, что выбранный метод модифицирован. Его

²³² Andrei A. Fadin, NPO Echelon, af@cnpo.ru

²³³ Valentin Tsirlov, Ph.D., Bauman Moscow State Technical University, v.tsirlov@bmstu.ru

²³⁴

Чичварин Н.В., к.т.н, доцент, МГТУ им. Н.Э. Баумана, Москва, genrih.gertz@gmail.com, Бушуев В.В., Иванников П.В., Сосенко А.С., МГТУ им. Н.Э. Баумана, Москва, vovabush94@mail.ru

особенностью является применимость для моделирования сканирования по любому произвольному закону. Ограничением является то, что модель распределения облученности должна реализоваться суперпозицией четных функций. При реализации метода сигнал на выходе СУ определяется выражением для вычисления взаимной ковариации:

$$\Phi(x_p, y_p) = \int_{-\infty}^{\infty} E(x', y') h(x' - x_p, y' - y_p) dx' dy' \quad (1),$$

Где $x_p = \cos(\omega t)$, $y_p = \sin(\omega t)$ – трансформированный закон сканирования.

В частотной области выражение (1) принимает вид:

$$F \{ \Phi(x', y') \} = F \{ E(x', y') \} F^* \{ h(x', y') \}, \quad (2)$$

Где $F \{ * \}$ – оператор преобразования Фурье, $F^* \{ * \}$ – оператор преобразования Фурье, приводящего к комплексно сопряженной функции.

Поскольку $h(x', y')$ – строго вещественная функция, ее Фурье – образ совпадает с комплексно сопряженным и (1) преобразуется к интегралу свертки:

$$\Phi(x_p, y_p) = \int_{-\infty}^{\infty} E(x', y') h(x_p - x', y_p - y') dx' dy' \quad (3),$$

И выражение (2) становится интегралом свертки в частотной области:

$$F \{ \Phi(x', y') \} = F \{ E(x', y') \} F^* \{ h(x', y') \} \quad (4),$$

Для полноты описания достаточно заметить, что искомая функция $\Phi(t)$ получается путем вычисления обратного преобразования Фурье от $F \{ \Phi(x', y') \}$ и подстановки выражений для анализа.

Описание программного обеспечения

Результатом проделанной работы является удобный инструмент, который может быть использован при проектировании СУ. Его особенностью является возможность моделирования [2] процесса анализа изображения с произвольным законом развертки. Кроме того, открывается возможность синтеза законов сканирования.

Общий интерфейс выглядит следующим образом: при запуске ПО пользователю предоставляется возможность по выбору типа анализатора (рис. 1).

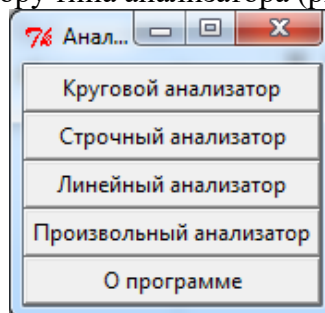


Рис.1. Главное меню

При выборе кругового анализатора пользователю открывается окно, в верхней части которого возможен выбор необходимых параметров для анализа, по середине – сам круговой анализатор, в самом низу – график функции на выходе анализатора, см. рис.2.

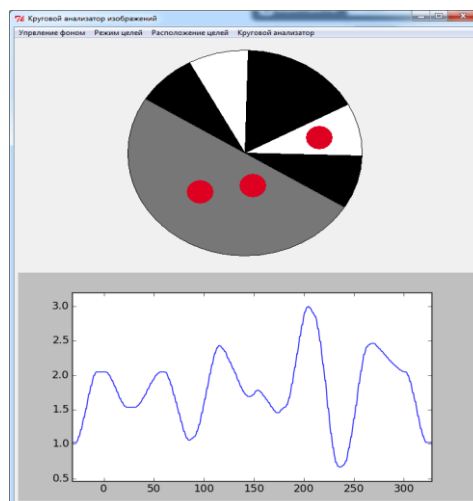


Рис.2. Окно кругового анализатора

Программа может позволить пользователю настроить такие параметры среды, как шум, его интенсивность, характер распределения (равномерный или нормально распределенный). У пользователя есть возможность как самому создавать цели, рис.3, с указанием нужных параметров, так и загружать определенные изображения в роли целей или воспользоваться стандартными шаблонами. Также программа способна менять тип анализирующей системы, выбирая их из заранее предложенного пула.

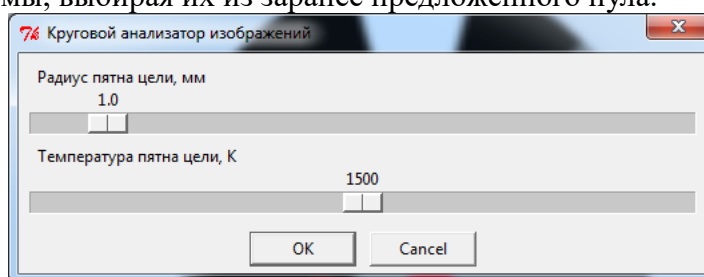


Рис.3. Создание цели с определенными параметрами

Режим строчного анализатора является аналогом ПЗС-матрицы и демонстрирует ее работу в замедленном действии. Строчный анализатор представляет собой построчно перемещающееся анализирующее окно, которое можно наблюдать на рис.4. Данный режим также поддерживает моделирование воздействий нестационарных помех.

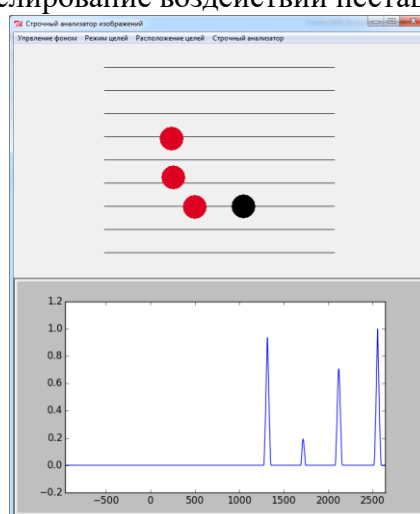


Рис.4. Режим строчного анализатора

В ПО реализован дополнительный режим, позволяющий проектанту моделировать произвольный закон развертки. При моделировании воздействия случайных сигналов это

позволяет учитывать их возможную нестационарность. В этом случае возможно применение метода Монте – Карло.

Существо метода Монте-Карло применительно к ПО.

В нашем ПО метод Монте-Карло [3] применяется для свертки двух произвольных трехмерных функций. Но из-за специфики решаемой задачи можно работать с взвешенными проекциями этих функций на плоскость и использовать метод Монте-Карло для вычисления площади взвешенного пересечения этих проекций, а именно, анализатора и цели. Речь идет о взвешенном пересечении [4], т.к. в общем случае анализатор обладает зависящей от координат чувствительностью: $S(x, y)$, а цель обладает зависящей от координат интенсивностью: $I(x, y)$. Нам же нужно посчитать следующий интеграл, величина которого и будет являться амплитудой сигнала на выходе анализатора.

$$U = \iint_{x,y} S(x, y)I(x, y)dxdy \quad (5),$$

Геометрический метод Монте-Карло подходит в нашем случае очень хорошо. Плюс, благодаря конструкции метода, мы сможем регулировать соотношение точность/скорость вычислений, регулирую кол-во «бросков» - случайно выбранных точек на плоскости. Прodelывая вычисления методом Монте-Карло через заданные промежутки времени, будем иметь сигнал на выходе анализатора.

Анализ причин возникновения нестационарности случайного процесса при традиционном моделировании СУ. Известные методы учета, недостатки.

Учёт нестационарности случайного процесса при разработке ПО, связанного с анализом входного многомерного и выдаче выходного двумерного сигнала, важен, так как возникающие помехи способны серьезно повлиять на правильную форму и суть выходного сигнала при их неучёте.

Для борьбы с нестационарностью используются разные методы. Один из них – **метод формирующих фильтров** [5]. Он основан на возможности представления спектральной плотности входного процесса в виде дробно-рациональной функции частоты. В процессе преобразований система фильтров преобразует белый шум в функцию заранее заданного вида, что позволяет учитывать его при анализе, зная его параметры. Однако, с точки зрения высокоуровневого программирования, реализация данного метода представляется трудоемкой в виду необходимости работать как с интегрированием от бесконечных пределов, так и из-за работы с комплексными составляющими.

На ряду с предыдущим, используется **моделирование координатной функции**. Интегральное каноническое представление корреляционной функции можно выразить как:

$$t1,t2=-\infty+\infty G\omega*xt1,j\omega*xt2,j\omega d\omega \quad (6),$$

Где $x(t_1, j\omega)$ – координатная функция соответствующего канонического разложения случ. функции, а $G(\omega)$ – некоторая заданная функция.

Воспользуемся нестационарной параметрической передаточной функцией системы $W(t, j\omega)$ и перепишем выражение:

$$R_{\text{вых}}t1,t2=-\infty+\infty S_{\text{вх}}\omega Wt1,j\omega e^{-j\omega t1} Wt2,j\omega e^{j\omega t2} d\omega \quad (7),$$

Таким образом, в роли координатной функции выступает $W(t, j\omega)e^{-j\omega t}$, и, если она известна, то дело остается за малым. Выражение для нее имеет вид:

$W(t, j\omega)e^{-j\omega t} = \int_0^t \omega(t, \sigma)e^{j\omega\sigma} d\sigma$, где $\omega(t, \sigma)$ – импульсная переходная функция системы. Так как реально можно воспользоваться квадратом передаточной функции, то выходная функция примет вид:

$$R_{\text{вых}}(t_1, t_2) = \int_{-\infty}^{+\infty} S_{\text{вх}}(\omega)|W(t, j\omega)|^2 d\omega, \text{ где } |W(t, j\omega)|^2 = x_r^2(\omega, t) + x_i^2(\omega, t) \quad (8),$$

а каждое из слагаемых – мнимая и действительная часть координатной функции.

Этот способ не обеспечивает полной автоматизации процесса определения дисперсии. Также он оказался трудоемок для компьютера в режиме реального времени.

Вывод. Предложена методика модельного представления процесса сканирования различных изображений с произвольным растром и законом развертки. Разработано ПО для функционирования в составе АРМ САПР ОЭС, АЭС, РЭС.

Литература.

1. Войтишек А.В. Основы метода Монте-Карло // Учебное пособие // Новосиб. Гос. Ун-т Новосибирск, 2010. 108 с. URL: <http://mmf.nsu.ru/sites/default/files/voytishekav-basics-of-monte-carlo-method.pdf>
2. Феер К. Беспроводная цифровая связь: методы модуляции. — Пер. с англ. // Под. ред. В. И. Журавлёва. // М.: Радио и связь, 2000. URL: http://ra01.twirpx.net/0396/0396513_02923B80/feer_k_besprovodnaya_tsifrovaya_svyaz_metody_modulyatsii_i_r.djvu
3. Foulkes W. M. C., Mitas L., Needs R. J. and Rajagopal G. Quantum Monte Carlo simulations of solids // Reviews of Modern Physics, 2001. URL: <https://spiral.imperial.ac.uk/bitstream/10044/1/866/1/Quantum%20Monte%20Carlo%20simulations.pdf>
4. Alex F. B. Fundamentals of the Monte Carlo method for neutral and charged particle transport // The University of Michigan Department of Nuclear Engineering and Radiological Sciences, 2001. URL: <http://www-personal.umich.edu/~bielajew/MCBook/book.pdf>
5. Радченко Ю.С., Радченко Т.А., Основы статистического моделирования, часть 2, Моделирование случайных процессов // Учебное пособие для вузов, 2010. URL: rucont.ru/file.ashx?guid=fd48be40-c687-48c9-b9fe-0e0d86db8e1c

Software Wdt Scanning FSO

Chichvarin N.V., Bushuev V.V., Ivannikov P.V., Sosenko A.S.²³⁵

The publication presents the results of research have allowed to develop a software package for the design of devices that make up the means of steric stabilization of atmospheric secure communication lines (FSO). Are considered non-standard methods of scanning optoelectronic, laser, acousto-electronic and radar systems. The technique and algorithm modeling universal scanner to scan an arbitrary law. The proposed method allows to synthesize a random sweep in the design of scanning devices.

Keywords: workstation, algorithm analysis, model, charge-coupled device.

УДК 004.056;519.178;51-74

Обнаружение виртуальных пользователей в онлайн-социальных сетях путем анализа графов ближайшего окружения

Чесноков В.О.²³⁶

Работа проведена при поддержке РФФИ (грант № 16-29-09517 офи_м).

В связи с тем, что онлайн-социальные сети стали площадкой для информационного противоборства, актуальной задачей является поиск источников дезинформации и пропаганды. Предложен новый метод обнаружения виртуальных пользователей в онлайн-социальных сетях, основанный на качественном анализе сообществ графа ближайшего окружения пользователя. Эксперименты на двух тестовых выборках из социальной сети LiveJournal с использованием трех алгоритмов выделения сообществ показали, что с помощью набора пороговых правил можно отличить бота от легитимного пользователя с высокой точностью, полнотой и долей правильных ответов²³⁷.

²³⁵ Bauman Moscow State Technical University

²³⁶ Чесноков Владислав Олегович, МГТУ им. Н.Э. Баумана, Москва, v.o.chesnokov@yandex.ru

²³⁷ Работа проведена при поддержке РФФИ (грант № 16-29-09517 офи_м).

Ключевые слова: виртуальные пользователи, боты, граф ближайшего окружения, социальный граф, выделение сообществ, информационное противоборство.

Во многих областях человеческой деятельности для анализа общественного мнения используются системы мониторинга онлайн-социальных сетей. При этом большинство существующих систем ориентированы на сбор количественных показателей, таких как количество записей по теме, количество положительных оценок к ним и их эмоциональный окрас. В связи с этим онлайн-социальные сети весьма уязвимы к внешнему влиянию: при наличии достаточного количества ресурсов злоумышленник может создать большое количество поддельных аккаунтов (ботов) и поспособствовать искусственному росту сообщений с определенной точкой зрения, манипулируя таким образом общественным мнением.

В последние годы онлайн-социальные сети стали площадкой для информационного противоборства: они используются как средство распространения дезинформации и пропаганды. Губанов и др. [1] выделяют задачу анализа и обеспечения информационной безопасности социальных сетей как двойственную к задаче информационного управления и манипулирования. В проекте новой Доктрины информационной безопасности Российской Федерации в качестве одной из угроз указывается использование отдельными государствами информационно-психологических воздействий, направленных на дестабилизацию внутривнутриполитической и социальной ситуации, с применением информационных технологий.

подавляющее большинство исследователей используют комбинированный подход для обнаружения ботов, заключающийся в использовании нескольких методов одновременно. Зачастую он строится на машинном обучении, и позволяет на основе многих факторов выносить решение об обнаружении бота с некоторой долей уверенности. Основная задача заключается в отборе значимых факторов, подборе классификаторов и обучении модели.

Даже если не использовать машинное обучение, использование нескольких методов повышает вероятность обнаружения поддельных аккаунтов. Среди основных факторов, по которым происходит обнаружение ботов, можно выделить такие группы признаков как поведение пользователя в сети, характеристики текстов его записей, информация из профиля пользователя и свойства аккаунта как вершины социального графа.

Основная гипотеза многих ранних подходов обнаружения ботов на основе анализа структуры социального графа [2-4] заключалась в том, что боты имеют мало связей с легитимными пользователями и много связей между собой, т. е. образуют сообщество. Соответственно, выявить группы ботов возможно путем применения алгоритма выделения сообществ к социальному графу.

Однако, как было показано в работах [5] и [6], достаточно большой процент легитимных пользователей настроены очень открыто даже к незнакомым им людям. В рамках эксперимента [5] 20 процентов пользователей принимали запросы на дружбу от ботов, с которыми у них не было ничего общего, а 60% — от любых ботов, у которых был хотя бы один общий друг с ними. Более того, в работе [7] было показано, что достаточно много ботов не формируют тесно связанные группы вершин (сообщества).

Тем не менее, в многих работах [4, 7] отмечается, что боты устанавливают связи случайным образом, со всеми подряд. В то же время социальные графы легитимных пользователей имеют неоднородную структуру. Вероятно, перспективным будет подход, основанный на анализе качественных характеристик социального графа аккаунта [2].

Разработанный метод обнаружения ботов в онлайн-социальных сетях основан на

гипотезе о том, что графы ближайшего окружения ботов формируются случайно, и поэтому отличаются по своим характеристикам от графов обычных пользователей. Предлагаемый метод основан на выделении сообществ и сводится к набору из пороговых правил:

1. Сообщества размером меньше минимального или больше максимального не учитываются.
2. Если их количество превышает порог, то пользователь считается ботом.
3. Если количество друзей в сообществах больше максимального или меньше минимального, то пользователь — бот.
4. Если отношение количества друзей в и вне сообществ больше порога, то пользователь считается ботом.
5. Если количество сообществ больше максимального или меньше минимального, то пользователь — бот.
6. Иначе пользователь легитимный.

Для оценки качества разработанного метода использовалась стандартная процедура с экспертной оценкой. Были рассчитаны доля правильных ответов, точность, полнота и F -мера. Тестовыми выборками служили два набора графов ближайшего окружения ботов (автоматических и управляемых) из социальной сети LiveJournal, а также графы случайно выбранных легитимных пользователей. В качестве алгоритма выделения сообществ были использованы максимизация модулярности, *CESNA* [8] и алгоритм, предложенный в работе [9]. Пороговые значения были получены автоматически, перебором.

Эксперименты показали, что алгоритм *CESNA* не подходит для разработанного метода, однако при использовании двух других алгоритмов разработанный метод показал высокие значения всех мер качества, близкие к единице. Вариант алгоритма из работы [9], в котором отбрасывались сообщества с пустой меткой дает небольшой прирост эффективности метода.

Таким образом, даже простой анализ, затрагивающий лишь количество сообществ и их размер, позволяет отделить простых ботов от реальных людей. Большинство создателей виртуальных пользователей не утруждают себя таким уровнем проработки, поскольку подобный анализ почти невозможен без привлечения автоматизированных средств. Разработанный метод может быть использован как один из элементов подсистемы обнаружения виртуальных пользователей в системе мониторинга социальных сетей.

При условии полномасштабного мониторинга социальной сети возможно повышение качества работы метода. Очевидно, что, если большинство друзей пользователя боты, то и сам он скорее всего бот. Тогда для создания одного правдоподобного виртуального пользователя необходимо создать несколько профилей, и установить много связей с легитимными пользователями. Соответственно, стоимость создания ботов существенно возрастает.

Литература

1. Губанов Д.А., Новиков Д.А., Чхартисвили А.Г. Модели информационного влияния и информационного управления в социальных сетях // Проблемы управления. — 2009. — No 5. — С. 28-35.
2. Paradise A., Puzis R., Shabtai A. Anti-Reconnaissance Tools: Detecting Targeted Socialbots // IEEE Internet Computing. — 2014. — Vol. 18, no. 5. — pp. 11-19.
3. An Analysis of Social Network-based Sybil Defenses / B. Viswanath [et al.] // SIGCOMM Comput. Commun. Rev. — 2010. — Vol. 40, no. 4. — pp. 363-374.
4. Aiding the Detection of Fake Accounts in Large Scale Social Online Services / Q. Cao [et al.] // The 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12). — San Jose, CA: USENIX, 2012. — pp. 197-210.
5. Design and Analysis of a Social Botnet / Y. Boshmaf [et al.] // Computer Networks. — 2013. — Vol. 57, no. 2. — pp. 556-578.
6. Detecting spammers on social networks / X. Zheng [et al.] // Neurocomputing. — 2015. — Vol. 159. — pp. 27-34.

7. Uncovering the overlapping community structure of complex networks in nature and society / G. Palla [et al.] // Nature. — 2005. — Vol. 435, no. 7043. — pp. 814–818.
8. Yang J., McAuley J. J., Leskovec J. Community Detection in Networks with Node Attributes // CoRR. — 2014. — Vol. abs/1401.7267.
9. Чесноков В.О. Выделение пересекающихся сообществ в социальных графах по мажоритарному признаку соседей // «Ломоносов 2016»: XXIII Международная научная конференция студентов, аспирантов и молодых ученых; секция «Вычислительная математика и кибернетика». — М.: Издательский отдел факультета ВМиК МГУ; МАКС Пресс, 2016. — С. 49-51.

Научный руководитель: Ключарёв Петр Георгиевич, к.т.н., доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н.Э.Баумана, pgkl@yandex.ru

Detecting Sybils in Social Networking Services: An Ego-Network Analysis Approach

Chesnokov V.O.²³⁸

Online social networks have become an area for information warfare, so finding sources of misinformation and propaganda is an actual task. A new method for sybil detection in social networking services is proposed. It is based on analysis of user ego-network communities. Experiments on two datasets from LiveJournal social network with three community detection algorithms showed that a sybil can be distinguished from a legit user with high precision, recall and accuracy using a set of threshold rules.

Keywords: sybils, virtual users, ego-network, social graph, community detection, information warfare.

УДК 621.391

Метод защиты сообщений, передаваемых в оптико-электронных каналах

Чичварин Н.В.²³⁹

Рассмотрены вопросы безопасной передачи конфиденциальной документации по волоконно-оптическим и атмосферным линиям связи. Предлагается метод сокрытия данных, сочетающий стеганографическое маскирование сообщений в аудиофайлах с шифрованием ключа с помощью модифицированного протокола квантовой криптографии. На основе численных экспериментов проведен выбор алгоритма стеганографического сокрытия с закрытым ключом, передаваемым с применением модифицированного протокола квантовой криптографии.

Ключевые слова: атмосферная линия, безопасность, информация, криптография, кванты.

Сокращения:

АОЛС - атмосферная оптическая линия связи, (FSO - Free Space Optics)	НСД – несанкционированный доступ
ВОЛС – волоконно – оптическая линия	CAD/CAM – технологии автоматизированного проектирования
ИБ – информационная безопасность	CAD/CAM/PLM – технологии сопровождения объекта проектирования в период жизненного цикла

Введение

²³⁸ Vladislav Chesnokov, Bauman Moscow State Technical University, Moscow, v.o.chesnokov@yandex.ru

²³⁹ Чичварин Николай Викторович, к.т.н., доцент, МГТУ им. Н.Э. Баумана, г.Москва, genrih.gertz@gmail.com

Анализ характерных источников [1-6], что по сравнению с радиоэлектронными средствами, оптоэлектронные линии физически обеспечивают НСД в значительно большей степени. Развиваются методы модуляции и алгоритмы кодирования сигналов в ВОЛС и FSO. Большое внимание уделяется стеганографическим методам сокрытия в них конфиденциальных данных. Однако, поскольку известные и вновь разрабатываемые стеганографические методы [7,8] обладают меньшей криптоустойчивостью по сравнению с криптографическими, постоянно возникают потребности совершенствования криптостойких стеганографических алгоритмов. Одним из способов решения указанных задач представляется разработка метода, сочетающего простоту и доступность реализации стеганографических методов с преимуществами квантовой криптографии. Практическим применением таких методов могут являться системы CAD/CAM/PLM, когда часть проектной документации, составляющая коммерческую тайну, должна передаваться пооткрытым каналам связи [8]. Именно вопросам ИБ CAD/CAM/PLM уделяется основное внимание в настоящей публикации.

1. Результаты литературного обзора и патентного поиска. Постановка задачи

Анализ результатов обзора, приведенного в доступной литературе [7,8], позволяет утверждать, что для стеганографического сокрытия проектной документации в качестве контейнера предпочтительнее применение аудиофайлов. Для этого применяют стеганографические методы: широкополосное кодирование, фазовое кодирование, эхо-кодирование, метод замены шума, алгоритм «patchwork». В любом случае их применение требует наличия открытого, либо закрытого ключей. Для повышения криптоустойчивости требуется передача ключей синхронно со стегосообщением. Наиболее привлекательными для шифрования ключа представляется квантовое кодирование по протоколу BB84 [9,13] и его многочисленных модификаций [10 – 13]. Таким образом, задачей исследований, основные результаты которых приведены в настоящей публикации является разработка метода, сочетающего преимущества стеганографии и квантовой криптографии.

2. Существо предложения

Кодировать передаваемое сообщение предлагается следующими этапами:

2.1 Формируется цифровая Фурье – голограмма документа, математическая модель которой имеет вид [14]:

$$h(x, y) = \left[|w(x, y)| \exp\{j\Phi(x, y)\} + \exp\{j(xM + yN)\} \right]^2 = |w(x, y)|^2 + |w(x, y)| \cos[xM + yN + \Phi(x, y)] + 1. \quad (1)$$

где $w(x, y) = |w(x, y)| \exp(j\Phi(x, y))$ - преобразование Фурье изображения документа $W(u, v)$ в плоскости записи голограммы, $\exp\{j(xM + yN)\}$ - опорная когерентная волна $\exp\{j(xM + yN)\}$, где M и N – пространственные частоты, соответствующие углам падения волны по нормали к плоскости регистрации голограммы.

Первый член в выражении (1) характеризует дополнительную засветку голограммы пучком света от объекта и не содержит фазовой характеристики и не несет никакой информации о восстановленном изображении. Следовательно, получаем:

$$h(x, y) = A_0 + |w(x, y)| \cos[xM + yN + \Phi(x, y)], \quad (2)$$

где постоянная составляющая A_0 – максимальное значение $w(x, y) = w(0, 0)$. Значения M и N используются при восстановлении и представляют собой ключи шифрованному сообщению.

2.2 Голограмма записывается в аудиоконтейнер методом «patchwork». Псевдослучайные адреса размещения стего в контейнере составляют вторую группу ключей.

2.3 Передача стегосообщения производится по одной из мод ВОЛС. По другим модам передаются ключи, закодированные по протоколу BB84.

2.4 Декодирование сообщения производится в обратном порядке:

- расшифровка квантового кода ключей.
- восстановление Фурье – голограммы по алгоритму, обратному алгоритму формирования. Преобразование Фурье от полученной функции голограммы $h(x,y)$ будет состоять из суммы двух изображений водяного знака $W(u,v)$, смещенных относительно начала осей координат на величины несущих частот M и N :

$$\mathfrak{F}\{h(x,y)\} = \tilde{W}(u,v) = W(u-M, v-N) + W(-u-M, -v-N) + A(u,v), \quad (3)$$

где $\mathfrak{F}$ - оператор Фурье-преобразования, $A(u,v)$ – автокорреляционная функция. Автокорреляция $A(u,v)$ располагается в начале координат и подавляется как в цифровой голографии, так и в оптической. Второе изображение $W(-u-M, -v-N)$ является зеркальным отображением $W(u-M, v-N)$ относительно центра осей координат. При использовании Фурье-голограммы используется ее свойство избыточности, что позволяет использовать для последующего встраивания только часть массива, содержащего отсчеты цифровой голограммы.

Для кодирования ключей можно применить четыре квантовых состояния микросистемы, формирующие два сопряженных базиса (обозначенных здесь буквенными индексами А и В):

$$|0_A\rangle, |1_A\rangle, |0_B\rangle = \frac{1}{\sqrt{2}} (|0_A\rangle + |1_A\rangle), |1_B\rangle = \frac{1}{\sqrt{2}} (|0_A\rangle - |1_A\rangle). \quad (4)$$

Здесь состояния $|0_A\rangle$ и $|1_A\rangle$ кодируют значения "0" и "1" в базисе А, а $|0_B\rangle$ и $|1_B\rangle$ кодируют те же значения в базисе В. Можно представить их как поляризационные состояния фотонов. Тогда состояния $|0_A\rangle$ и $|1_A\rangle$ соответствуют горизонтальному (0°) и вертикальному (90°) направлениям поляризации, а $|0_B\rangle$ и $|1_B\rangle$ - двум диагональным, а именно $+45^\circ$ и -45° .

Заключение.

Предложенный метод позволяет получить технический эффект, не составляющий тривиальную сумму преимуществ стеганографического сокрытия сообщений и достоинств квантовой криптографии. Важно, что Фурье – голограмма избыточна и устойчива к искажениям [14]

Литература

1. Милинкус Б., Петров В. Атмосферная лазерная связь. Информост - Радиоэлектроника и Телекоммуникации №5(18), 2001.
2. Серопегин В.И. Беспроводные системы передачи данных локального, городского и регионального масштабов. Технология и средства связи, 1999, № 4, с. 72-77.
3. Гиносян Ю.А. Новые технологии беспроводного доступа. Технология и средства связи, 1999, № 4, с. 38-39.
4. Клоков А.В. Беспроводные ИК-технологии, истинное качество «последней мили». Технология и средства связи, 1999, № 5, с. 40-44.
5. Кулик Т. К., Прохоров Д.В. Методика сравнительной оценки работоспособности лазерных линий связи. Технология и средства связи, 2000, № 6, с. 8-18.

6. Кулик Т. К., Прохоров Д.В., Сумерин В. В., Хюппенен А. П. Особенности применения оптических линий связи. Лазер информ, 2001, вып. 9-10 (216-217), с. 1-6.
7. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая Стеганография. М.: СОЛОН-Пресс, 2002. – 272с.
8. Волосатова Т.М., Чичварин И.Н. Специфика информационной безопасности САПР// Известия высших учебных заведений. Машиностроение (специальный выпуск.) – 2012. С. 12 – 20.
9. Biham E., Boyer M., Brassard G., J. van de Graaf and Mor T. Security of Quantum Key Distribution against all Collective attacks. Quant-ph. 1998. 9801022.
10. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / Под ред. Д.Боумейстера, А. Экерта, А. Цайлингера; Пер. с англ. С.П.Кулика, Е.А.Шапиро. - М.: Постмаркет, 2002. - 375 с.
11. Clauser J.F. and Home M.A. Phys. Rev. 1974, D10, P.526.
12. G.Ribordy, J.-D.Gautier, N.Gisin, O.Guinnard and H.Zbinden. Electronics Letters. 1998. 34. P.2116-2117.
13. Bennett C.H., Brassard G. // Proceeding of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India. New York: IEEE, 1984. P.175.
14. Волосатова Т.М., Денисов А.В., Чичварин И.В. Комбинированные методы защиты данных в САПР». ИТ, Приложение. 2012.

The Method of Protection of Messages Transmitted in Optoelectronic Lines Chichvarin N.V.²⁴⁰

Abstract. *This paper considers the means of safe transmission of sensitive documentation transmission through optical fiber and free-space optics communication lines. It proposes a method of data concealing which combines a data masking of messages in audio files with a key encrypting using the modified Protocol of quantum cryptography. The choice of steganographic algorithm is bases on the result of a series of numerical experiments, private key in this case is transmitted with the use of a modified Protocol of quantum cryptography.*

Key words: *security, information, cryptography, quantum.*

²⁴⁰ Chichvarin N.V. Ph. D., Associate Professor, Bauman MSTU, Moscow, genrih.gertz@gmail.com

Формализация процесса функционирования безопасной подвижной интеллектуальной системы

Шевченко Т.Д.²⁴¹

В статье рассмотрена задача оценки надежности защиты подвижной ИС. Предоставлен обзор критериев анализа рисков и показателей, определяющих вероятность реализации угроз.

Ключевые слова: Информационная безопасность, автоматизированная система обнаружения и блокировки НСД, оценка рисков корпоративной ИС.

Введение

Задача оценки надёжности защитных механизмов подвижной ИС сводится к построению математической модели защиты ИС. В исследуемой ИС выявляются каналы передачи данных, рабочие места и другие сущ. средства, через которые возможно осуществить несанкционированный доступ (НСД) к защищаемой информации. В ИС должны существовать определенные средства и механизмы защиты, перекрывающие данные каналы НСД. Если же такие средства не используются или же используются как некая гипотетическая защита ИС, то защищённость данной ИС можно считать равной нулю [1].

Оценка безопасности функционирования ИС

Математическая модель защиты позволяет:

- Оценить надёжность каждого применяемого средства защиты;
- Получить итоговую оценку защищённости ИС.

Такие средства защиты как межсетевые экраны (firewall) тоже реализуют методику обнаружения и блокировки. Однако такое средство защиты нельзя рассматривать в рамках этой модели, т.к., во-первых, время обнаружения и блокировки одинаково, а во-вторых, данное средство можно обойти или нарушить его работоспособность. Таким образом, вероятность обнаружения и блокировки будет равна единице, если МСЭ работоспособен и его не смог обойти потенциальный нарушитель [2].

Для полного представления прочности преграды в виде автоматизированной системы обнаружения и блокировки НСД необходимо учесть надёжность её функционирования и пути возможного обхода её нарушителем [3, 5].

Вероятность отказа системы определяется по формуле:

$$P_{отк}(t) = e^{-\lambda t} \quad (1), \text{ где}$$

λ - интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки НСД;

t - рассматриваемый интервал времени функционирования системы обнаружения и блокировки НСД.

Таким образом, расчёт прочности преграды со свойствами обнаружения и блокировки, с учетом отказа системы контроля, можно производить по формуле:

$$P_{СЗИ} = P_{обл} \times (1 - P_{отк}) \times (1 - P_{обх1}) \times \dots \times (1 - P_{обхK}) \quad (2)$$

²⁴¹ Шевченко Тимофей Дмитриевич, МГТУ им. Н.Э. Баумана, г. Москва, tdshevchenko@gmail.com

$P_{обл}$ - вероятность обнаружения и блокировки НСД;

$P_{обх}$ - вероятность обхода j - й преграды;

$P_{обх}$ и количество путей обхода j определяется экспертным путём на основе анализа принципов построения системы контроля и блокировки НСД.

Под **риском** [4] в дальнейшем понимается ситуация, когда внешняя или внутренняя угроза использует уязвимости системы для нарушения её функционирования или совершения иных вредоносных действий.

Анализ рисков производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера.

Цель анализа рисков заключается в определении характеристик рисков корпоративной информационной системы и её ресурсов. Результаты анализа рисков используются в рамках мероприятий по экспертизе средств защиты как один из критериев оценки уровня защищённости системы.

При проведении анализа рисков учитываются следующие основные факторы:

- ценность программно-аппаратных и информационных ресурсов системы;
- значимость угроз и уязвимостей;
- эффективность существующих или планируемых средств обеспечения информационной безопасности.

Показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами (преимущественно для стоимостных характеристик), так и качественными (в частности, учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды).

Возможность реализации угрозы оценивается вероятностью её реализации в течение заданного отрезка времени для некоторого ресурса компании. При этом вероятность реализации угрозы определяется следующими основными показателями:

- привлекательность ресурса (показатель используется при рассмотрении угрозы от умышленного воздействия со стороны человека);
- возможность использования ресурса для получения дохода (также используется при рассмотрении угрозы от умышленного воздействия со стороны человека);
- технические возможности реализации угрозы;
- степень лёгкости реализации уязвимости.

Проведение анализа рисков позволяет:

- предметно описать состав и структуру информационной системы;
- расположить имеющиеся ресурсы по приоритетам, основываясь на степени их важности для полноценного функционирования Системы;
- оценить угрозы и идентифицировать уязвимости системы.

Методика проведения внутреннего анализа рисков не регламентируется и может быть выбрана локальным администратором информационной безопасности в соответствии с организационными особенностями подразделения и параметрами технических средств подсети. В качестве типовой может быть использована следующая методика.

Оценка вероятностей проявления угроз и возможных потерь производится администратором подсети как оценка потенциального ущерба в зависимости от заранее определённых коэффициентов.

Выводы

Представлена формула расчета прочности преграды с элементами обнаружения и блокировки. Описаны цели и критерии анализа рисков, показатели, влияющие на вероятность реализации угроз.

Литература

1. Медведев Н.В. Исследование процесса функционирования информационных каналов мобильных робототехнических комплексов. //Электромагнитные волны и электронные системы.- 2002.- № 8.-с. 29-36.
2. Медведев Н.В., Троицкий И.И. Приоритетное обслуживание в локальных вычислительных сетях. // Компьютер. – 2015. - №2. – с.39 – 45.
3. Wooldridge M., Jennings N. Intelligent Agents: Theory and Practice //Knowledge Engineering Review.– 2015.– V.10, №2.– P.75-82.
4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. — М.: Гелиос АРВ, 2013. — 480 с.
5. Reddy R. Epistemology of Knowledge Based Simulation //Simulation.– 2014.– V.48, №4.– P.147-162.

Научный руководитель: *Медведев Николай Викторович, к.т.н., доцент кафедры ИУ8 МГТУ им. Н.Э. Баумана*

Formalization of the Process of Safe Operation in Mobile Intelligent System

Shevchenko T. D.²⁴²

Is the problem of assessing the reliability of the protection of movable IS are considered. Criteria of risk analysis and the determinants of the probability of realization of threats are briefly touched upon.

Keywords: *Information security, automated system for detecting and blocking unauthorized access, risk assessment, corporate IS.*

УДК 004.056

Дополнительные меры защиты при работе с медицинскими информационными киосками

Чубатая А.²⁴³

В докладе обоснована необходимость дополнительных мер защиты данных для медицинских информационных киосков. Проведено исследование по работе с данной автоматизированной системой. Изучены известные биометрические методы идентификации людей и проведен сравнительный анализ среди них. Отобран оптимальный метод дополнительной биометрической аутентификации.

Ключевые слова: *медицинская информационно-аналитическая система, идентификация человека, биометрические методы*

Введение

С 2013 года происходит активный переход медицинских учреждений на Единую медицинскую информационно-аналитическую систему (ЕМИАС). Основная задача ЕМИАС - сделать использование бесплатных медицинских услуг доступнее, качественнее и удобнее для граждан, избавить медицинских работников от рутинной бумажной работы, а также дать им простой и удобный доступ к необходимой информации для оказания медицинской помощи [1-3].

²⁴² Shevchenko Timofey Dmitrievich, Moscow State Technical University, Moscow, tdshevchenko@gmail.com

²⁴³ Чубатая Анастасия, МГТУ им. Н.Э. Баумана, Москва, ForUchebaBmstu@yandex.ru

С введением ЕМИАС у пациента появилась возможность взаимодействия с медицинским учреждением посредством специального приложения на мобильных устройствах, через интернет или с помощью медицинского информационного киоска. Через интернет или приложение есть возможность записаться на прием к врачу или узконаправленному специалисту, следить за своими направлениями, а также отменить прием. Медицинский информационный киоск, в дополнение ко всем вышеперечисленным функциям, может осуществлять прикрепление пациента к конкретному медицинскому учреждению [4, 5].

Система ЕМИАС продолжает развиваться и в планах есть идеи введения других удобных и нужных нововведений через медицинский информационный киоск. Однако для их реализации будет недостаточно той защиты данных, которая реализована в данный момент.

Идентификация пациентов в системе

Идентификация пользователя в системе ЕМИАС (рис. 1) производится с помощью идентификационного документа (1), которым может являться:

- полис ОМС;
- полис ОМС нового образца;
- универсальная электронная карта;
- социальная карта москвича.

Идентификация происходит посредством считывания штрих-кода с идентификационного документа считывающим устройством (2). При успешном прохождении этого процесса пациенту будет предложен ряд возможных последующих действий (3).

Например, в настоящее время с помощью медицинских информационных киосков можно производить запись к врачам, выбирать удобное время и нужного специалиста, прикрепиться к медицинскому учреждению, распечатать талоны на прием и т.д. Для данных функций вполне хватает идентификации пациента по полису.



Рис. 1. Идентификация пациента в системе

Обоснование дополнительных мер защиты

Для введения новых функций, которые ускорили и упростили бы процедуру получения некоторых услуг (например, получение направления на анализы, получение рецепта на лекарства и т.д.), данной идентификации будет недостаточно [6-8].

Одним из вариантов решения данной проблемы является двухфакторная аутентификация, первым фактором которой также останется медицинский полис, а вторым фактором будет являться биометрическая аутентификация [9].

Рассмотрим различные методы (табл. 1).

Таблица 1.

Надежность биометрических методов

Характеристика/метод	Отпечаток пальца	Распознавание лица 2D	Распознавание лица 3D	Сетчатка глаза	Рисунок вен
FAR	0,001%	0,1%	0,0005%	0,0001%	0,0008%
FRR	0,6%	2,5%	0,1%	0,4%	0,01%
Фальсификация	Возможна	Возможна	Проблематична	Невозможна	Невозможна
Неизменность характеристики	Низкая	Низкая	Высокая	Средняя	Средняя
Скорость аутентификации	Высокая	Средняя	Низкая	Низкая	Высокая
Бесконтактная аутентификация во время движения	Безуспешно	На большом расстоянии	На среднем расстоянии	Невозможно	На маленьком расстоянии

Проведя сравнение биометрических методов, выбор можно остановить на двух методах - аутентификации по сетчатке глаза и по венам (табл. 2).

Таблица 2.

Критерии выбора биометрического метода

Критерии выбора	Сетчатка глаза	Рисунок вен
Комфорт пользователя	Низкий	Средний
Стоимость	Высокая	Средняя
Доступность на российском рынке	Низкая	Высокая

Сравнивая эти два метода между собой, можно сделать вывод, что биометрическая аутентификация по венам является более подходящей исходя из характеристик комфорта, стоимости и доступности.

Выводы

В ходе выполнения работы были исследованы особенности медицинских информационных киосков системы ЕМИАС. Были изучены различные биометрические методы, и на основе их характеристик проведен сравнительный анализ и отобран наиболее оптимальный метод аутентификации, которым оказался метод аутентификации по венам.

Литература

1. Концептуальная модель виртуального центра охраны здоровья населения / В.С. Анищенко, Т.И. Булдакова, П.Я. Довгалецкий и др. // Информационные технологии. 2009. №12. С. 59-64.
2. Гусев А.В. Обзор электронных регистратур // Врач и информационные технологии. 2010. № 6. С. 4-15.
3. Троицкая Н. Л. Социально-экономическая модель здравоохранения современной России // Вестник Томского государственного университета. 2009. № 327 (окт.). С. 171-174.

4. Ланцберг А.В., Тройч К., Булдакова Т.И. Развитие системы электронных услуг муниципальной поликлиники (на основе анализа зарубежных web-ресурсов) // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2011. № 4. С. 1-7.
5. Ланцберг А.В., Тройч К., Булдакова Т.И. Особенности оценки качества медицинской электронной услуги // Информационное общество. 2011. № 4. С. 28-37.
6. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2). С. 28-35.
7. Булдакова Т.И., Суятинов С.И., Миков Д.А. Анализ информационных рисков виртуальных инфраструктур здравоохранения // Информационное общество. 2013. № 4. С. 6.
8. Булдакова Т.И., Кривошеева Д.А. Угрозы безопасности в системах дистанционного мониторинга // Вопросы кибербезопасности. 2015. № 5. С. 45-50.
9. Система телемедицины с предварительным шифрованием биометрической информации / Ю.Г. Горшков, А.М. Каиндин, А.С. Веряев, Е.Л. Зорин, А.С. Марков, В.Л. Цирлов // Вопросы кибербезопасности. 2015. № 5 (13). С. 63-69.

Научный руководитель: Булдакова Татьяна Ивановна, доктор технических наук, профессор, МГТУ им. Н.Э. Баумана, buldakova@bmstu.ru

Additional Measures of Protection During the Work with Medical Interactive Kiosk

Chubataja A.²⁴⁴

In the report need of additional measures of protection of data for medical information kiosks is proved. The research on work with this automated system is conducted. The known biometric methods of identification of people are studied and the comparative analysis among them is carried out. The optimum method of additional biometric authentication is selected.

Keyword: medical information and analytical system, identification of the person, biometric methods

²⁴⁴ Chubataja Anastasia, Bauman Moscow State Technical University, Moscow, ForUchebaBmstu@yandex.ru

Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем

Чукляев И.И.²⁴⁵

Исследование выполнено при поддержке РФФИ в рамках научного проекта № 13-07-97518 и гранта Президента Российской Федерации № МК-3603.2014.10

В статье уточнен понятийно-терминологический аппарат управления рисками информационной безопасности, представлено описание разработанного метода и реализующих его моделей для комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем. Предлагаемый подход позволяет детализировать информационно-управляющие системы относительно функциональной, информационной, организационной и технической подсистем; сформировать функционально-ориентированные информационные ресурсы, структура которых содержит многоаспектную информацию для выполнения всей совокупности задач управления информационно-управляющими системами; расширить возможности по созданию перспективных средств защиты, ориентированных на комплексную защиту выполнения задач с учетом уровней управления систем.²⁴⁶

Ключевые слова: сложная организационно-техническая система, функционально-ориентированные информационные ресурсы, риск-событие, риск-ситуация нарушения защищенности.

Введение

Интеграция информационно-телекоммуникационных технологий в информационно-управляющих системах (ИУС) актуализирует вопросы обеспечения их защищенности от несанкционированных внешних и/или внутренних воздействий дестабилизирующего характера (НСВ), заключающихся в разрушении, повреждении компонентов, модификации (искажении) данных [1, 2], ведущих к нарушению выполнения задач управления.

В настоящее время предложены разнообразные методы и средства обеспечения защищенности ИУС и циркулирующих данных в условиях НСВ. Однако, как правило, они «локализованы» относительно отдельных совокупностей данных и процессов и не ориентированы на комплексную защиту выполнения задач с учетом уровней управления ИУС и комплексное управление рисками нарушения их защищенности [1].

Актуальность

Риск является неизбежным, сопутствующим фактором функционирования и развития любой сложной системы или процесса. Управление рисками представляет собой одну из основных современных концепций управления сложными организационно-техническими системами (ОТС) [1, 3, 4].

Понятийно-терминологический аппарат

Существующий понятийно-терминологический аппарат, применяемый при формализации процессов выполнения задач с учетом уровней управления и комплексного управления рисками нарушения защищенности сложных ОТС, является разобщенным, допускает различную трактовку, характеризуется слабой связанностью и требует уточнения.

Исходя из этого, информационно-управляющую систему предлагается рассматривать как функциональную, информационную, организационную и техническую подсистемы. Компоненты этих подсистем распределены по уровням управления ИУС (табл.1) [5-7].

²⁴⁵ Чукляев Илья Игоревич, кандидат технических наук, доцент, Военная академия войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А.М.Василевского, г. Смоленск, smolarm@pochta.ru

²⁴⁶ *Исследование выполнено при поддержке РФФИ в рамках научного проекта № 13-07-97518 и гранта Президента Российской Федерации № МК-3603.2014.10*

Таблица 1.

Пример распределения компонентов подсистем
информационно-управляющей системы на смежных уровнях управления

Уровни управления ИУС	Подсистемы ИУС			
	Функцио- нальная	Информа- ционная	Организа- ционная	Техническая
ИУС	Задачи управления <Функция>	Информационные потoki данных <IR>	Должностные лица (ДЛ) <ДЛ>	Техническая основа <Механизм>
Уровень A_i	Задачи управления, реализуемые ДЛ <Функция ¹ _{nm} >	Информационные потoki <IR>, <Вход Функция ¹ _{nm} >, <Управление Функция ¹ _{nm} >, <Вызов Функция ¹ _{nm} >, <Выход Функция ¹ _{nm} >	Должностные лица органов управления <ДЛ _{bc} >	Средства автоматизации <СрАвт>
Уровень A_j	Задачи управления, реализуемые устройствами (аппаратурой) <Функция ³ _{nmkl} >	Показатели структуры <N _{IR} > информационных потокoв данных, <Вход Функция ³ _{nmkl} >, <Управление Функция ³ _{nmkl} >, <Вызов Функция ³ _{nmkl} >, <Выход Функция ³ _{nmkl} >	Действия ДЛ <ДЛ _{bcd} >	Устройства (аппаратура) <Устройства>

Предлагаемая структура функционально-ориентированных информационных ресурсов (ФОИР) ИУС содержит многоаспектную информацию для выполнения всей совокупности задач управления ИУС и представляются в виде [5, 6]:

$$\text{ФОИР}_{\text{ИУС}} = \{ \text{ФОИР}_{A_i} \} \triangleright \triangleleft \{ \text{IR} \} \triangleright \triangleleft \{ \text{Функция} \} \triangleright \triangleleft \{ \text{Право} \} \triangleright \triangleleft \{ \text{ДЛ} \} \triangleright \triangleleft \{ \text{Механизм} \} \triangleright \triangleleft \{ \text{Взаимосвязи} \} \triangleright \triangleleft \{ \text{Свойства} \} \triangleright \triangleleft \{ \text{Временные параметры} \}; \quad (1)$$

Функционально-ориентированные информационные ресурсы для решения задач i -го уровня управления:

$$\begin{aligned} \text{ФОИР}_{A_i} = \{ \text{ФОИР}_{A_j} \} \triangleright \triangleleft \{ \text{Вход Функция}^1_{nm} \} \triangleright \triangleleft \{ \text{Управление Функция}^1_{nm} \} \triangleright \triangleleft \{ \text{Вызов Функция}^1_{nm} \} \triangleright \triangleleft \\ \triangleright \triangleleft \{ \text{Выход Функция}^1_{nm} \} \triangleright \triangleleft \{ \text{Функция}^1_{nm} \} \triangleright \triangleleft \{ \text{Право} \} \triangleright \triangleleft \{ \text{ДЛ}_{bc} \} \triangleright \triangleleft \{ \text{СрАвт} \} \triangleright \triangleleft \\ \triangleright \triangleleft \{ \text{Взаимосвязи} \} \triangleright \triangleleft \{ \text{Свойства} \} \triangleright \triangleleft \{ \text{Временные параметры} \}; \end{aligned} \quad (2)$$

Функционально-ориентированные информационные ресурсы для решения задач j -го уровня управления:

$$\begin{aligned} \text{ФОИР}_{A_j} = \{ N_{IR} \} \triangleright \triangleleft \{ \text{Функция}^3_{nmkl} \} \triangleright \triangleleft \{ \text{Право} \} \triangleright \triangleleft \{ \text{ДЛ}_{bcd} \} \triangleright \triangleleft \{ \text{Устройства} \} \triangleright \triangleleft \\ \triangleright \triangleleft \{ \text{Взаимосвязи} \} \triangleright \triangleleft \{ \text{Свойства} \} \triangleright \triangleleft \{ \text{Временные параметры} \}, \end{aligned} \quad (3)$$

где: $\{ \text{ФОИР}_{\text{ИУС}} \}$, $\{ \text{ФОИР}_{A_i} \}$, $\{ \text{ФОИР}_{A_j} \}$ – функционально-ориентированные информационные ресурсы ИУС соответствующих уровней управления, $\{ \text{Взаимосвязи} \}$ – взаимосвязи функционально-ориентированных информационных ресурсов ИУС соответствующих уровней управления, $\{ \text{Свойства} \}$ – свойства защищенности, предъявляемые к функционально-ориентированным информационным ресурсам ИУС соответствующих уровней управления, $\{ \text{Временные параметры} \}$ – временные параметры, $\triangleright \triangleleft$ – операция агрегирования, характеризующая объединение и укрупнение показателей функционально-ориентированных информационных ресурсов ИУС соответствующих уровней управления.

Риски нарушения защищенности ФОИР ИУС предлагается рассматривать как совокупность источников риск-событий SR , риск-событий RE , риск-ситуаций RS нарушения защищенности ФОИР ИУС и взаимосвязей Con между ними (рис.1) [1, 3].

Источник риск-события нарушения защищенности ФОИР ИУС – элемент функциональной, информационной, организационной и технической подсистем ФОИР ИУС, на которые направлены угрозы применения НСВ, порождающие риск-события нарушения защищенности ФОИР ИУС.

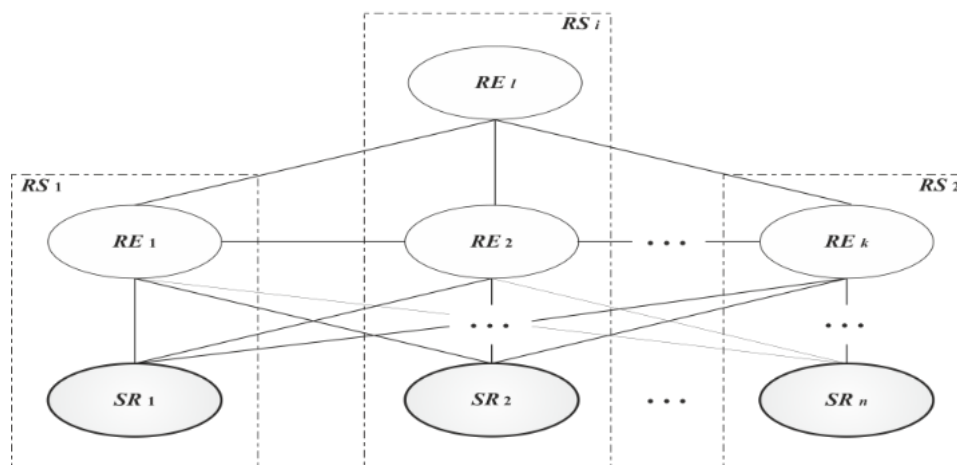


Рис.1. Графическое представление источников риск-событий SR, риск-событий RE и риск-ситуаций RS нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющей системы

Риск-событие нарушения защищенности ФОИР ИУС – событие, наступление которого может привести к нарушению защищенности ФОИР ИУС.

Риск-ситуация нарушения защищенности ФОИР ИУС – совокупность обусловленных причинно-следственными связями источников риск-событий и риск-событий нарушения защищенности ФОИР ИУС.

Таким образом, предлагаемый аспект рассмотрения рисков нарушения защищенности ФОИР ИУС детализируется понятиями «источник риск-события», «риск-событие» и «риск-ситуация» нарушения защищенности ФОИР ИУС.

Данное уточнение позволяет дифференцировано охарактеризовать как причины возникновения рисков, в том числе и единичного, последствия, так и мероприятия, направленные на устранение результатов возникновения рисков нарушения защищенности ФОИР ИУС, а также принадлежность традиционно «приписываемых» характеристик к следующим понятиям: «уровень риска», «событие», «существенность», «категория» и «приемлемость», «мероприятие». «уровень последствия».

Постановка задачи

Формализованное описание комплексного управления рисками нарушения защищенности ФОИР ИУС представляется в виде [1, 3, 7-13]:

$$Z_{\text{ФОИР ИУС}}(Q_k, V_k) \xrightarrow{\tilde{P}_k} V_k \max ; \quad (4)$$

$$\text{Risk}_{\text{ФОИР ИУС}} = f(Z_{\text{ФОИР ИУС}}), \quad (5)$$

где: $Z_{\text{ФОИР ИУС}}$ – защищенность функции управления верхнего уровня функционально-ориентированных информационных ресурсов ИУС, Q_k – смешанные оптимальные стратегии угроз применения НСВ нарушения защищенности функционально-ориентированных информационных ресурсов ИУС,

V_k – оптимальный риск нарушения защищенности функционально-ориентированных информационных ресурсов ИУС при взаимном применении сторонами смешанных оптимальных стратегий (P_k и Q_k), $\tilde{P}_k$ – классы мероприятий (оптимальные смешанные стратегии) управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов

ИУС, $Risk_{FOIP\ ИУС}$ – риск нарушения защищенности функции управления верхнего уровня функционально-ориентированных информационных ресурсов ИУС.

Гибридная нечеткая модель комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем

Процессы управления рисками (рис.2) регламентированы руководящими документами [1, 3, 14] и определяют реализацию следующих этапов (подпроцессов):

анализ и мониторинг;

обмен информацией и консультации;

управление рисками: определение контекста, оценка рисков (идентификация рисков, анализ рисков, оценивание рисков) и обработка рисков.

Разработанный метод комплексного управления рисками нарушения защищенности ФОИР ИУС основан на гибридной нечеткой модели комплексного управления рисками нарушения защищенности ФОИР ИУС.

В работе разработана диаграмма, иллюстрирующая взаимосвязи созданной нечеткой гибридной модели комплексного управления рисками нарушения защищенности ФОИР ИУС и структуры составляющих ее нечетких моделей, направленных на реализацию метода комплексного управления рисками нарушения защищенности ФОИР ИУС [1, 3, 7-13].

Формализованное описание гибридной нечеткой модели комплексного управления рисками нарушения защищенности ФОИР ИУС представляется в виде [1, 3]:

$$\left\{ \begin{array}{l} SR, RE, RS, Con \\ Risk_{SR}, Risk_{RE}, Risk_{RS}, Con, Oper \\ A_k, a_{ij}^k, p_m^k, q_m^k, P_k, Q_k, \alpha, \beta, V_k \\ V_k, P_k \end{array} \right\} \rightarrow q_m^k, Q_k, \tilde{P}_k, \quad (6)$$

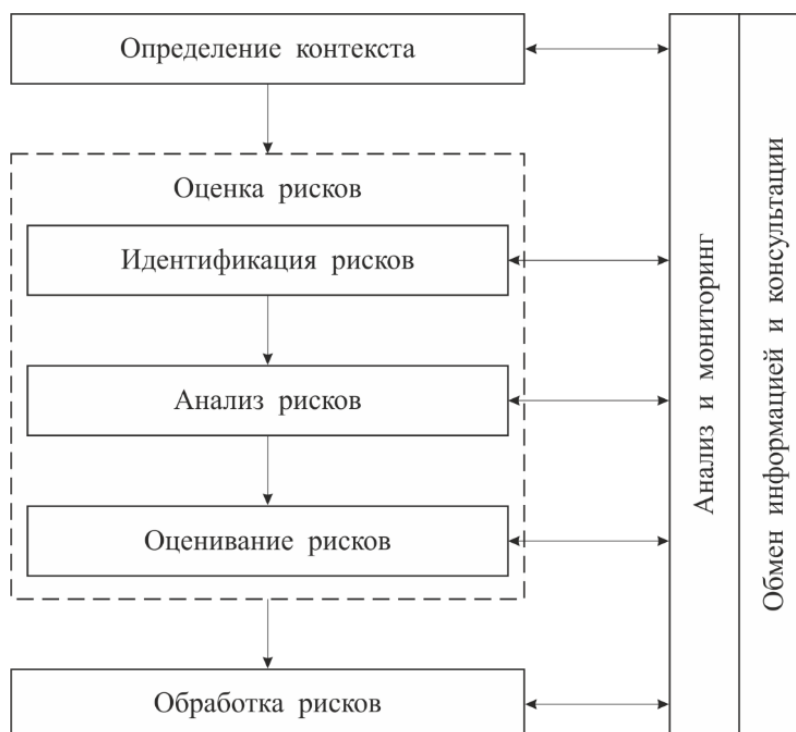


Рис.2. Графическое представление процессов управления рисками

где: $Risk_{SR}$, $Risk_{RE}$, $Risk_{RS}$ – значения рисков источников риск-событий, риск-событий и риск-ситуаций ФОИР ИУС, $Oper$ – логические Т-операции t -нормы («И») или min-конъюнкции между источниками риск-событий и риск-событиями нарушения защищенности ФОИР ИУС, A_k – матрица рисков нарушения защищенности ФОИР ИУС, a_{ij}^k – элементы матрицы рисков A_k нарушения защищенности ФОИР ИУС, p_m^k – чистые стратегии применения мероприятий управления рисками нарушения защищенности ФОИР ИУС, q_m^k – чистые стратегии угроз применения НСВ нарушения защищенности ФОИР ИУС, α – допустимые значения уровней рисков нарушения защищенности ФОИР ИУС, β – критические β значения уровней рисков нарушения защищенности ФОИР ИУС.

Выводы

Предлагаемые метод и модели комплексного управления рисками нарушения защищенности ФОИР ИУС обеспечивают расширенные возможности по созданию перспективных средств защиты, ориентированных на комплексную защиту выполнения задач с учетом уровней управления ОТС.

Литература

1. Чукляев И.И. Метод и модели комплексного управления рисками нарушения защищенности информационно-управляющих систем. Монография. Смоленск: ВА ВПВО ВС РФ. 2015. 141 с.
2. Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.
3. Чукляев И.И. Управление рисками защищенности распределенных информационно-вычислительных систем // Системы компьютерной математики и их приложения. 2015. № 16. С. 110-112.
4. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. Монография // Москва, 2012. 284 с.
5. Чукляев И.И. Функционально-ориентированные ресурсы. База данных информационно-управляющей системы. Монография. Смоленск: ВА ВПВО ВС РФ. 2015. 114 с.
6. Чукляев И.И. Композиционная модель и способ построения функционально-ориентированных информационных ресурсов информационно-управляющих систем // Труды ИСП РАН, 2016, том 28, выпуск 2, с. 259-270.
7. Чукляев И.И. Система комплексной защиты функционально-ориентированных информационных ресурсов информационно-управляющих систем // Системы компьютерной математики и их приложения. 2016. № 17. С. 85-88.
8. Чукляев И.И. Игровая модель обоснования применения средств комплексной защиты информационных ресурсов иерархической информационно-управляющей системы // Т-Comm: Телекоммуникации и транспорт. – 2015. – №2. – С. 64-68.
9. Чукляев И.И. Нечеткая оценка взаимосвязей системных факторов информационно-управляющей системы в интересах повышения защищенности информационных ресурсов // Системы управления, связи и безопасности. 2015. №1. С. 4-15.
10. Чукляев И.И. Методика построения и нечеткая модель оценки защищенности и выбора классов мероприятий по минимизации рисков на основе нейронечеткого классификатора // Известия Смоленского государственного университета. 2015. № 2-1. С. 312-319.
11. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.
12. Чукляев И.И. Анализ уязвимостей в исходных кодах программного обеспечения статическими и динамическими методами // В сборнике: XII всероссийское совещание по проблемам управления ВСПУ-2014 Институт проблем управления им. В.А. Трапезникова РАН. 2014. С. 9232-9242.
13. Чукляев И.И. Оценка уязвимостей программного обеспечения информационно-управляющих систем различного назначения методами обратной инженерии // В сборнике: Кибернетика и высокие технологии XXI века XV Международная научно-техническая конференция. НПФ «САКВОЕЕ» ООО. 2014. С. 230-237.
14. Бутусов И.В., Нащекин П.А., Романов А.А. Теоретико-семантические аспекты организации комплексной системы защиты информационных систем // Вопросы кибербезопасности. 2016. № 1 (14). С. 9-16.

Научный консультант: Борисов Вадим Владимирович, доктор технических наук, профессор, профессор кафедры Национального исследовательского университета «МЭИ» в г. Смоленске, г. Смоленск, vadim.v.borisov@mail.ru.

**Methodical Providing Complex Management of Risks of Informational Security of
Function-Oriented Information Resources Management Information Systems**
Chucklyaev I.I.²⁴⁷

In article the conceptual framework of risk management of information security is specified. The description of the developed method and models realizing it for complex management of risks of informational security of function-oriented information resources of management information systems is provided. The developed methodical approach allows to detail management information systems of rather functional, information, organizational and technical subsystems and to create function-oriented information resources which structure contains multiaspect information for execution of set of tasks of control of management information systems.

Keywords: organizational and technical system, function-oriented information resources, risk management of information security.

²⁴⁷ Ilya Chucklyaev, Ph.D., Associate Professor, Marshal of the Soviet Union A.M.Vasilevsky Army Air Defense Military Academy, Smolensk, smolarm@pochta.ru

**Применение метода контурного анализа для аутентификации по рисунку
кровеносных сосудов**
Щербакова Д.П.²⁴⁸

***Аннотация.** В статье рассмотрена работа системы биометрической аутентификации. Рассмотрены уязвимости биометрических систем и требования к защищенности биометрического шаблона. Рассмотрена возможность применения метода контурного анализа для распознавания рисунка кровеносных сосудов. Приведена блок-схема алгоритма распознавания рисунка кровеносных сосудов. Перечислены преимущества метода контурного анализа.*

***Ключевые слова:** двухфакторная аутентификация, биометрия, контурный анализ, рисунок кровеносных сосудов.*

Введение. На сегодняшний день существует множество разных технологий биометрической аутентификации человека. Это обусловлено тем, что интерес к ним растет, и область их применения расширяется. Одной из таких технологий является аутентификация по рисунку кровеносных сосудов. Эта технология обладает высокой надежностью, поскольку кровеносные сосуды находятся внутри организма и имеют множество различных черт, благодаря чему нашла свое применение в банковской сфере [1]. Данная технология требует использования алгоритма сравнения образа, полученного от считывателя, с эталонным образом. В основе такого алгоритма может лежать метод контурного анализа. Метод контурного анализа уже используется с целью идентификации личности, к примеру, выделение радужной оболочки глаза [2] или нахождение меры сходства кистей рук [3]. В ходе исследований метод показал высокую производительность и качество идентификации.

Работа системы аутентификации по рисунку кровеносных сосудов. На этапе регистрации ИК-сканер облучает ладонь в ближнем инфракрасном диапазоне и считывает рисунок кровеносных сосудов, которые теплее окружающих их тканей за счет крови, приходящей из сердца. Затем из биометрического образца извлекаются индивидуальные черты – контуры рисунка кровеносных сосудов и узловые точки. Данные индивидуальные черты называются шаблонами. Биометрическая система сохраняет полученный шаблон в базе данных вместе с другими идентификаторами, такими как имя, идентификационный номер. Во время аутентификации ладонь пользователя сканируется повторно. Из полученного образца извлекаются черты, которые служат запросом для сравнения с шаблоном заявленной личности с помощью алгоритма сопоставления. Система возвращает рейтинг соответствия, отражающий степень схожести между шаблоном и запросом. Система принимает запрос, только если рейтинг соответствия превышает заранее заданный порог.

Уязвимости биометрических систем

Биометрическая система уязвима для ошибок двух видов (рис.1). Когда система не распознает легитимного пользователя, происходит отказ в обслуживании, а когда злоумышленник неверно идентифицируется в качестве авторизованного пользователя, говорят о вторжении. Для таких сбоев существует масса возможных причин, их можно поделить на естественные ограничения и атаки злоумышленников [4].

²⁴⁸ Щербакова Д.П., АО «НПО «Эшелон», г. Москва, d.scherbakova@npo-echelon.ru

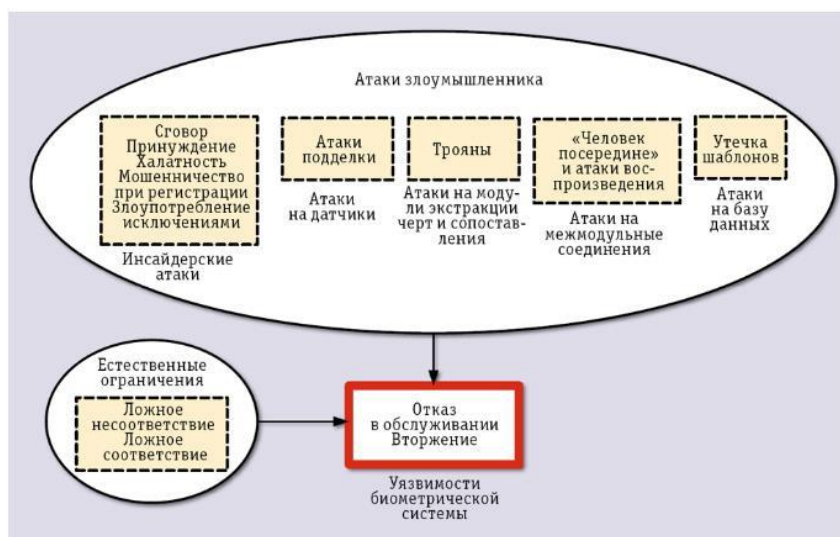


Рис. 1. Уязвимости биометрической системы

Требования к защищенности шаблона. Основная трудность при разработке схем защиты биометрического шаблона состоит в том, чтобы достигнуть приемлемого компромисса между тремя требованиями.

Необратимость. Злоумышленнику должно быть затруднительно вычислительным путем восстановить биометрические черты из сохраненного шаблона, либо создать физические подделки биометрического признака.

Различимость. Схема защиты шаблона не должна ухудшать точность аутентификации биометрической системой.

Отменяемость. Должна быть возможность из одних и тех же биометрических данных создать несколько защищенных шаблонов, которые нельзя будет связать с этими данными. Это свойство не только позволяет биометрической системе отзывать и выдавать новые биометрические шаблоны в случае компрометации базы данных, но и предотвращает перекрестное сопоставление между базами данных, за счет чего сохраняется приватность данных о пользователе.

Распознавания узловых точек кровеносных сосудов методом контурного анализа. Контурный анализ позволяет описывать, хранить, сравнивать и производить поиск объектов, представленных в виде своих внешних очертаний – контуров, а также эффективно решать основные проблемы распознавания образов – перенос, поворот и изменение масштаба изображения образа.

В контурном анализе контур кодируется последовательностью, состоящей из комплексных чисел. На контуре фиксируется точка, которая называется начальной. Затем контур обходится (например, по направлению движения часовой стрелки), и каждый вектор смещения записывается комплексным числом

$$a + ib, \quad (1)$$

где a – смещение точки по оси x ; b – то же по оси y .

Смещение берется относительно предыдущей точки (рис.2) [5].



Рис.2. Кодирование контура

Проиллюстрируем применение метода контурного анализа [6] на примере распознавания узловых точек кровеносных сосудов.

1. *Этап предварительной обработки.* На этапе предварительной обработки выполняется подавление шума. Происходит выделение основных признаков изображения – очертания кровеносных сосудов. После этого выделяются узловые точки – точки пересечений контуров кровеносных сосудов. Результатом является точечная сцена $s_{эт}(x, y)$ и массив координат обнаруженных узловых точек $\{(x_i, y_i)\}_{1,N}$.

2. *Этап выделения группы узловых точек.* Оператор выделения группы узловых точек осуществляет локализацию группы точек. Результатом этой процедуры является множество точек Q_m с числом, не меньшим заданного N_{min} .

3. *Этап формирования ассоциированного сплошного образа (АСО) группы узловых точек.* Оператор формирования изображения АСО реализует алгоритм расфокусировки точечного изображения и формирует на своем выходе изображение АСО $h_m(x, y)$.

4. *Этап выделения контуров АСО группы узловых точек.* Следующий оператор осуществляет выделение контура АСО на изображении с помощью алгоритма Розенфельда и формирует цепной стандартный комплекснозначный код контура $\Gamma_{мст}$. Здесь же осуществляется приведение стандартного кода контура случайной размерности k_m к коду фиксированной размерности k (эквализация) и, как следствие, переход к произвольному коду контура Γ_m . Произвольный контур Γ_m , состоящий из элементарных векторов, запишем как элемент k -мерного комплексного векторного пространства C^k :

$$\Gamma_m = \{\gamma(n)\}_{0,k-1} = \{\gamma(0), \gamma(1), \dots, \gamma(k-1)\}, \quad (2)$$

где $\gamma(n)$ – элементарный вектор, $n = 0, 1, \dots, k-1$.

5. *Этап идентификации контуров группы узловых точек.* Оператор идентификации контура группы узловых точек предназначен для идентификации контуров АСО. Результатом работы оператора служит идентификатор H_j , присваиваемый контуру группы узловых точек m : $(Q_m \leftrightarrow H_j)$.

6. *Этап предварительной идентификации узловых точек в контуре.* Оператор предварительной идентификации узловых точек производит идентификацию узловых точек в контуре. Работа оператора заканчивается присвоением номерам i обнаруженных узловых точек идентификаторов N_i эталонных узловых точек из каталога: $(i \leftrightarrow N_i)$, $i \in Q_m$.

7. *Этап совмещения контуров АСО.* Оператор совмещения контуров АСО выполняет совмещение полученного от считывателя образа с опознанным АСО группы узловых точек и эталонного образа с одноименным эталонным АСО. Совмещение осуществляется путем совмещения центров тяжести контуров АСО и поворота одного из кадров на угол, равный

полученной оценке $\Delta \varphi$ при распознавании. В качестве меры сходства, таких контуров предложено использовать нормированное скалярное произведение контуров:

$$\eta_{C^k} = \frac{(\Gamma, N)_{C^k}}{\|\Gamma\| \|N\|}, \quad (3)$$

где скалярное произведение контуров и норма определены стандартным для пространства C^k способом.

8. *Этап идентификации множества обнаруженных узловых точек.* Оператор идентификации узловых точек с учетом полученной предварительной оценки ориентации реализует окончательную идентификацию всех узловых точек образа по критерию ближайшего соседства: $\{(i \Leftrightarrow N_i)\}_{1, N_{min}}$.

Укрупненная блок-схема алгоритма представлена на рис.3.



Рис.3. Укрупненная блок-схема алгоритма распознавания

Выводы.

Применение метода контурного анализа открывает перед собой большие перспективы для дальнейших исследований в области биометрической аутентификации. Созданный алгоритм обработки биометрических образов может быть с успехом применен в различных отраслях деятельности человека.

Основными достоинствами рассмотренного подхода к распознаванию группы узловых точек являются:

1. низкая трудоемкость за счет малой размерности описания (обычно не более 100), а также инвариантности алгоритма распознавания к масштабу и угловой скорости ориентации образа;
2. надежность принимаемых решений по совокупности признаков остается в рамках

значений, представляющих практический интерес, т.е. не хуже 0,9 – 0,95 в диапазоне интенсивных ложных отметок до $1,57 \cdot 10^{-3}$, что подтверждается расчетными и эмпирическими, полученными статистическим моделированием, характеристиками алгоритмов.

Литература

1. Дремин А. Биометрические технологии по рисунку вен ладони. решения для банков // Алгоритм безопасности. 2015. № 3. С. 52-54. URL: http://www.algoritm.org/arch/15_3/15_3_20.pdf.
2. Харитонов А.В. Выделение радужной оболочки глаза с использованием контурного анализа // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. 2014. № 1 (20). С. 62-67. URL: <http://elibrary.ru/download/59976479.pdf>.
3. Басараб М.А., Кондрашов К.В. Моделирование геометрии кисти руки методом R-функций в задачах биометрии // Инженерный журнал: наука и инновации. 2012. № 3 (3). С. 40. URL: <http://engjournal.ru/articles/131/131.pdf>.
4. Jain, A. K., & Nandakumar, K. Biometric authentication: System security and user privacy. Computer, 45(11), 2012, pp. 87-92. [6353458]. DOI: 10.1109/MC.2012.364.
5. Сакович И.О., Белов Ю.С. Обзор основных методов контурного анализа для выделения контуров движущихся объектов // Инженерный журнал: наука и инновации. 2014. № 12 (36). С. 11. URL: <http://engjournal.ru/articles/1280/1280.pdf>.
6. Фурман Я.А. Введение в контурный анализ; приложения к обработке изображений и сигналов / Я.А. Фурман, А.В. Кревецкий, А.К. Передреев и др. – М.: ФИЗМАТЛИТ, 2003. – 588 с.

***Научный руководитель** – Басараб Михаил Алексеевич, профессор, доктор физико-математических наук, профессор кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н.Э. Баумана, m.basarab@bmstu.net*

Application of the Contour Analysis Method to the Pattern of Blood Vessels Authentication **Shcherbakova D.²⁴⁹**

The article describes the system for biometric authentication. Considered the vulnerabilities of biometric systems and the requirements for security a biometric template. Considered the applicability of the contour analysis method for the recognition of the pattern of blood vessels. Showed the block diagram of the recognition algorithm of the pattern of blood vessels. The advantages of the contour analysis method were listed.

Keyword: two-factor authentication, biometrics, contour analysis, pattern of blood vessels.

²⁴⁹ Dariya Scherbakova, NPO Echelon, d.scherbakova@npo-echelon.ru

Экспериментальное использование сетевой системы IDS SNORT по обнаружению сетевых атак

Юшкевич А.С.²⁵⁰

На конкретных примерах показан процесс разработки конфигураций правил для сетевой системы обнаружения вторжений - IDS Snort. Рассматриваемые в качестве примера блоки правил успешно проходят тестирование на созданном виртуальном стенде, выполняя все поставленные задачи и достигая установленные для каждого правила цели. Сформированные правила позволяют эффективно отследить и заблокировать потенциальные сетевые угрозы, а так же оповестить о них администратора сети.

Ключевые слова: информационная безопасность, сетевые системы обнаружения вторжений, открытый программный инструмент, конфигурация правил, идентификация угроз.

Введение

В современном мире информация представляет значительную ценность для общества, а значит остро стоит вопрос о её защите. На данный момент существуют аппаратные и программные средства защиты. При всех преимуществах аппаратных устройств, программные средства так же позволяют эффективно обнаруживать вторжение, а так же могут оповестить об этом сетевого администратора и устранить или пресечь вредоносные действия злоумышленника или вредоносного программного обеспечения.

Рассматривая защиту информации в компьютерных сетях, хочется обратить внимание на системы обнаружения вторжений (COB) или Intrusion Detection System (IDS). Располагаясь в локальных сетях предприятий, данные системы могут обеспечить отслеживание вторжений внутри сети и вести наблюдение сразу за несколькими хостами. Данные системы производят в режиме реального времени, мониторинг внутрисетевого трафика на предмет соответствия происходящих процессов заранее определённым правилам. В базе данных хранятся признаки и описываются сигнатуры возможных атак, а так же устанавливаются алгоритмы действий, которые должны быть выполнены системой при срабатывании конкретного правила. Такая база данных может обновляться и пополняться её пользователем по мере необходимости.

Примером одной из таких систем служит IDS Snort. IDS Snort (Martin Roesch, 1998 г.) – свободно распространяемая сетевая COB, написанная на языке C. Система имеет сформированный разработчиками некий набор базовых правил. Однако, чтобы обнаружить несанкционированную деятельность с конкретными требованиями, которые характерны для определённого пользователя, можно разрабатывать и добавлять в базу данных собственные правила [1]. IDS Snort – это эффективный и открытый инструмент обнаружения атак.

Пример применения IDS Snort

С целью отладки и тестирования разработанных правил, был создан виртуальный сетевой стенд, состоящий из следующих элементов: два пользователя (Windows_7_1, Windows_7_2) и три маршрутизатора (FreeBSD 1, FreeBSD 2, FreeBSD 3). Конфигурация стенда представлена на рис. 1.



Рис. 1. Сеть для тестирования правил IDS Snort.

²⁵⁰ Юшкевич Алексей Сергеевич, МГТУ им. Н. Э. Баумана, г. Москва, 19-97leshka@rambler.ru

Для запуска IDS Snort в командной строке администратора компьютера, где установлена система, указываем путь к каталогу, с которым будет проводиться дальнейшая работа (рис. 2 «а»), вводим команду [2]:

```
snort -A console -i 1 -c c:\Snort\etc\snort.conf
```

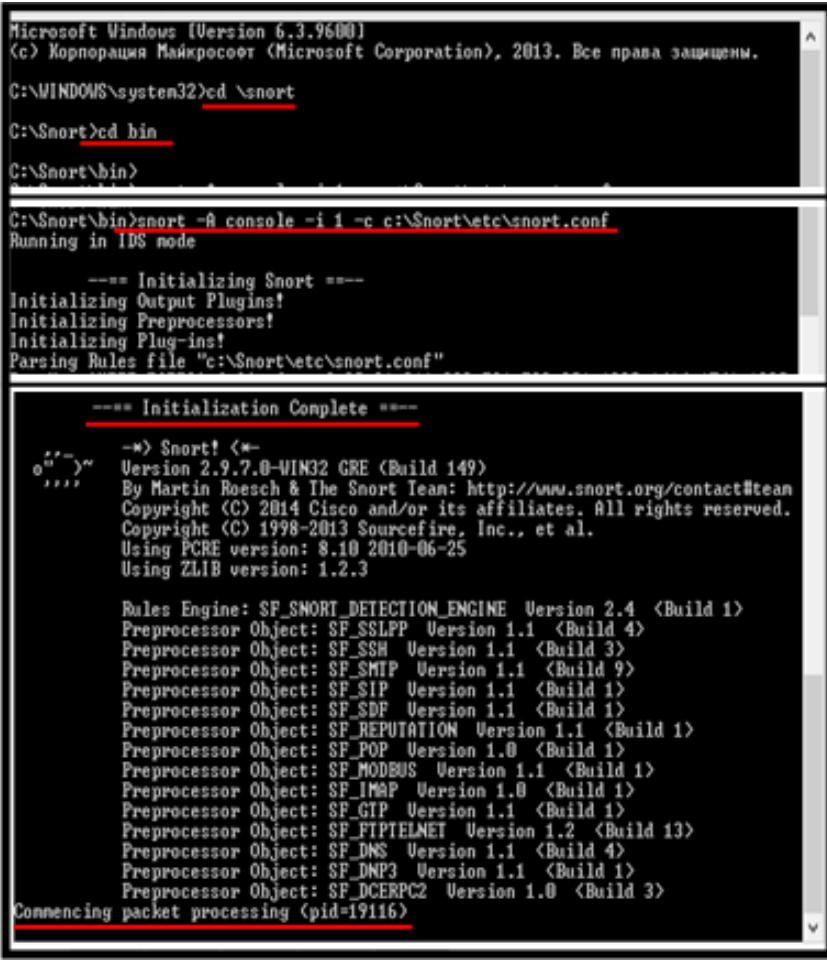
Процесс инициализации программы запущен (рис. 2 «б»).

Конфигурацию данной строки можно менять, в зависимости от необходимого результата работы программы. Так в приведённом примере система будет выводить на экран результаты работы правил.

Изменим команду:

```
snort -A fast -b -i 1 -c c:\Snort\etc\snort.conf
```

IDS Snort создаст в папке log файл alert.ids, в который будет записывать результаты сработанных правил. Через некоторое время после ввода команды инициализации, строка администратора выдаст сообщение о завершении инициализации и о начале обработки пакетов (рис. 2 «в»). С этого момента система IDS Snort начинает сканировать информационные потоки и сверять их с правилами [3].



```
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\WINDOWS\system32>cd \snort
C:\Snort>cd bin
C:\Snort\bin>
C:\Snort\bin>snort -A console -i 1 -c c:\Snort\etc\snort.conf
Running in IDS mode

---- Initializing Snort ----
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"

---- Initialization Complete ----

--> Snort! <*-
o"  )~
****
Version 2.9.7.0-WIN32 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 (Build 1)
Preprocessor Object: SF_SSLPP Version 1.1 (Build 4)
Preprocessor Object: SF_SSH Version 1.1 (Build 3)
Preprocessor Object: SF_SMTP Version 1.1 (Build 9)
Preprocessor Object: SF_SIP Version 1.1 (Build 1)
Preprocessor Object: SF_SDF Version 1.1 (Build 1)
Preprocessor Object: SF_REPUTATION Version 1.1 (Build 1)
Preprocessor Object: SF_POP Version 1.0 (Build 1)
Preprocessor Object: SF_MODBUS Version 1.1 (Build 1)
Preprocessor Object: SF_IMAP Version 1.0 (Build 1)
Preprocessor Object: SF_GTP Version 1.1 (Build 1)
Preprocessor Object: SF_FTPTELNET Version 1.2 (Build 13)
Preprocessor Object: SF_DNS Version 1.1 (Build 4)
Preprocessor Object: SF_DNP3 Version 1.1 (Build 1)
Preprocessor Object: SF_DCERPC2 Version 1.0 (Build 3)
Commencing packet processing (pid=19116)
```

Рис. 2.

В запущенных маршрутизаторах нужно ввести команду, которая выдавала бы необходимые результаты сканирования системы или выполняла конкретные действия, соответствующие командам. Например, выполняя команду «snort -vd» консоль будет журналировать содержимое пакетов (рис. 3). При помощи команды «snort -e» система будет журналировать информацию о заголовке пакета (рис. 4). Эти команды можно вводить как по отдельности на каждой машине, так и все вместе на одном маршрутизаторе. Однако, в последнем случае, будет формироваться слишком большой отчёт о пакетах и, следовательно, потребуется значительное время на обработку данных,

что неизбежно замедлит процесс мониторинга информационных потоков сети и может привести к срыву потока информации [4].

```

Len: 99
=====
02/12-23:59:54.090237 08:00:27:B3:D9:C2 -> 33:33:00:01:00:02 type:0x86DD len:0xA
1
fe80::99d4:945:9876:4e29:546 -> ff02::1:2:547 UDP TTL:1 TOS:0x0 ID:0 IpLen:40 Dg
mLen:147
Len: 99
=====
02/12-23:59:55.622492 08:00:27:90:75:7F -> 33:33:00:01:00:02 type:0x86DD len:0xA
1
fe80::9cb:ae47:d747:f4b0:546 -> ff02::1:2:547 UDP TTL:1 TOS:0x0 ID:0 IpLen:40 Dg
mLen:147
Len: 99
=====
02/12-23:59:56.103162 08:00:27:B3:D9:C2 -> 33:33:00:01:00:02 type:0x86DD len:0xA
1
fe80::99d4:945:9876:4e29:546 -> ff02::1:2:547 UDP TTL:1 TOS:0x0 ID:0 IpLen:40 Dg
mLen:147
Len: 99
=====

```

Рис. 3. Результат команды «snort -vd».

```

1 alert icmp 192.168.11.5/24 any -> 192.168.11.6/24 any (msg:"There was an exchange of packets with a dangerous location (ICMP)"; sid:99990;)
2 alert udp 192.168.11.5/24 any -> 192.168.11.6/24 any (msg:"There was an exchange of packets with a dangerous location (UDP)"; sid:99991;)
3 alert ip 192.168.11.5/24 any -> 192.168.11.6/24 any (msg:"There was an exchange of packets with a dangerous location (IP)"; sid:99992;)

```

Рис. 4. Результат команды «snort -e».

Для примера составим несколько блоков правил.

Первый блок правил «new1.rules», показанный на рис. 5, разработан для проверки работы IDS Snort с созданной сетью.

```

02/12-23:49:06.269796 192.168.11.5:54565 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:6615 IpLen:20 DgmLen:50
Len: 22
55 8B 00 00 00 01 00 00 00 00 00 04 77 70 61 U.....wpa
64 00 00 01 00 01 d.....

=====
02/12-23:49:06.368063 fe80::9cb:ae47:d747:f4b0:50066 -> ff02::1:3:5355
UDP TTL:1 TOS:0x0 ID:0 IpLen:40 DgmLen:70
Len: 22
55 8B 00 00 00 01 00 00 00 00 00 04 77 70 61 U.....wpa
64 00 00 01 00 01 d.....

=====
02/12-23:49:06.368436 192.168.11.5:54565 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:6616 IpLen:20 DgmLen:50
Len: 22
55 8B 00 00 00 01 00 00 00 00 00 04 77 70 61 U.....wpa
64 00 00 01 00 01 d.....

=====

```

Рис. 5. Первый блок правил для IDS Snort.

Соблюдая предложенные правила, система должна выдавать тревогу при обнаружении icmp, udp, ip пакетов, исходящих от первого пользователя сети (Windows_7_1) из любых его портов к

любым портам второго пользователя (Windows_7_2). Тревога будет сопровождаться сообщением о том, что был совершён обмен пакетами определённого типа с опасной локацией.

Второй блок (рис. 6.) имеет несколько опций в одном правиле. При их выполнении будет генерироваться предупреждение в том случае, если размер udp, ip пакетов, поступающих от первого пользователя ко второму, будет соответствовать диапазону от 90 до 4000 байт. При этом на экране появится сообщение «It is very big packet! Attention! May be network attack!» (англ.) (Этот пакет очень большой! Внимание! Возможно это сетевая атака!). Так же при наличии в пакетах, например, такого набора символов: «01» - система выдаст сообщение о том, что был передан пакет с подозрительным содержимым и выдаст тревогу.

```
1 alert udp 192.168.11.5/24 any -> 192.168.11.6/24 any (msg:"It is very big packet! Attention! May be network attack!"; dsize: 90<4000; sid: 100001;)
2 alert udp 192.168.11.5/24 any -> 192.168.11.6/24 any (msg:"It is very big packet! Attention! May be network attack!"; dsize: 90<4000; sid: 100002;)
3 alert udp 192.168.11.5/24 any -> 192.168.11.6/24 any (msg:"Was handed a package with suspicious content"; content:"01"; nocase; sid: 100003;)
4 alert ip 192.168.11.5/24 any -> 192.168.11.6/24 any (msg:"Was handed a package with suspicious content"; content:"01"; nocase; sid: 100004;)
```

Рис.6. Второй блок правил для IDS Snort.

Выполняя третий блок правил (рис. 7), система будет выдавать тревогу тогда, когда адрес отправителя совпадет с адресом получателя. Появится сообщение, информирующее о том, что произошло соединение пользователя Windows_7_1 с самим собой.

```
1 alert icmp 192.168.11.5/24 any -> any any (msg:"There was a connection user Windows_7_1 with yourself "; sameip; sid:100010;)
2 alert udp 192.168.11.5/24 any -> any any (msg:"There was a connection user Windows_7_1 with yourself "; sameip; sid:100011;)
3 alert ip 192.168.11.5/24 any -> any any (msg:"There was a connection user Windows_7_1 with yourself "; sameip; sid:100012;)
4 alert tcp 192.168.11.5/24 any -> any any (msg:"There was a connection user Windows_7_1 with yourself "; sameip; sid:100013;)
```

Рис. 7. Третий блок правил для IDS Snort.

Для обеспечения наглядности результатов тестирования, испытание разработанных правил произведём с помощью команды:

snort -A fast -b -i 1 -c c:\Snort\etc\snort.conf

Результаты тестирования разработанных правил представлены на рисунках: для первого блока правил на рис. 8, для второго – рис. 9, для третьего – рис. 10.

```
1 02/19-21:42:38.026478 ** [1:99990:0] There was an exchange of packets with a dangerous location (IP) ** (Priority: 0) (UDP) 192.168.11.1:137 -> 192.168.11.255:137
2 02/19-21:43:38.068656 ** [1:99990:0] There was an exchange of packets with a dangerous location (ICMP) ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
3 02/19-21:44:38.776621 ** [1:99990:0] There was an exchange of packets with a dangerous location (IP) ** (Priority: 0) (UDP) 192.168.11.1:137 -> 192.168.11.255:137
4 02/19-21:44:38.776621 ** [1:99990:0] There was an exchange of packets with a dangerous location (UDP) ** (Priority: 0) (UDP) 192.168.11.1:137 -> 192.168.11.255:137
5 02/19-21:45:28.457475 ** [1:44442:0] There was an exchange of packets with a dangerous location (IP) ** (Priority: 0) (UDP) 192.168.11.1:137 -> 192.168.11.255:137
```

Рис. 8. Результат тестирования первого блока разработанных правил.

```
1 02/19-21:52:09.207902 ** [1:100003:0] Was handed a package with suspicious content ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
2 02/19-21:52:09.208674 ** [1:100004:0] Was handed a package with suspicious content ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
3 02/19-21:53:40.305422 ** [1:99992:0] There was an exchange of packets with a dangerous location (IP) ** (Priority: 0) (UDP) 192.168.11.1:137 -> 192.168.11.255:137
4 02/19-21:53:49.878246 ** [1:100002:0] It is very big packet! Attention! May be network attack! ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
5 02/19-21:53:49.878246 ** [1:100001:0] It is very big packet! Attention! May be network attack! ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
6 02/19-21:53:49.878246 ** [1:99992:0] There was an exchange of packets with a dangerous location (IP) ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
```

Рис. 9. Результат тестирования второго блока разработанных правил.

```
1 02/19-21:50:40.527372 ** [1:99991:0] There was an exchange of packets with a dangerous location (UDP) ** (Priority: 0) (UDP) 192.168.11.1:137 -> 192.168.11.255:137
2 02/19-21:50:40.527372 ** [1:100002:0] It is very big packet! Attention! May be network attack! ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
3 02/19-21:50:46.934216 ** [1:100003:0] There was a connection user Windows_7_1 with yourself ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
4 02/19-21:50:46.934216 ** [1:99990:0] There was an exchange of packets with a dangerous location (IP) ** (Priority: 0) (UDP) 192.168.11.1:137 -> 192.168.11.255:137
5 02/19-21:52:09.208674 ** [1:99992:0] There was an exchange of packets with a dangerous location (UDP) ** (Priority: 0) (UDP) 192.168.11.1:138 -> 192.168.11.255:138
```

Рис. 10. Результат тестирования третьего блока разработанных правил.

IDS Snort

Все множество методов обнаружения атак можно разделить на два класса: методы обнаружения аномалий и злоупотреблений. Например, модель IDES (Intrusion detection expert system – (англ.) экспертная система обнаружения вторжений) (Dorothy Denning, 1986 г.), являющаяся основой для большинства современных COB, использовала методы: экспертный, статический анализ и нейронная сеть. Тем самым одна система COB объединяла в себе оба рассматриваемых класса. Принцип работы IDS Snort, одного из последователей IDES, основывается на сигнатурном методе обнаружения злоупотреблений, так как сигнатуры атак прописываются в правилах системы и составляют пополняемую базу [1]. Каждое правило состоит из двух частей: заголовков и опции [3].

Составляющие заголовка:

1. Действие. Ключевое слово, определяющее действие, которое будет выполняться при совпадении всех заданных правилом условий. В конфигурации правила всегда указывается первым и может быть одним из следующих ключевых слов:

- alert – генерировать сигнал тревоги и зарегистрировать пакет;

- log – записать информацию о пакете в журнальный файл;
- pass – пропустить (игнорировать) пакет;
- activate – генерировать сигнал тревоги и активизировать другое динамическое правило.

2. Протокол. IDS Snort в настоящее время различает 4 протокола - TCP, UDP, ICMP и IP. В будущем планируется включить протоколы - ARP, IGRP, GRE, OSPF, RIP, IPX;

3. Отправитель, порт. Указываются адреса и номера портов отправителя или получателя для данного правила;

4. Направление. Операторы «->», «<>» показывают направление передачи трафика для данного правила.

Опции правила включают сообщение и информацию о том, какие части пакета следует проверить, чтобы определить следует ли применять по отношению к пакетам заданное действие. Каждое правило должно иметь свой идентификационный номер, который указывается в опциях в конце правила с ключевым словом «sid» [5].

К основным возможностям IDS Snort можно отнести:

1. Мониторинг трафика сети;
2. Сканирование системы (порты, операционные системы (ОС), пользователи);
3. Обнаружение атак на такие службы как Telnet, FTP, DNS;
4. Выявление атак, связанных с Web-серверами, атаки на базы данных SQL, Oracle;
5. Возможность выполнения роли Web-фильтров;
6. Обнаружение вирусов.

Датчики, места расположения и способы применения IDS Snort

Машину, на которой работает IDS Snort, называют – датчиком (англ. sensor). Для правильного и эффективного действия системы обнаружения, IDS Snort нужно размещать за каждым из брандмауэров и маршрутизатором [3]. В том случае, если сеть содержит демилитаризованную зону (DMZ), IDS Snort может быть помещен и в этой зоне.

Вывод

Правила сформированные в системе IDS Snort позволяют не только эффективно выявлять сетевые вторжения, но и дают возможность администратору сети самостоятельно формировать конкретные требования через программные средства.

В настоящее время IDS Snort, при грамотном её использовании, может надёжно защищать сетевые информационные потоки. Широкое использование программы доказывает эффективность, универсальность и хорошие адаптивные возможности этого инструмента. Преимущество IDS Snort состоит в том, что помимо предлагаемых ею базовых правил для защиты сети от стандартных и распространенных атак, есть возможность разрабатывать и внедрять собственные правила для обнаружения специфических атак или иной вредоносной деятельности с признаками, характерными и вероятными, по мнению администратора, для данной конкретной сети.

Литература

1. Гамаюнов Денис Юрьевич. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов. М. 2007. С. 10, 12-13, 24-25.
2. В.А. Алешин, И.С. Строганов. Изучение и тестирование возможностей операционных систем. М. 2013. С. 20-26.
3. Mary Sudul, Jerry Votta, DesignSource, Maura Zaldivar, Jill Harry, Noreen Regina, Dan DePasquale. Intrusion Detection Systems with Snort // Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID. 2003. С. 8, 36-37, 55, 79, 82-89. URL: <https://ptgmedia.pearsoncmg.com/images/0131407333/downloads/0131407333.pdf>.
4. Chris Green. Snort Users Manual 2.9.8.2 // The Snort Project. 2016. С. 9-12. URL: <https://www.snort.org/documents/1>.
5. Николай Малых. Правила Snort. 2013. С. 3, 10-11, 14. URL: mirrors.pdp-11.ru/_misc/_otherDOC/SnortRules.pdf.

Научный руководитель: Валерий Александрович Матвеев, руководитель Научно-учебного комплекса «Информационная безопасность и системы управления», Заслуженный деятель науки РФ, профессор, д-р техн. наук, v.a.matveev@bmstu.ru

Experimental use of IDS SNORT network system as intrusion detection

Yushkevich A.²⁵¹

The process of establishing rules for the configuration of IDS Snort the system for the detection of network intrusions is illustrated on the specific examples. Considered as an example the sets of rules are successfully tested on the newly created virtual stand, performing all the tasks and reaching the goals set for each rule. Investigated rules will effectively track and block potential threats to network and inform about them the network administrator.

Keywords: information security, network intrusion, detection systems, rules configuration, identification of threats.

²⁵¹ Yushkevich Alex, Bauman Moscow State Technical University, Moscow, 19-97leshka@rambler.ru

Информационная безопасность России в условиях глобализации

Шепелёва О.Ю.²⁵²

Проведенная работа позволяет понять масштаб реальных проблем информационного пространства, стоящих перед РФ в современном глобальном мире, без успешного решения которых любое государство в кратчайшие сроки теряет суверенитет.

Ключевые слова: Глобальное информационное пространство, информационное общество, информационная безопасность, угрозы информационной безопасности.

1. Введение.

Становление глобального информационного общества в начале XXI в., которое привело к существенным изменениям облика системы социальных институтов и современная геополитическая ситуация в мире, конфликты в Африке, на Ближнем Востоке и Украине, террористическая угроза со стороны самопровозглашённого государства Игил, все новые и новые конфликты между отдельными странами за глобальное и региональное лидерство, перераспределение сфер влияния и борьба за ограниченные природные ресурсы, и еще многое другое актуализирует вопрос, касающийся объективного анализа информационной среды мирового сообщества и вопросов обеспечения национальной безопасности государства [1-8]. На фоне этих геополитических конфликтов и преобразований информация выступает в качестве мощнейшего стратегически важного ресурса, обладание которым может помочь усилить государственные позиции на международной арене и создать условия для контроля политических, экономических, социальных и культурных процессов, протекающих в международных системах [9-12].

2. Цель исследования.

Проанализировать современную ситуацию и выявить основные угрозы информационной безопасности России в условиях глобализации и формировании информационного общества.

3. Современное состояние информационной безопасности Российской Федерации

На современном этапе развития перед Россией, как и перед другими государствами объективно существует ряд реальных угроз информационной безопасности государства, недопущение или преодоление которых выступает важнейшим элементом Государственной стратегии обеспечения национальной безопасности в условиях полицентризма, когда сразу несколько государств претендуют на роль региональных центров силы. «Россия и Китай - страны со схожим военным потенциалом в киберпространстве и в отличие от обычных вооруженных сил, где США доминируют над другими странами, здесь у нас есть соперники, обладающие абсолютно тем же военным потенциалом, что и мы» - директор Американского Агентства обеспечения национальной безопасности (INB), глава Киберкомандования адмирал Майкл Роджерс [5, 12]. Такая ситуация означает, что в скором времени произойдут корректировки в концепции национальной безопасности любого из названных государств и, как следствие, изменятся формы информационного воздействия как на своих союзников, так и на противников.

3.1 Внешние угрозы информационной безопасности России

Рост числа членов НАТО, что ведет к географическому расширению зоны влияния и сферы военно-информационного воздействия Америки. Формирование единого

²⁵² Шепелёва Ольга Юрьевна, Санкт-Петербургский государственный экономический университет, Санкт-Петербург, shepeleva-olga@list.ru

глобального информационного пространства, где доминирующая роль в контроле над информационными потоками отводится США и странам ЕС. Рост взаимозависимости государств из-за формирования глобальной информационной инфраструктуры на основе сети Интернет. Проблема кибершпионажа, при которой только состоятельные корпорации и рыночные гиганты, у которых достаточно финансирования для закупки дорогостоящих ИТ-систем могут обеспечивать собственную безопасность, а их более «бедные» конкуренты остаются в заведомо проигрышном положении [5].

Вмешательство стран во внутренние дела России с целью навязывания определенных экономических и политических решений, препятствующих развитию и вынуждающих ориентироваться на экспорт сырья в ущерб развитию научных и высокотехнологических отраслей промышленности. Напряженность взаимоотношений с Исламскими государствами, играющими все возрастающую роль в современном мире посредством активного воздействия на политику, экономику и международные отношения крупных держав. Мотивирование образованных людей к переезду из России на постоянное место жительства/работы за границу.

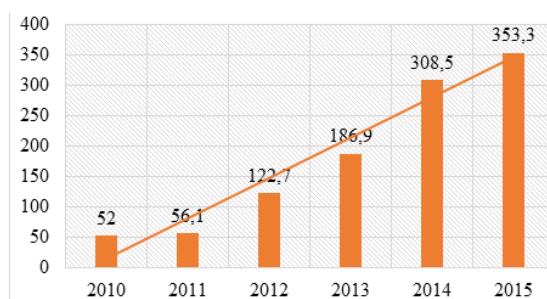


Рисунок 10 Миграция россиян, тыс. человек [9]

Создание условий для утечки капитала и непривлекательности долгосрочного инвестирования в экономику РФ. Поощрение зависимости от финансовых институтов запада и потери экономической и продовольственной самостоятельности.

3.2 Внутренние угрозы национальной безопасности Российской Федерации

Угрозы в сфере национально-этнического и религиозного экстремизма, активизация сепаратизма.

Антигосударственная политика некоторых СМИ в отношении органов власти.

Манипулирование общественным мнением, существенно влияющим на функционирование информационно-психологической среды общества, которая в свой черед принимает или противостоит политическим и экономическим реформам.

Проблема «цифрового» разрыва, т.е. разделения общества на тех, кто имеет возможность пользоваться высокими технологиями (ИТ, Интернет, телекоммуникации) и тех, кому эти технологии не доступны по каким-либо причинам, что прямо ведет к социальному неравенству, проявляющемуся в агрессивном настрое, социальной разобщенности и прогрессирующей пространственной сегрегации на основе отделения имущих слоев населения от неимущих.

Угроза вытеснения России с внутреннего информационного рынка и необходимость платить технологическую ренту странам за доступ к основным элементам киберпространства.

Распространение локальных военных конфликтов.

Усиление региональных противоречий и обострение информационного противоборства.

Все эти угрозы, как внешние, так и внутренние, стимулируются так или иначе через информационное влияние и направлены на дестабилизацию общероссийской социально-политической и экономической обстановки. Поэтому для России основной задачей сегодня является сохранение территориальной целостности, суверенитета и не допущение дальнейшего распространения антироссийского влияния Запада на территории как внутри страны, так и на ее ближних соседей.

4. Выводы

Россия занимает особое географическое положение и имеет свою специфическую культуру, которая объединяет многие народы. Такое пространственно-территориальное расположение определяет ее роль в системе геополитических отношений и в нарождающемся глобальном информационном пространстве. Внешняя политика нашей страны так или иначе затрагивает интересы как азиатских, так и европейских держав, что безусловно вынуждает ее участвовать во всех конфликтах на протяженности своей границы. Поэтому выполненный анализ современной ситуации дает основания сделать вывод, что Правительству Российской Федерации целесообразно рассмотреть возможность переоценки эффективности функционирования информационной организации государства.

Литература

1. Аналитический раздел сайта журнала Cnews [Электронный ресурс]. - URL: www.safe.cnews.ru, режим доступа свободный. (дата обращения: 28. 10.2016).
2. Бастрыкин А.И. Пора поставить действенный заслон информационной войне // Коммерсант-Власть. 18 Апреля 2016. [Электронный ресурс]. - URL: <http://sledcom.ru/press/interview/item/1030737/> (дата обращения: 28. 10. 2016).
3. Кучерявый М. М. Обеспечение национальной безопасности Российской Федерации в аспекте глобальных политических процессов современного мира // Власть. Общенациональный научно-политический журнал. 2014. № 2 (февраль). С. 105-109.
4. Кучерявый М. М. Основные факторы влияния политики информационной безопасности на национальную безопасность современной России // Евразийская интеграция: экономика, право, политика. 2013. № 14. С. 164-168.
5. Марков А.С. Летописи кибервойн и величайшего в истории перераспределения богатства // Вопросы кибербезопасности. 2016. № 1 (14). С. 68-74.
6. Сайт аналитической группы Gartner Group [Электронный ресурс]. - URL: www.gartner.com, режим доступа свободный. (дата обращения: 28. 10.2016).
7. Сайт Совета Безопасности Российской Федерации [Электронный ресурс]. - URL: <http://www.scrf.gov.ru/index.html>, режим доступа свободный. (дата обращения: 28. 10.2016).
8. Петренко С.А., Петренко А.С. Новая Доктрина информационной безопасности Российской Федерации // Защита информации. Инсайд. 2017. №1 (73). С. 7-14.
9. Сайт Федеральной службы государственной статистики [Электронный ресурс]. - URL: <http://www.gks.ru/>, режим доступа свободный. (дата обращения: 28. 10.2016).
10. Сайт центра аудита информационной безопасности [Электронный ресурс]. - URL: <http://bezpeka.ladimir.kiev.ua/>, режим доступа свободный. (дата обращения: 28. 10.2016).
11. Сулимин А.Н. Информационная безопасность России и угрозы глобального информационного сообщества [Электронный ресурс]. - URL: <http://elibrary.ru/download/82470986.pdf>, режим доступа свободный. (дата обращения: 28. 10.2016).
12. США назвали три страны—соперницы в киберпространстве // Коммерсант. ru [Электронный ресурс]. - URL: <http://www.kommersant.ru/Doc/2956905>, режим доступа свободный. (дата обращения: 28. 10.2016).
13. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности // Мониторинг правоприменения. 2017. № 1 (22). С. 53-61.

Научный руководитель: Минаков Владимир Фёдорович, доктор технических наук, профессор СПбГЭУ, Санкт-Петербург, m-m-m-m-m@mail.ru

Information Security of Russia in the Context of Globalization **Shepeleva O.**²⁵³

The work performed allows us to understand the real problems of the information space, facing Russia in the contemporary global world, without the successful solution of which any state in the shortest time loses its sovereignty.

Keywords: global information space, information society, information security

УДК 004.056

Проектирование приложения по отслеживанию уязвимостей ядра Linux **Вотрина М.И.**²⁵⁴

Аннотация. Доклад посвящен проблеме необходимости дополнительного метода контроля за исполнением политик безопасности в отношении уязвимостей ядра Linux. Проведено исследование существующих уязвимостей и их параметров. Предложены атрибуты базы данных для хранения важной информации об уязвимостях, а также структура приложения по их отслеживанию.

Ключевые слова: CVE, программная заплатка, обновления, демон аудита

Введение

Ядро – это главная часть любой операционной системы. Каждый, кто работал с операционной системой Linux, знаком с таким понятием как ядро Linux [1, 2]. Ядро отвечает за взаимодействие операционной системы с аппаратной частью компьютера, распределение ресурсов, управление процессами и за другие важные функции.

В современном мире все больше государственных и коммерческих предприятий переходят на операционные системы Linux, поэтому проблема безопасности работы в данной ОС ощущается наиболее остро [3]. Исходный код Linux содержит более тринадцати миллионов строк, поэтому неудивительно, что в нем периодически обнаруживаются уязвимости. Задачей администратора является своевременное получение информации о появившейся уязвимости и оперативное устранение бреши в безопасности. Регулярное обновление системы позволяет решить проблемы безопасности. Однако несмотря на присутствие пункта о регулярных обновлениях в политике безопасности каждой серьезной компании или учреждении довольно часто на практике можно столкнуться с несоблюдением данного пункта. Возникает необходимость в средстве, которое будет в автоматизированном режиме следить за выполнением регулярных обновлений, касающихся безопасности системы [4].

Информация об уязвимостях ядра

На данный момент в сети Интернет присутствует множество источников информации о существующих уязвимостях ядра Linux [5, 6]. У каждой найденной уязвимости есть несколько наиболее важных свойств в описании, а именно:

- название уязвимости;
- CVE-ID (уникальный идентификатор уязвимости);
- версии ядер Linux, для которых угроза актуальна;
- описание угрозы;
- ссылка на программную заплатку.

²⁵³ Shepeleva Olga, Saint-Petersburg State University of Economics, St. Petersburg, shepeleva-olga@list.ru

²⁵⁴ Вотрина М.И., МГТУ им. Н.Э. Баумана, г. Москва, marina7votrina@gmail.com

Эти данные наиболее важны для администратора операционной системы, чтобы понять, необходимо ли ему то или иное обновление. Руководствуясь своими знаниями и опытом, администратор должен принять взвешенное решение об установке программной заплатки или же запустить предложенное системой обновление.

База данных уязвимостей

Для создания программы, контролирующей наличие уязвимостей в системе, нужно прежде всего иметь базу данных самих уязвимостей в корректном для дальнейшего представления виде [7]. Разумно использовать для атрибутов реализуемой базы наиболее важные свойства уязвимостей ядра Linux (табл.1).

Таблица 1.

Пример содержимого базы данных уязвимостей ядра Linux

ID	Имя	CVE	Версия ядра	Описание	Ссылка на программную заплатку
1	rds	2010-3904	2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34, 2.6.35, 2.6.36	Функция <code>rds_page_copy_user</code> в <code>net/rds/page.c</code> реализация протокола Reliable Datagram Sockets (RDS) в ядре Linux до версии 2.6.36 включительно, прежде чем правильно проверить адреса, полученные из пользовательского пространства, что позволяет локальному пользователю получить привилегии с помощью использования системных вызовов <code>sendmsg</code> и <code>recvmsg</code> .	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3904
2	full-nelson	2010-4258	2.6.31, 2.6.32, 2.6.35, 2.6.37	Функция <code>do_exit</code> в <code>kernel/exit.c</code> в ядре Linux до версии 2.6.36.2 не проводит должным образом захват значения <code>KERNEL_DS</code> из <code>get_fs</code> , что позволяет локальному пользователю обойти ограничения, предназначенные для <code>access_ok</code> , перезаписать произвольные ячейки памяти ядра, а также привилегии усиления за счет использования (1) BUG, (2) указателя <code>NULL</code> , или (3) ошибки страницы, что показано векторами, связанными с функцией <code>clear_child_tid</code> и сращиванием системных вызовов.	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4258
...	...	...	...	...	...

Содержимое базы данных подлежит регулярному обновлению в соответствии с выбранными для этого достоверными источниками (рис. 1), например, NVD.



Рис. 1. Работа приложения и базы данных в общем случае

Расширение демона аудита

Демон – это программа, которая запускается системой и работает в фоновом режиме без всякого взаимодействия с пользователем. Спроектированная база данных послужит основой для создания подобия расширения демона аудита, так как приложение будет взаимодействовать с пользователем. Программа будет следить за соблюдением политик безопасности в отношении критических обновлений ядра Linux и проверять присутствие имеющихся в базе обновлений на конкретном устройстве. В случае нарушений администратору будет предлагаться информация о неустановленных обновлениях и возможность их установить или узнать подробнее.

Интерфейс

Интуитивно понятный графический интерфейс для администратора должен предполагать наиболее полное отражение содержащейся в базе данных информации, которая необходима для предоставления администратору (рис. 2). Должны быть доступны сортировка и поиск по основным параметрам (название, CVE, версия ядра). Также предполагается наличие флагов, которые уведомляют администратора о том, что соответствующая уязвимость была устранена.

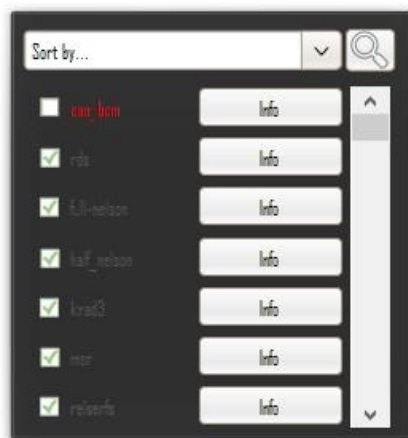


Рис. 2. Предлагаемый внешний вид приложения для анализа уязвимостей

Выводы

Выполненная работа позволит создать функционально полное и удобное приложение для аудита уязвимостей ядра Linux, которое позволит следить за соблюдением политик безопасности. Программа будет использовать информацию из достоверных источников и может стать полезным инструментом для администраторов ОС Linux. Впоследствии разработанный демон аудита будет использован для анализа угроз и рисков для верхнего уровня АСУ ТП АЭС в Иране.

Литература

1. Стахнов А. Linux (4 изд.). СПб.: БХВ-Петербург, 2011. 752 с.
2. Матвейчиков И.В. Обзор методов динамического встраивания в ядро операционной системы (на примере Linux) // Безопасность информационных технологий. 2014. № 4. С. 75-82.
3. Матвейчиков И.В. О методах повышения защищенности ядра Linux // Вестник Национального исследовательского ядерного университета МИФИ. 2014. Т. 3. № 1. С. 112.
4. 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.

5. Мищенко А.И. Механизмы поиска уязвимостей в операционных системах, построенных на базе ядра Linux // Системы и средства информатики. 2013. Т. 23. № 1. С. 27-32.
6. Цыварев А.В., Хорошилов А.В. Использование симуляции сбоев при тестировании компонентов ядра ОС Linux // Труды Института системного программирования РАН. 2015. Т. 27. № -5. С. 157-174.
7. Булдакова Т.И., Коршунов А.В. Обеспечение информационной безопасности ERP-систем // Вопросы кибербезопасности. 2015. № 5 (13). С. 41-44.

Научный руководитель: Булдакова Татьяна Ивановна, доктор технических наук, профессор, МГТУ им. Н.Э. Баумана, buldakova@bmstu.ru

Designing Application for Tracking Vulnerabilities in Linux Kernel

Votrina M. I.²⁵⁵

The report focuses on the problem of necessary an additional method of execution of policies with regards to Linux kernel vulnerabilities. The research of existing vulnerabilities and their parameters was conducted. A database attribute for storing important information about vulnerabilities and an application structure for their tracking were offered.

Keywords: CVE, patch, update, audit daemon

УДК 004.056.55

Разработка схемы квантового распределения ключей на основании протокола BB84 для повышения криптостойкости данного протокола за счет увеличения длины ключа по средствам введения в алгоритм доверенного центра

Соколов А.В.²⁵⁶

Статья посвящена разработке алгоритма, позволяющего увеличить криптостойкость существующего протокола BB84 за счет внедрения доверенного центра. Результатом статьи является схема, позволяющая повысить криптостойкость протокола при неизменных количественных затратах квантовой передачи для каждой из сторон, участвующих в процессе квантового распределения ключа. Данный результат представляет интерес в области развития квантовой криптографии.

Ключевые слова: BB84, квантовая криптография, квантовое распределение ключей, доверенный центр.

Введение

Практически каждый день публикуются новые научные работы и статьи об успехах в области квантовой физики, а также аппаратной реализации устройств, принцип действия которых основан на законах квантового взаимодействия. В совокупности объем названных материалов приближает день появления полноценного квантового компьютера, готового к массовому производству и не только не уступающему по своим характеристикам современным электронным вычислительным машиннам, но и во многом их превосходящего. Наступление этого дня будет означать крах современной классической криптографии [1].

Криптографы с 80-х годов пытаются подготовиться к возникновению квантовых компьютеров и разрабатывают криптоалгоритмы, основанные на квантовых вычислениях.

²⁵⁵ Votrina M. I., Bauman Moscow State University, Moscow, marina7votrina@gmail.com

²⁵⁶ Соколов А.В. МГТУ им.Н.Э.Баумана, sav193@yahoo.com

Первым протоколом распределения квантового ключа стал созданный в 1984 году Чарльзом Беннетом и Жилем Brassardом протокол «BB84» [2]. В основе криптостойкости данного алгоритма в первую очередь лежит принцип квантовой физики, согласно которому не представляется возможным детектировать квантовую частицу, при этом не изменив ее состояния.

Подробнее о протоколе BB84

BB84 был разработан для секретного распределения ключей между абонентами. Физической средой передачи информации в данном случае являются фотоны, поляризованные определенным образом [3]. По сложившейся традиции абонентов, участвующих в криптографической передаче называют Алисой и Бобом, а злоумышленника, пытающегося скомпрометировать защищаемую информацию Евой. Алиса генерирует поток фотонов и отправляет Бобу. Полученные фотоны Боб детектирует одним из двух способов для каждого из фотонов.

Фотоны могут быть поляризованы под углом в 0, 45, 90, 135 градусов, чему соответствуют обозначения: «|» - вертикальная поляризация, «--» - горизонтальная поляризация, «/» - поляризация под углом 45 градусов и «\» - поляризация под углом 135 градусов. В случае попадания вертикально или горизонтально поляризованного фотона на прямоугольный детектор, обозначаемый «+», фотон распознается однозначно и не изменяется [4]. Аналогично для ситуации прохождения фотона, поляризованного под углом 45 или 135 градусов через диагональный детектор, обозначаемый «х». В противном случае, когда поляризация фотона не совпала с формой детектора, через который он прошел, фотон может принять случайное значение из диапазона допустимых для данного детектора значений поляризации фотона [5]. Иными словами, если, например, фотон «/» с поляризацией 45 градусов прошел сквозь прямоугольный детектор «+», то на выходе с вероятностью $\frac{1}{2}$ фотон будет поляризован либо горизонтально «--», либо вертикально «|».

Таблица 1.

Результаты прохождения поляризованных фотонов через
прямоугольный и диагональный детекторы.

Поляризация		--	\	/		--	\	/
Детектор	+	+	+	+	х	х	х	х
Результат		--	?	?	?	?	\	/

Знак «?» означает, что результат принимает случайную поляризацию из диапазона допустимых значений для конкретного детектора

Далее приводится алгоритм работы описываемого протокола:

- 1) Алиса отправляет Бобу последовательность фотонов, поляризованных случайным (на практике псевдослучайным) образом, при этом приняв фотоны «|» и «\» за единичный бит, а фотоны «--» и «/» за нулевой бит.
- 2) Боб принимает последовательность фотонов, анализируя каждый из них прямоугольным или диагональным детектором и записывает полученные значения.
- 3) Боб связывается с Алисой и сообщает какие детекторы были использованы им во время приема. В ответ Алиса сообщает какие детекторы были выбраны верно, а какие нет.
- 4) Боб и Алиса вычеркивают те позиции, в которых детектор был подобран неверно, а для оставшихся записывают значения в виде битов. Таким образом у Алисы и Боба имеется одинаковая последовательность бинарных символов, известных только им. Именно эта последовательность будет являться ключом шифрования для дальнейших преобразований.

В случае, если злоумышленник, то есть Ева попытается скомпрометировать ключевую информацию, вмешавшись в процесс передачи, она тем самым изменит первоначальную последовательность, генерируемую Алисой. В таком случае Боб получит искаженную последовательность, в результате чего его ключ будет отличаться от ключа Алисы.

Обычно, для проверки на отсутствие прослушки со стороны Евы выбирается некоторое количество n проверочных бит. Тогда с вероятностью $1 - 2^{-n}$ канал прослушивается.

Слабые стороны протокола BB84

После анализа используемых детекторов выходная последовательность значительно уменьшается. В случае бесконечно длинной последовательности эта вероятность составляет 50%. Таким образом, только примерно половина переданной информации в дальнейшем служит в качестве ключа.

Кроме того, существуют некоторые другие недостатки, связанные с физическими особенностями квантовой физики, а также несовершенством существующих аппаратных реализаций, которые не будут рассматриваться в данной статье.

Предлагаемая схема решения некоторых недостатков протокола BB84

Для решения проблемы уменьшения размера ключа, а также для увеличения криптостойкости алгоритма в статье предлагается использование следующей схемы реализации протокола BB84:

В процесс квантового распределения дополнительно вводится третья сторона, доверенный центр, называемый Charlie.

- 1) Алиса и Боб отправляют Чарли поляризованный поток фотонов по квантовому каналу (рис.1).

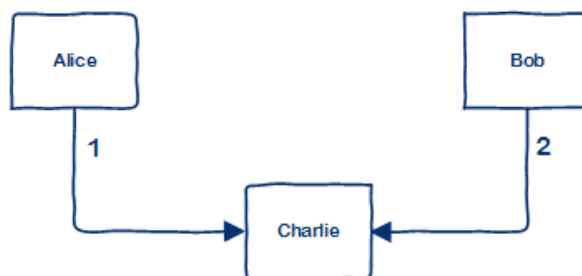


Рис.1. Передача поляризованных фотонов доверенному центру.

- 2) Чарли принимает фотоны и анализирует одним из детекторов. После этого Чарли связывается с Алисой и Бобом и узнает какие детекторы были применены верно, а какие нет (рис.2).

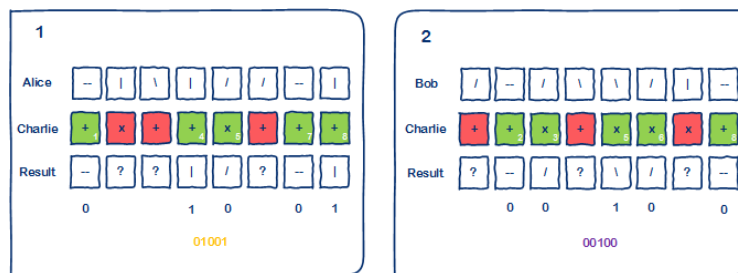


Рис.2. Получение результатов ключа после проверки корректности выбора детекторов

- 3) Чарли известны ключи Алисы и Боба, полученные им на предыдущем шаге. Далее Чарли необходимо передать Алисе ключ Боба, а Бобу ключ Алисы (рис.3).

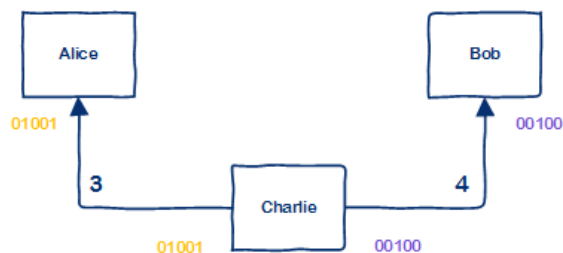


Рис.3. Доверенный центр должен передать ключи Алисы и Боба Бобу и Алисе соответственно

- 4) Для передачи Алисе и Бобу ключей Боба и Алисы соответственно Чарли связывается с каждым и сообщает последовательность корректно выбранных детекторов на шаге 2 таким образом, чтобы их конечные значения повторяли ключ Боба и Алисы (рис.4).



Рис.4. Передача ключей на основании ранее выбранных верных детекторов.

- 5) Получив ключ Боба, Алиса склеивает его ключ со своим, получая тем самым ключ большей длины. Боб делает тоже самое, склеивая ключ Алисы со своим. В Итоге и Алиса и Боб имеют ключ равный длине суммы их ключей по отдельности, после чего они могут шифровать и дешифровать информацию на основе полученного ключа (рис.5).



Рис.5. Шифрование данных ключем, полученным конкатенации ключей Алисы и Боба.

Выводы

Достоинствами данного метода является увеличение длины ключа при тех же количественных значениях квантовой передачи в оригинальной схеме BB84 в n раз, где $n \in [1..2]$ и $n = 2$ при $k \rightarrow \infty$, где k - количественная характеристика квантовой передачи.

Кроме того, данный метод увеличивает криптостойкость за счет того, что для получения полного ключа шифрования злоумышленнику потребуется перехватывать информацию одновременно на двух каналах, что требует больших временных, материальных и других затрат. При этом вероятность обнаружения вмешательства возрастает.

Недостатками такой схемы являются дополнительные расходы на реализацию доверенного центра. Временные затраты не оказывают значительного влияния, если доверенный центр способен принимать и передавать информацию одновременно для обоих абонентов, участвующих в процессе передачи.

Литература

1. Востоков Н., Борисова С.Н. Квантовая криптография // Успехи современного естествознания. 2012. №6. С. 88-90.
2. Кулик С. Квантовая криптография // Фотоника. 2013. №2. С. 36-41.
3. Кайраллапова А.Н. Стойкость протокола BB84. Караганда. 2014. С. 227-228.
4. Кронберг Д.А., Молотков С.Н. Квантовая схема для оптимального прослушивания протокола квантового распределения ключей BB84 // Известия Российской академии наук. Серия физическая. 2010. № 7. С. 954-960.
5. Пономарева В.В., Розова Я.С. Протоколы квантового распределения ключей // Прикладная информатика. 2014. С. 113-123.

Рецензент: Лебедев Анатолий Николаевич, доцент, к.ф.-м.н., сотрудник кафедры ИУ-8 МГТУ им. Баумана, заместитель по учебной работе, lan@lancrypto.com

Working Out the Scheme of Quantum Key Distribution on the Basis of Protocol BB84 for Increasing Cryptographic Strength of Given Protocol at the Expense of Increasing Key Length through Putting into Algorithm of Confident Center Sokolov A.V.²⁵⁷

The article is devoted to the working out the algorithm allowing to increase cryptographic strength of the existing protocol BB84 through inclusion the confident center. The result of this article is the scheme allowing to increase cryptographic strength of protocol at constant quantitative expenditures quantum transmission for each of the parties taking part in the process of quantum distribution of keys. The given result is interesting in the sphere of developing quantum cryptography.

Keywords: BB84, quantum cryptography, quantum key distribution, confident center.

УДК 004.05; ГРНТИ 81.93.29; ВАК 05.13.19

К вопросу о реализации сигнатурно-эвристического анализа безопасности программ

Фадин А.А.²⁵⁸, Рауткин Ю.В.²⁵⁹

Аннотация: Описано применение статического анализа для обнаружения уязвимостей и дефектов программного кода. Показано, что полноту проверок можно осуществить, используя предлагаемый сигнатурно-эвристический анализ безопасности программного кода. Рассмотрены вопросы формального описания сигнатурно-эвристического анализа безопасности программного кода. Дано описание программной реализации статического анализатора. Представлены результаты оценки его эффективности.

Ключевые слова: безопасность программ; дефекты безопасности; уязвимости; эвристический анализ; недеklarированные возможности

Введение. Большой объем, сложность и динамизм обновлений современного программного кода и объективное наличие в нем ошибок и уязвимостей определяет ряд проблемных задач в области обеспечения информационной безопасности компьютерных систем [1]. Использование автоматизированных средств аудита безопасности

²⁵⁷ Sokolov A. Bauman Moscow State Technical University. sav193@yahoo.com

²⁵⁸ Фадин Андрей Анатольевич, CISSP, ЗАО «НПО «Эшелон», af@cnpo.ru

²⁵⁹ Рауткин Юрий Владимирович, канд. техн. наук, ВП МО РФ, Москва

программного кода позволяет повысить эффективность работы эксперта за счёт локализации потенциально опасных фрагментов программного кода [2-5]. В частности, применение статических анализаторов исходных текстов программного обеспечения (ПО) позволяет проводить аудит безопасности программного кода в приемлемые сроки [6-11].

Среди средств статического анализа на практике применяются как коммерческие продукты (AppChecker, Appercut, CppCat), так и продукты с открытыми исходными текстами (CppCheck, PDM, Rats). Авторы проанализировали инструменты статического анализа исходных текстов согласно проектам NIST SP 500-268 и SATEC (формирующим наборы требований к функциональным особенностям анализаторов), а также согласно к классам обнаруживаемых дефектов. Важными критериями при анализе статических анализаторов являются наличие соответствия обнаруженных дефектов различным классификациям, функционал по работе с ложно позитивными срабатываниями и возможность совместной работы нескольких экспертов в системе [12]. Особое внимание уделялось на возможности инструментов статического анализа по предоставлению результатов работы, как наиболее востребованные аудитором исходных текстов в своей работе.

Сравнение показало, что большинство анализаторов предоставляет возможность конфигурировать, группировать и создавать свои правила анализа, формировать отчеты в форматах HTML и XML, настраивать и сохранять фильтры ложных срабатываний. Помимо перечисленных возможностей, только ApperCut и AppChecker опираются на известный стандарт CWE [13], являющийся открытым, исчерпывающим источником информации о дефектах. Средства CppCat и CppCheck позволяют проводить ревью найденных потенциально опасных конструкций кода ещё до завершения анализа, что способствует более продуктивной работе.

При анализе проектов, содержащих большие объёмы исходных текстов, на первый план выходят возможности по совместной работе нескольких экспертов над одним проектом, а так же возможности по одновременному анализу нескольких проектов. В полной мере этим требованиям удовлетворяют продукты AppChecker и ApperCut.

Необходимо упомянуть, что длительность анализа является результатом компромисса между точностью, глубиной и масштабируемостью применяемых механизмов анализа. Большинство анализаторов используют упрощения и эвристические алгоритмы для уменьшения времени анализа. [7, 9-11, 15].

Эвристический анализ представляет поиск дефектов в программном коде, сравнивая фрагменты кода с образцами из базы данных дефектов безопасности (эвристические правила) [15-17]. Эксперт дает окончательное заключение о критичности дефекта и возможности его эксплуатации злоумышленниками. Эксплуатируемый дефект безопасности представляет собой уязвимость, которая представляет угрозу информационной безопасности.

Для повышения унификации обнаружения стандартных дефектов и уязвимостей авторами предлагается использовать многоуровневую модель эвристического анализа, так как она обеспечивает обнаружение дефектов для таких вариантов исходного кода, как:

- лексический код;
- синтаксическое дерево;
- дерево Канторовича (абстрактное синтаксическое дерево, AST);
- граф потока управления (CFG);
- граф потока данных (DFG);
- SSA-представление;
- абстрактный семантический граф (ASG) [15, 17].

Для формализации обнаружения дефектов кода авторы предлагают использовать

продукционную модель представления знаний, так как она является легкой для понимания и применения, с учетом того, что в настоящее время известны не более 100 классов критических дефектов для определенного языка программирования [18].

Заключение. Обнаружение дефектов программного кода является одной из важнейших задач информационной безопасности. Применение современных статических анализаторов с использованием метода сигнатурно-эвристического анализа позволяет не только обеспечить полноту проверок, а также значительно повысить качество анализа и уменьшить время его проведения [19, 20].

Литература

1. Петренко А.С., Петренко С.А. Технологии больших данных (BigData) в области информационной безопасности // Защита информации. Инсайд. 2016. №4 (70). С. 82-88.
2. Барабанов А.В., Евсеев А.Н. Вопросы повышения эффективности анализа уязвимостей при проведении сертификационных испытаний программного обеспечения по требованиям безопасности информации // Труды международного симпозиума "Надежность и качество". 2015. Т. 1. С. 330-333.
3. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1 (2). С. 40-48.
4. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Известия ЮФУ. Технические науки. 2006. № 7 (62). С. 82-87.
5. Рибер Г., Малмквист К., Щербakov А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1 (3). С. 36-39.
6. Медведев Н.В., Марков А.С., Фадин А.А. Применение метода статического сигнатурного анализа для выявления дефектов безопасности веб-приложений // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2012. № 9. С. 21.
7. Ayewah, N., Hovemeyer, D., Morgenthaler, J. D., Penix, J., Pugh, W. 2008. Using Static Analysis to Find Bugs. IEEE Software. 25, 5 (Sep./Oct. 2008), 22-29. DOI= <http://dx.doi.org/10.1109/MS.2008.130>.
8. Boulanger, J. L. (Ed.). 2011. Static Analysis of Software: The Abstract Interpretation. Wiley-ISTE.
9. Hovemeyer, D., Spacco, J., Pugh, W. 2006. Evaluating and tuning a static analysis to find null pointer bugs. CM SIGSOFT Software Engineering Notes. 31, 1 (Jan. 2006), 13-19. DOI= <http://dx.doi.org/10.1145/1108768.1108798>.
10. Seoa, S.-H., Gupta, A., Sallama, A. M., Bertino, E., Yimb, K. 2014. Detecting mobile malware threats to homeland security through static analysis. Journal of Network and Computer Applications. 38 (Feb. 2014), 43-53. DOI= <http://dx.doi.org/10.1016/j.jnca.2013.05.008>.
11. Zhu, F., Wei, J. 2014. Static analysis based invariant detection for commodity operating systems. Computers and Security. 43, 49-63. DOI= <http://dx.doi.org/10.1016/j.cose.2014.02.00>.
12. Markov A., Rautkin Y., Luchin D., Tsirlov V. Evolution of a Radio Telecommunication Hardware-Software Certification Paradigm in Accordance with Information Security Requirements // В сборнике: 2015 International Siberian Conference on Control and Communications, SIBCON 2015 - Proceedings 2015. С. 7147139.
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. Марков А.С., Фадин А.А., Швеи В.В. Сравнение статических анализаторов безопасности программного кода // Защита информации. Инсайд. 2015. № 6 (66). С. 38-47.
15. 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.
16. Марков А.С., Фадин А.А. Статический сигнатурный анализ безопасности программ // Программная инженерия и информационная безопасность. 2013. № 1. С. 50-56.
17. Markov A.S., Fadin A.A., Tsirlov V.L. Multilevel Metamodel for Heuristic Search of Vulnerabilities in the Software Source Code // International Journal of Control Theory and Applications, 2016, Volume 9, Issue No. 30, pp. 313-320.
18. Марков А.С., Фадин А.А., Цирлов В.Л. Концептуальные основы построения анализатора безопасности программного кода // Программные продукты и системы. 2013. № 1. С. 10.
19. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls // Journal of Theoretical and Applied Information Technology. 2016. Т. 88. № 1. С. 77-88.
20. Markov A., Fadin A., Shvets V., Tsirlov V. The Experience of Comparison of Static Security Code Analyzers // International Journal of Advanced Studies. 2015. Т. 5. № 3. С. 55-63.

Научный руководитель: Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник, профессор МГТУ им.Н.Э.Баумана, Москва, a.markov@bmstu.ru

Implemental Basics of Signature-Heuristic Analysis of Security Softwaer

A. Fadin²⁶⁰, Yu. Rautkin²⁶¹

Abstract: The application of static code analysis to detect vulnerabilities and weaknesses in software code is analyzed. It is shown that the completeness of checks can be carried out using the proposed analysis of the security code. The problems of the formal description of the signature-heuristic analysis of security software are considered. The description of the software of static analyzer is presented. The results of the evaluation of its effectiveness are shown.

Keywords: software security; weakness; vulnerability; heuristic analysis; undeclared capabilities

²⁶⁰ Andrei A. Fadin, CISSP, NPO Echelon, af@cnpo.ru

²⁶¹ Yurii V. Rautkin, Ph.D., VP MO RF.

Оглавление

1	Алешин В.В. Определение актуальных угроз в критических системах информационной инфраструктуры и противодействие им	3
2	Авдеев В.С. Противодействие несанкционированному доступу в операционной системе Android	7
3	Авезова Я.Э., Фомичёв В.М. Признак наличия петель в заданном множестве вершин ориентированного графа	10
4	Бакеренков П.С. Разработка алгоритма стеганографической передачи информации	16
5	Барабанов А.В. Концепция создания информационных систем автоматизации деятельности по анализу уязвимостей программного обеспечения при проведении сертификационных испытаний	22
6	Бабурин В.Н. Реализационные основы доверенной загрузки на средствах виртуализации и вычислительной техники	26
7	Барабанов А. В. , Вареница В.В. , Савченко В.В. , Пургин А.Д. Информационная система автоматизации процесса поиска подтвержденных уязвимостей программного обеспечения	30
8	Барабанов А.В., Работаев И.М., Работаев Н.М. Подход к формированию требований по сертификации средств мониторинга событий безопасности на основе «Общих критериев»	34
9	Басан А.С., Басан Е.С. Методика оценки доверия в беспроводной сенсорной сети	38
10	Бельфер Р.А., Кулинич Р.С., Прищепин Е.П. Алгоритм установления виртуального соединения на абонентском доступе сети передачи данных учебного лабораторного стенда	41
11	Безик О.В., Басараб М.А. Генерация узоров кровеносных сосудов человека для создания базы данных искусственных биометрических образов	48
12	Бельфер Р. А., Кулинич Р. С., Прищепин Е. П. Алгоритм взаимной аутентификации транспортной части сети передачи данных в учебном лабораторном стенде	52
13	Бердюгин А.А. Обеспечение информационной безопасности дистанционного банковского обслуживания	58
14	Бельфер Р.А., Куянов М.С., Мерзляков Д.И., Зенькович С.А. Алгоритм взаимной аутентификации на абонентском доступе сети передачи данных в учебном лабораторном стенде	61
15	Бельфер Р.А. , Мазуров А.М. Алгоритм функции установления виртуального соединения многомаршрутной сети ПД в учебном лабораторном стенде	68
16	Булдакова Т.И., Александров М.Ю. Создание области загружаемых файлов для обеспечения безопасности электронно-библиотечной системы	73
17	Бондарев В. В. Возможный подход к оценке средств защиты информации	77
18	Будюкина Е.Н. Стеганографические методы защиты проектной документации САПР в аудиосигналах .	79
19	Булдакова Т.И., Кривошеева Д.А. Модель угроз безопасности при дистанционном мониторинге состояния человека	83
20	Быков А.Ю., Глинская Е.В., Стручкова А.В., Колинько Ф.К. Применение обучающей среды имитационного моделирования на основе технологии облачных вычислений при изучении дисциплины «Моделирование систем» для подготовки специалистов по информационной безопасности	88
21	Булдакова Т. И., Коршунов А.В. Автоматизированное обнаружение уязвимостей в веб-приложениях с помощью Team Foundation Server и OWASP ZAP	94
22	Волосатова Т.М. Метод защиты информационной подсистемы САПР от несанкционированного доступа	100
23	Варфоломеев А.А. О методах введения идентификаторов и перемешивания для обезличивания (анонимизации) персональных данных	103
24	Волкович Е.К. Разработка защищенного протокола обмена информацией о целевых компьютерных атаках на кредитно-финансовые организации	105
25	Воронина П. А., Козарь А. А. Анализ защищенности бортовых вычислительных средств	108
26	Гасанов Э.О., Медведев Н.В. Разработка способа управления доставкой сетевых пакетов	111
27	Гордеев Э.Н. О сохранении целостности информации в сетях с быстроменяющейся структурой	116
28	Голов И.Ю., Кукишев Д.А. Основные положения национальной инициативы США в области кибербезопасности	119
29	Гордеев Э.Н. Об одном подходе к оценке рисков при моделировании систем защиты информации	125
30	Ефремов Е.А., Ковалевский А.Е. Анализ автоматических систем контроля доступа	128
31	Горшков Ю.Г. , Марков А.С. , Цирлов В.Л. Новые технологии анализа и засекречивания речевых сигналов	135
32	Горшков Ю.Г., Марков А.С., Матвеев В.А., Цирлов В.Л. Современные тренды в области кибербезопасности	138
33	Зорин Е. Л., Басараб М. А., Матвеев В. А. Развитие концепции безопасных социальных сетей	142
34	Завадская Т.Е. К вопросу о защищенности систем сотовой связи	144

35	Кажемский М.А. Комбинирование форматного и пространственного методов встраивания цифровых водяных знаков в изображения графических форматов JPEG и BMP	147
36	Дорофеев А.В. Прикладные вопросы анализа социальных сетей.....	153
37	Зырянов Е.А. Формально-вербальная модель противодействия угрозам информационной безопасности	155
38	Козачок А.В., Кочетков Е.В. Подход к построению формальной модели функционирования процесса в операционной системе	158
39	Ключарёв П.Г. Обобщённые клеточные автоматы, как основа для построения функций формирования ключа	162
40	Ключарёв П.Г. Социальные сети: перспективные направления исследований.....	164
41	Куренкова П.Ю. Способ выбора сканера отпечатков пальцев.....	167
42	Козлов А.А. Сравнение линейных и разностных свойств операций сложения по модулю 2^n и AND.....	170
43	Комаров А.И., Комаров Н.И. Биометрические методы в симметричном шифровании	174
44	Лебедев А. Н., Островский Д.Е. Безопасное распределение конфиденциальной информации при инициализации приложения.....	177
45	Лебедев А. Н., Барсукова А. С. Анализ надежности защиты баз данных методами современной криптографии.....	180
46	Лебедев А. Н., Карондеев А.М., Козлов А.А. Новый алгоритм блочного шифрования «NASH»	183
47	Левиев Д.О., Герасимчук С.Н. Правовые аспекты защиты информации в лабораторных информационных системах	187
48	Лебедев А. Н., Соколов А.В. Квантовое распределение ключей с доверенным центром	189
49	Лебедев А. Н., Степанов Б.А., Онуфриев С. В. Способ строгой многофакторной аутентификации	194
50	Массель А.Г., Массель Л.В., Гаськова Д.А. Кибербезопасность в критических инфраструктурах (на примере энергетики)	197
51	Луценко А.Э. NTLM-авторизация при интеграции данных через ESB.....	200
52	Максимов Р.Л., Рафиков А.Г. Современные криптоконтроллеры для построения эффективных подсистем безопасности автономных систем.....	203
53	Медведев Н.В. , Глинская Е.В. Стеганография на основе ортогональных вейвлетов	208
54	Медведев Н.В., Карташова Ж.К. Определение оптимального базиса для представления сигнала со сложным спектральным составом в реальном масштабе времени	211
55	Мусихина Д. А. Критический обзор методических документов в сфере защиты персональных данных	213
56	Песков А.В. Приведение общей классификации факторов аутентификации	217
57	Надеина И.С. Базовые системы ввода-вывода как объект реализации угроз безопасности информации	221
58	Назарова Е.К. Информационная безопасность облачных технологий	225
59	Полужтков В.В. Способы статического и динамического анализа уязвимостей программного обеспечения	228
60	Петренко С.А. Создание национальной системы раннего предупреждения о компьютерном нападении.....	232
61	Родионов Д.Е., Рудакова Е.В. Обнаружение вторжений в компьютерные сети. технологии обнаружения аномальной активности	238
62	Полянский А.Ю. Исследование вопросов повышения эффективности анализа уязвимостей при проведении сертификационных испытаний программного обеспечения по требованиям безопасности информации	240
63	Пугачев Д.А. Автоматическая идентификация личности по изображениям лиц с использованием сверточных нейронных сетей.....	244
64	Самсонова В.Г. , Кулинич Р.С. Сравнительный анализ систем управления информационной безопасностью и событиями безопасности.....	248
65	Сараева Е.С. Экспериментальные исследования алгоритма распознавания образов на основе SURF	253
66	Русских А.Н., Басараб М.А. Анализ социальных сетей и выявление сообществ.....	258
67	Смолянинова К.А. Создание приложения для работы со Smart-картой.....	261
68	Скворцов М.А., Шахалов И.Ю. Обзор методов и средств оценки рисков информационной безопасности	265
69	Тарасов Я.В. Опыт использования технологий нейронных сетей для обнаружения низкоинтенсивных DDoS-атак	270
70	Султанов Д.Р. Исследование алгоритма дешифрования полностью гомоморфных шифров	274
71	Соколов М.Н. Анализ защищенности биометрических иммобилайзеров	279
72	Фокин М.С. Анализ процесса оценки защищенности веб-приложений	283
73	Троицкий И. И., Якубов Р. Ж. Применение метода k-ближайших соседей для распознавания дискретного сигнала в аддитивном шуме для двух каналов передачи информации при наличии общего шума	287

74	Фадин А.А. , Цирлов В.Л. К вопросу о централизации управления информационной безопасностью корпоративной сети.....	292
75	Чичварин Н.В., Бушуев В.В., Иванников П.В., Сосенко А.С. Программное обеспечение АРМ проектирования средств сканирования в FSO	295
76	Чесноков В.О. Обнаружение виртуальных пользователей в онлайн-социальных сетях путем анализа графов ближайшего окружения	299
77	Чичварин Н.В. Метод защиты сообщений, передаваемых в опто-электронных каналах.....	302
78	Шевченко Т.Д. Формализация процесса функционирования безопасной подвижной интеллектуальной системы	306
79	Чубатая А. Дополнительные меры защиты при работе с медицинскими информационными киосками .	308
80	Чукляев И.И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем	312
81	Щербакова Д.П. Применение метода контурного анализа для аутентификации по рисунку кровеносных сосудов	318
82	Юшкевич А.С. Экспериментальное использование сетевой системы IDS SNORT по обнаружению сетевых атак.....	323
83	Шепелёва О.Ю. Информационная безопасность России в условиях глобализации	329
84	Вотрина М.И. Проектирование приложения по отслеживанию уязвимостей ядра Linux	332
85	Соколов А.В. Разработка схемы квантового распределения ключей на основании протокола BB84 для повышения криптостойкости данного протокола за счет увеличения длины ключа по средствам введения в алгоритм доверенного центра	335
86	Фадин А.А. , Рауткин Ю.В. К вопросу о реализации сигнатурно-эвристического анализа безопасности программ	339

Сайт конференции: www.baumanist.ru

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 24.01.2017, Заказ № 011701
Формат 60х90/8. Гарнитура Times New Roman
Усл.печ. 13.07. Тираж 200 экз.