

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»

МЕЖДУНАРОДНАЯ
НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

(Москва, 6-7 апреля 2021 года)

СБОРНИК ТРУДОВ КОНФЕРЕНЦИИ

МГТУ им. Н.Э.Баумана
НУК «Информатика и системы управления»
МОСКВА-2021

УДК 003.26.7:004.09
ББК 32.937.202
Б31

Б31

Безопасные информационные технологии. Сборник трудов XI международной научно-технической конференции "Безопасные информационные технологии" – М.: МГТУ им. Н.Э.Баумана, 2021. 376 с. – илл.

ISBN 978-5-9906630-7-7

Сборник содержит тезисы докладов, представленных на международной научно-технической конференции "Безопасные информационные технологии" (БИТ-2021), проходившей 6-7 апреля 2021 г. в Москве в МГТУ им. Н.Э.Баумана.

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

Редакционный совет:

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



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

Вероятностная оценка рисков для реализации процесса управления человеческими ресурсами системы

Авдонин Р.Ю.¹, Костогрызов А.И.², Нистратов А.А.³

***Аннотация.** Предложены вероятностные методы решения задач по оценке возможных рисков, возникающих в процессе управления человеческими ресурсами системы с учетом требований по защите информации. Использование предложенных методов в жизненном цикле систем приведет к снижению рисков, в т.ч. в области информационной безопасности. Работоспособность методов продемонстрирована на примерах.*

***Ключевые слова:** анализ, безопасность, модель, риск, система, управление.*

1. Введение

Целью процесса управления человеческими ресурсами системы является своевременное оснащение системы необходимыми специалистами и поддержание их компетентности на уровне, достаточном для обеспечения нужного качества создаваемой системы и эффективности ее эксплуатации.

В процессе управления человеческими ресурсами системы могут возникать угрозы нарушения требований по защите информации. Такие риски могут быть связаны как с объективными и субъективными факторами, воздействующими на защищаемые активы и информацию, так и с неопределенностью ответственности за обеспечение защиты информации в процессе управления человеческими ресурсами системы, а также с преднамеренным отклонением от установленных норм и правил работы. Несмотря на множество работ по управлению рисками (например, [1-10]) проблематика, связанная с прогнозированием количественных рисков нарушения реализации процесса управления человеческими ресурсами системы и обоснованием эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых пределах продолжает оставаться остро актуальной.

2. Общие положения

В общем случае основными выходными результатами процесса управления человеческими ресурсами системы являются информационные и нематериальные результаты. К информационным результатам управления относятся планы управления человеческими ресурсами и подбора персонала, база данных по персоналу, трудовые договоры, планы и отчеты о выполнении проектов, в свою очередь к нематериальным результатам относятся непосредственно квалифицированный и мотивированный персонал, назначенный

¹ Авдонин Р.Ю., Федеральный исследовательский центр «Информатика и управление» Российской академии наук, e-mail: ft.99@yandex.ru

² Костогрызов А.И., д.т.н, проф., Федеральный исследовательский центр «Информатика и управление» Российской академии наук, e-mail: Akostogr@gmail.com

³ Нистратов А.А., к.т.н., ФБУ «НТЦ Энергобезопасность», Федеральный исследовательский центр «Информатика и управление» Российской академии наук, e-mail: andrey.nistratov@gmail.com

на соответствующие должности, полученные навыки, общедоступные знания, удовлетворенность персонала работой, уровень текучести кадров, удовлетворяющий потребности предприятия в работниках, приемлемый социально-психологический климат на предприятии, требуемый уровень безопасности, качества и эффективности функционирования системы, инновационный потенциал предприятия и пр. В жизненном цикле систем должны быть обеспечены как надежная реализация самого процесса управления человеческими ресурсами системы, так и защита связанной с этим информации.

3. Предлагаемые показатели для оценки

Для прогнозирования рисков в процессе управления человеческими ресурсами системы предлагается использовать следующие количественные показатели:

- риск нарушения надежности реализации процесса без учета требований по защите информации $R_{надежн}(T_{зад})$;
- риск нарушения требований по защите информации в процессе $R_{наруш}(T_{зад})$;
- интегральный риск нарушения реализации процесса с учетом требований по защите информации $R_{интегр}(T_{зад})$.

При оценке риска нарушения надежности реализации процесса предполагается, что в течение задаваемого периода прогноза надежность обеспечена, если в течение этого периода для всех элементов моделируемой системы обеспечена их целостность. Это означает, что в течение периода прогноза для всех осуществляемых недублируемых действий или получаемых выходных результатов процесса будет наблюдаться элементарное состояние «Целостность элемента моделируемой системы сохранена».

Оценки осуществляют с использованием вероятностных показателей нахождения элементов моделируемой системы в определенном элементарном состоянии. В сопоставлении с возможным ущербом вероятность нахождения в состоянии «Целостность элемента моделируемой системы нарушена» характеризует риск нарушения надежности выполнения соответствующего действия или получения выходного результата реализуемого процесса.

Прогнозирование интегрального риска предлагается оценивать в сопоставлении с возможным ущербом по формуле

$$R_{интегр}(T_{зад}) = 1 - [1 - R_{надежн}(T_{зад})] \cdot [1 - R_{наруш}(T_{зад})] \quad (1)$$

где $R_{надежн}(T_{зад})$ — риск нарушения надежности реализации процесса без учета требований по защите информации;

$R_{наруш}(T_{зад})$ — риск нарушения требований по защите информации в процессе.

Сами значения рисков $R_{надежн}(T_{зад})$ и $R_{наруш}(T_{зад})$ предлагается рассчитывать с использованием методов, подробно изложенных в [1-10].

5. Примеры

5.1 Пусть некоторое предприятие осуществляет комплекс действий по управлению человеческими ресурсами. Согласно рекомендациям ГОСТ Р МЭК 62508, посвященного анализу влияния человеческого фактора на надежность систем, основными действиями предприятия должны быть:

- формирование человеческих ресурсов;
- использование человеческих ресурсов;
- развитие человеческих ресурсов;
- оценка эффективности, связанной с управлением человеческими ресурсами.

В рамках примеров, не вдаваясь в детали, анализируется структура комплекса действий для получения выходных результатов в процессе управления человеческими ресурсами системы, представленная на рисунке 1.

Формальное описание действий согласно ГОСТ Р МЭК 62508 для получения выходных результатов процесса управления человеческими ресурсами



Рисунок 1 — Структура моделируемой системы в виде комплекса действий

Эта структура описывает моделируемую систему, элементами которой являются:

- подсистема 1, формально представляющая собой действия по формированию человеческих ресурсов, т.е. 1-й элемент системы;
- подсистема 2, формально представляющая собой действия по использованию человеческих ресурсов, связанные с функциональной поддержкой, оценкой и контролем. Подсистема 2 обозначена в моделируемой системе как два дублирующих друг друга элемента системы - элементы 21 и 22. Дублирование на практике означает, что действия выполняются более, чем одним исполнителем, один из которых – человек, функции другого исполнителя могут осуществляться или другим человеком (например, начальником) и/или поддерживаться роботом и/или какой-либо системой искусственного интеллекта. С точки зрения элементарных событий такое взаимодействие, по существу, означает, что действия будут выполнены подсистемой 2, если «ИЛИ» элемент 2.1 «ИЛИ» элемент 2.2 будут находиться в элементарном состоянии «Целостность элемента моделируемой системы сохранена»;
- подсистема 3, формально представляющая собой действия по развитию человеческих ресурсов (такие, как профессиональное обучение и повышение квалификации, наставничество, консультирование), т.е. это 3-й элемент системы;
- подсистема 4, формально представляющая собой действия по оценке эффективности реализации процесса и обозначенная как 4-й элемент системы.

По определению надежность реализации процесса управления человеческими ресурсами моделируемой системы считается обеспеченной в течение заданного периода прогноза, если в течение этого периода надежно выполнены «И» действия процесса по формированию человеческих ресурсов (по элементу 1), «И» по использованию человеческих ресурсов (по элементу 2.1 «И»/«ИЛИ» элементу 2.2), «И» по развитию человеческих ресурсов (по элементу 4), «И» по оценке эффективности (по элементу 4). Сам период прогноза для отдельного элемента может быть интерпретирован как относящийся к стадии создания (по угрозам, свойственным этой стадии), так и к стадии эксплуатации в будущем (по потенциально возможным угрозам), моделируя приемлемость решений и подтверждение гарантий неперевышения допустимых рисков.

5.2 Пример 1. Прогнозирование риска нарушения надежности реализации процесса управления человеческими ресурсами системы без учета требований по защите информации проиллюстрировано с помощью моделирования комплекса действий, представленных на рисунке 1. Выявлено множество возможных угроз, влияющих на безопасность каждого из структурных элементов моделируемой системы. При этом учтены не только угрозы здоровью и возможности человеческих ошибок, но и гипотетичные угрозы, связанные с возможными последствиями этих ошибок на этапе функционирования предприятия. Исходные данные по каждой из 4-х составных подсистем представлены в Таблице 1.

Таблица 1 — Исходные данные для прогнозирования риска нарушения надежности реализации процесса управления человеческими ресурсами системы без учета требований по защите информации (модели из [1-10], см. также ГОСТ Р 59333-2021)

Исходные данные	Значение	Комментарий
σ – частота возникновения источников угроз нарушения надежности реализации процесса для элемента	1-й элемент	1 раз в 5 лет (из-за утрачиваемых квалификации или знаний для решения задач) — это угроза, связанная с причинами нарушения необходимых сроков в определении требований к набираемому персоналу и составлении планов
	Элемент 2.1	2 раза в год (из-за недостаточной квалификации или знаний для решения задач или из-за проблем со здоровьем персонала) — это угроза, связанная с неэффективной функциональной поддержкой, оценкой и контролем действий
	Элемент 2.2	То же, что для элемента 2.1
	3-й элемент	1 раз в 3 года — это угроза, связанная с причинами нарушения необходимых сроков профессионального обучения и повышения квалификации
	4-й элемент	1 раз в год — это угроза, связанная с причинами нарушения необходимых сроков или качества периодической оценки эффективности реализации процесса
β – среднее время развития угроз для элемента с момента возникновения источников угроз до нарушения с возможным ущербом	1-й элемент	3 месяца — это означает, что развитие угрозы в течение этого срока может привести к последующим потерям или ущербам из-за несвоевременных решений в определении требований к набираемому персоналу и составлении планов
	Элемент 2.1	2 месяца — это означает, что развитие угрозы в течение этого срока может привести к нарушению качества продукции или услуг из-за неквалифицированной функциональной поддержки, оценки и контроля действий персоналом
	Элемент 2.2	То же, что для элемента 2.1

	3-й элемент	6 месяцев — это означает, что развитие угрозы в течение этого срока может привести к потерям и ущербам на предприятии из-за несвоевременного повышения квалификации, организации наставничества и проведения консультирования персонала
	4-й элемент	6 месяцев — это означает, что развитие угрозы в течение этого срока может привести к потерям и ущербам на предприятии из-за несвоевременной или некачественной оценки эффективности реализации процесса и функционирования организации
Тмеж – среднее время между окончанием предыдущей и началом очередной диагностики возможностей	по всем элементам	1 раз в неделю - с такой частотой на предприятии проводятся планерки с принятием управляющих решений
Тдиаг – среднее время диагностики состояния элемента	Элемент 1	1 час - такое среднее время требуется для контроля выполнения функций, связанных с определением требований к набираемому персоналу и составлением планов
	Элемент 2.1	15 минут - определяется временем медицинского обследования перед работой
	Элемент 2.2	То же, что для элемента 2.1
	3-й элемент	8 часов - такое среднее время требуется для контроля выполнения функций, связанных с повышением квалификации, организацией наставничества и проведением консультирования персонала
	4-й элемент	8 часов - такое среднее время требуется для контроля выполнения функций, связанных с оценкой эффективности реализации процесса и функционирования организации
Твосст – среднее время восстановления элемента после выявления нарушений	1-й элемент	1 день — это время исправления ошибок в определении требований к набираемому персоналу и составлением плана подбора персонала
	Элемент 2.1	1 час — это время замены человека, отстраненного от выполнения обязанностей (например, из-за болезни), и возложения необходимых обязанностей на заменяющего
	Элемент 2.2	То же, что для элемента 2.1
	3-й элемент	1 неделя — это время исправления ошибок в обеспечении повышения квалификации, организации наставничества и проведения консультирования персонала
	4-й элемент	3 дня — это время исправления ошибок в обеспечении своевременной и качественной оценки эффективности реализации процесса и функционирования организации
Тзад – задаваемая длительность периода прогноза	По всем элементам	от 1 года 4-х лет (для определения периода, при котором сохраняются гарантии непревышения допустимого риска нарушения надежности реализации процесса)

Анализ результатов расчетов показал, что в вероятностном выражении риск нарушения надежности реализации процесса управления человеческими ресурсами системы без учета требований по защите информации в течение 2-х лет составит за весь комплекс действий около 0.102 (см. рисунок 2), при увеличении периода прогноза от 1 года до 4-х лет (см. рисунок 3) риск возрастает от 0.043 до

0.241. Для допустимого риска на уровне 0.05 обоснован период до 14 месяцев, при котором сохраняются гарантии неперевышения допустимого риска в условиях, близких к реальным и характеризуемых условиями примера из таблицы 1.

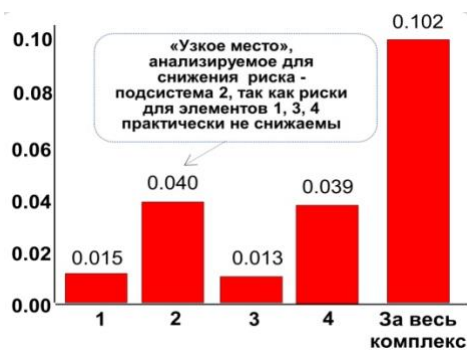


Рисунок 2 — Оценки риска нарушения надежности реализации процесса управления человеческими ресурсами в течение 2-х лет без учета требований по защите информации

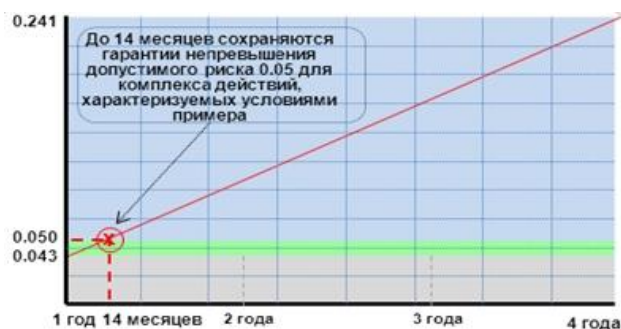


Рисунок 3 — Зависимость риска от периода прогноза длительностью от 1 года до 4-х лет

«Узким местом», характеристики которого имеет смысл анализировать на предмет снижения риска, является лишь подсистема 2 – это совокупность действий по использованию человеческих ресурсов, связанных с функциональной поддержкой, оценкой и контролем. Выявление этого «узкого места» заставляет провести дополнительный анализ на предмет выявления способов снижения риска. Самым простым вариантом является объединение усилий в использовании человеческих ресурсов. Эти усилия подразумевают взаимопомощь, включая взаимный контроль деятельности, а с точки зрения моделирования в структуре вместо элемента 2.2 с характеристиками, идентичными элементу 2.1, использование элемента 2.2, для которого частота возникновения источников угроз, связанных с неэффективной функциональной поддержкой, оценкой и контролем действий (σ) будет составлять не 2 раза в год (как в таблице 1 для персонала средней квалификации), а 1 раз в 2 года, т.е. в 4 раза реже. Это вполне достижимо за счет выполнения функций человеком-исполнителем более высокой квалификации и/или роботом и/или с поддержкой какой-то системой искусственного интеллекта. Все остальные исходные данные для моделируемой системы – те же, что представлены в таблице 1.

В итоге дополнительного моделирования установлено: за счет предпринятых мер обосновано снижение риска нарушения надежности реализации процесса управления человеческими ресурсами без учета требований по защите информации до уровня 0.076 (т.е. на 34.2%) и увеличение с 14 до 16 месяцев периода, для которого сохраняются гарантии неперевышения допустимых рисков (см. рисунок 4).

Собственно, на практике именно эти меры (объединение усилий нескольких лиц в параллельном решении одной задачи с взаимным контролем подготавливаемых решений) приводят к успеху. В примере представлена лишь количественная оценка результатов применения подобных мер.

5.3 Пример 2. Продолжая пример 1, прогнозирование риска нарушения требований по защите информации проиллюстрировано для комплекса действий согласно рекомендациям ГОСТ Р ИСО/МЭК 27002 (раздела 8) в части обеспечения безопасности персонала (см. рисунок 5).

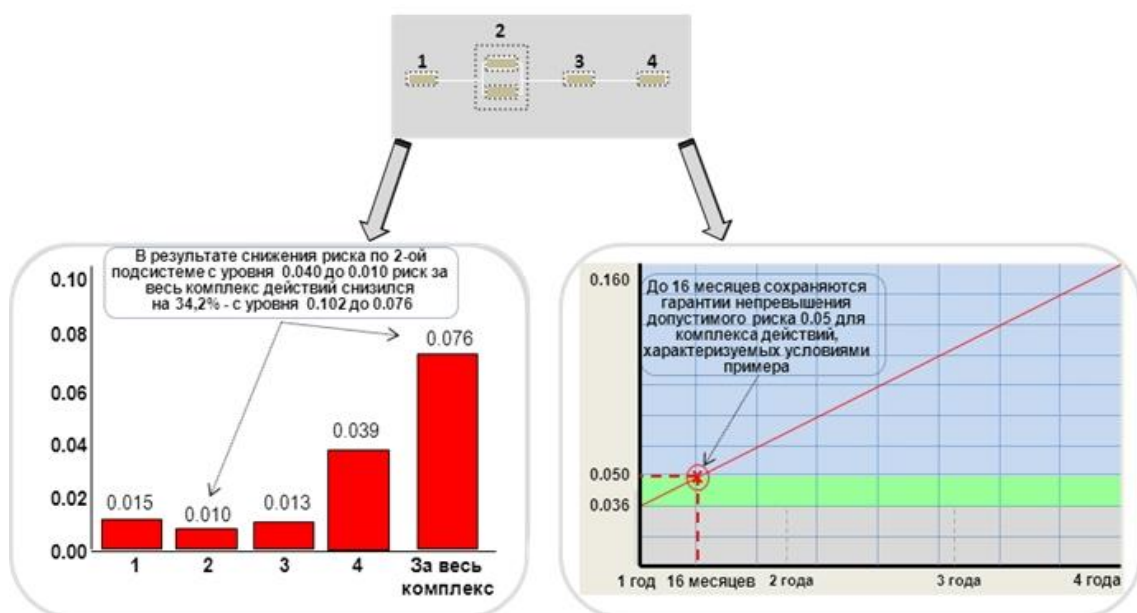


Рисунок 4 — Риск нарушения надежности реализации процесса управления человеческими ресурсами системы снижается, а период, для которого сохраняются гарантии неперевышения допустимого риска, увеличивается



Рисунок 5 Структура моделируемой системы для комплекса действий в части обеспечения безопасности персонала

Исходные данные по каждому из 3-х составляющих элементов представлены в Таблице 2.

Таблица 2 — Исходные данные для прогнозирования риска нарушения требований по защите информации в процессе управления человеческими ресурсами системы

Исходные данные	Значения и комментарии		
	для 1-го элемента	для 2-го элемента	для 3-го элемента
σ – частота возникновения источников угроз нарушения требований по защите информации	1 раз в 5 лет — это угрозы, связанные с субъективными факторами перед трудоустройством	1 раз в год (что соизмеримо со временем наработки на отказ оборудования) — это угрозы ущерба в течение занятости персонала	2 раза в год после прекращения или при смене занятости персонала – это угрозы возникновения ущерба при предыдущих ошибках или вследствие неудовлетворенности уволенного персонала

β – среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации	2 недели (что соизмеримо со временем использования уязвимостей) – это возможное время до ущерба от нарушения требований по защите информации перед трудоустройством конкретного лица	1 сутки (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее суток) – это время до ущерба после возникновения признаков угроз	1 сутки (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее суток) – это время до ущерба после признаков угроз от предыдущих ошибок или вследствие неудовлетворенности уволенного персонала
Тмеж – среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы	1 неделя - определяется регламентом контроля целостности ПО и активов, относящихся к набираемому персоналу	1 час - определяется регламентом контроля целостности ПО и активов, относящихся к персоналу предприятия	1 час - определяется регламентом контроля целостности ПО и активов, относящихся к персоналу предприятия
Тдиаг – среднее время диагностики состояния активов и самой системы защиты информации	30 секунд - автоматический контроль целостности активов, относящихся к персоналу предприятия	30 секунд - автоматический контроль целостности ПО и активов, относящихся к персоналу предприятия	30 секунд - автоматический контроль целостности ПО и активов, относящихся к персоналу предприятия
Твосст – среднее время восстановления требуемой нормы эффективности защиты информации	5 минут (включая перезагрузку ПО и восстановление персональных данных)	5 минут (включая перезагрузку ПО и восстановление данных)	5 минут (включая перезагрузку ПО и восстановление данных)
Тзад – задаваемая длительность периода прогноза	от 1 до 4-х лет (для определения периода, при котором сохраняются гарантии непревышения допустимого риска для обеспечения нормы эффективности защиты информации)		

Анализ результатов расчетов показал, что в вероятностном выражении риск нарушения требований по защите информации в течение двух лет составит за весь комплекс действий около 0.130, составляя для 1-го элемента – 0.014, для 2-го элемента – 0.041, для 3-го элемента – 0.080 («узкое место»). При увеличении периода прогноза от года до 4-х лет риск возрастает от 0.067 до 0.243. Для допустимого риска на уровне 0.050 обоснован период до 8 месяцев, при котором сохраняются гарантии непревышения допустимого риска в выбранном комплексе действий, характеризующихся условиями примера из таблицы 2.

Выявлено «узкое место» — сохранение возможностей прекратившего или сменившего обязанности лица воспользоваться полученной информацией (элемент 3). При этом причиной «узкого места» является нарушитель, способный (согласно принятой модели безопасности информации) в течение суток использовать эту гипотетическую уязвимость.

5.4 Пример 3. В продолжение примеров 1 и 2 рассчитывается интегральный риск $R_{\text{интегр}}(T_{\text{зад}})$ нарушения реализации процесса управления человеческими ресурсами системы с учетом требований по защите информации. Учитывая, что периода прогноза $T_{\text{зад}} = 2$ года, по результатам 1-го примера $R_{\text{надежн}}(T_{\text{зад}}) = 0.076$, а по результатам 2-го примера $R_{\text{наруш}}(T_{\text{зад}}) = 0.130$ получается:

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - (1 - 0.076) \cdot (1 - 0.130) \approx 0.196.$$

В итоге интегральный риск нарушения реализации процесса управления человеческими ресурсами системы в течение 2-х лет с учетом требований по защите информации составит 0.196. При этом риск нарушения требований по защите информации (0.13) в 1.7 раза превышает риск нарушения надежности реализации процесса управления человеческими ресурсами системы без учета требований по защите информации. Это означает, что необходим дополнительный системный анализ причин сравнительно высокого риска нарушения требований по защите информации и поиск эффективных мер для их выполнения. Таким образом, с помощью приведенных трех примеров продемонстрирована работоспособность предлагаемых методов.

Вывод

Предлагаемые методы позволяют оценивать на уровне вероятностных показателей различные риски для процесса управления человеческими ресурсами системы. Достоверность подтверждена на уровне реализации методов по предложениям авторов статьи в ГОСТ Р 59333-2021 «Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы».

Ожидается, что рациональное использование предложенных методов в жизненном цикле систем будет способствовать выявлению «узких мест» и снижению рисков в процессе управления человеческими ресурсами системы.

Литература

1. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд. "Вооружение, политика, конверсия", 2008. – 404с.
2. Andrey Kostogryzov, Andrey Nistratov, George Nistratov Some Applicable Methods to Analyze and Optimize System Processes in Quality Management // InTech. 2012. P. 127–196. URL = <http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management>
3. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G. Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V. 1. P. 217–244. <http://www.scirp.org/journal/ajor/>
4. Andrey Kostogryzov, Pavel Stepanov, Andrey Nistratov, George Nistratov, Oleg Atakishchev and Vladimir Kiselev Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling // Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186-192. www.dropbox.com/s/a4zw1yds8f4ecc5/AMSM2016%20Full%20Proceedings.pdf?dl=0
5. Костогрызов А.И., Степанов П.В., Нистратов А.А., Григорьев Л.И., Червяков Л.М. Прогнозирование рисков для обеспечения качества информации в сложных системах // Системы высокой доступности №3, т.2, 2016, с. 25-37
6. Vladimir Artemyev, Andrey Kostogryzov, Jury Rudenko, Oleg Kurpatov, George Nistratov, Andrey Nistratov Probabilistic methods of estimating the mean residual time

- before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20-22, 2017, Milan, Italy, pp. 368-373
7. Vsevolod Kershenbaum, Leonid Grigoriev, Petr Kanygin and Andrey Nistratov / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, pp. 55-79. <http://dx.doi.org/10.5772/intechopen.74963>
 8. Probabilistic Modeling in System Engineering. / By ed. A.Kostogryzov, - London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
 9. Костокрызов А.И. Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта / БИТ. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019, сс. 220-229.
 10. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364. <https://www.springer.com/gp/book/9783030468941>

Risk estimation for the implementation of the system's human resource management process

Avdonin R.Y.⁴, Kostogryzov A.I.⁵, Nistratov A.A.⁶

Abstract.

Probabilistic methods for solving problems of estimating possible risks in the process of managing the system's human resources, taking into account the requirements to information protection, are proposed. The use of the proposed methods in the life cycle of systems will reduce the risks considering the field of information security. The efficiency of the methods is demonstrated by examples.

Keywords: *analysis, security, model, risk, system, management.*

⁴ Avdonin R.Y, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, Moscow

⁵ Kostogryzov A.I, Dr.Sc., Prof., Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, Moscow

⁶ Nistratov A.A., Ph.D., “Scientific&Technical Center Energobezопасnost”, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, Moscow

Методы анализа рисков для процесса управления знаниями о системе

Авдонин Р.Ю.⁷, Костогрызов А.И.⁸, Нистратов А.А.⁹

Аннотация. Предложены методы, позволяющие анализировать различные риски при приобретении, создании и распространении полезных знаний о системе с учетом требований по защите информации. Использование предложенных методов в жизненном цикле систем будет способствовать выявлению «узких мест» и снижению интегрального риска нарушения процесса управления знаниями о системе.

Ключевые слова: анализ, защита информации, модель, риск, управление.

1. Введение

В общем случае главной целью процесса является повышение качества и/или безопасности и/или эффективности системы или связанных с ней систем за счет приобретения, создания, распространения, своевременного применения и сохранения полезных знаний в их жизненном цикле. В условиях множественных неопределенностей возникают различного рода риски, требующие рационального управления (см., например требования по ГОСТ Р 57193, ГОСТ Р 57127, ГОСТ Р 57133, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000). Несмотря на множество работ по управлению рисками (например, [1-10]) проблематика, связанная с прогнозированием количественных рисков нарушения реализации процесса с учетом требований по защите информации и обоснования эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых пределах продолжает оставаться остро актуальной.

2. Общие положения

В общем случае основными выходными результатами процесса управления знаниями о системе являются:

- стратегия управления знаниями (включая ТЗ, планы, программы и методики, инструкции, руководства пользователя);
- таксономия для применения активов знаний;
- организационные знания и активы знаний;
- конкурентные преимущества организации;
- методы и технологии повышения эффективности;
- «ноу-хау» и инновации в отношении процессов жизненного цикла конкретных систем, инфраструктуры, архитектуры новой продукции и программного обеспечения;
- результаты системного анализа в части обеспечения и повышения качества

⁷ Авдонин Р.Ю., Федеральный исследовательский центр «Информатика и управление» Российской академии наук, e-mail: ft.99@yandex.ru

⁸ Костогрызов А.И., д.т.н, проф., Федеральный исследовательский центр «Информатика и управление» Российской академии наук, e-mail: Akostogr@gmail.com

⁹ Нистратов А.А., к.т.н., ФБУ «НТЦ Энергобезопасность», Федеральный исследовательский центр «Информатика и управление» Российской академии наук, e-mail: andrey.nistratov@gmail.com

и/или безопасности и/или эффективности применения конкретных систем и удовлетворенности заинтересованных сторон.

В жизненном цикле систем должны быть обеспечены как надежная реализация самого процесса управления знаниями о системе, так и защита связанной с ним информации.

3. Предлагаемые показатели

Для прогнозирования рисков в процессе управления знаниями о системе предлагается использовать следующие количественные показатели:

- риск нарушения надежности реализации процесса без учета требований по защите информации;
- риск нарушения требований по защите информации в процессе;
- интегральный риск нарушения реализации процесса с учетом требований по защите информации.

При этом риск нарушения надежности реализации процесса без учета требований по защите информации предлагается характеризовать соответствующей вероятностью в зависимости от нарушения надежности реализации процесса приобретения знаний, создания полезных знаний о системе и распространения приобретенных или созданных полезных знаний о системе (все без учета требований по защите информации) в сопоставлении с возможным ущербом.

В качестве вероятностных показателей частных рисков предлагаются:

- вероятность нарушения надежности реализации процесса приобретения знаний без учета требований по защите информации;
- вероятностью нарушения надежности создания полезных знаний о системе без учета требований по защите информации;
- вероятностью нарушения надежности распространения приобретенных или созданных полезных знаний о системе без учета требований по защите информации.

В свою очередь надежное распространение приобретенных или созданных полезных знаний о системе предполагает их своевременное применение.

4. Расчетные формулы

4.1 Предлагаемый подход к оценке рисков демонстрируется на примере вероятности нарушения надежности реализации процесса приобретения знаний без учета требований по защите информации.

Для приобретения знаний предлагается оценивать:

- риск незавершенности выполнения необходимых действий по поставке приобретаемых знаний;
- риск нарушения сроков поставки приобретаемых знаний;
- риск наличия недопустимого брака в приобретаемых знаниях (аналитических ошибок, описок, необоснованных заключений и/или рекомендаций).

Риски характеризуются соответствующими вероятностями в сопоставлении с возможными ущербами, оцениваемыми тяжестью последствий для системы и ее заинтересованных сторон.

4.2 В каждом процессе приобретения знаний о системе должны быть выполнены необходимые действия. С точки зрения тяжести ущерба в случае незавершения выполнения необходимых действий процесса приобретаемые знания

могут быть условно сгруппированы по K типам, $K \geq 1$. В общем случае для каждого типа требования к завершенности процесса приобретения знаний формулируют на уровне инструкций должностных лиц.

На основе применения статистических данных вероятность незавершения выполнения необходимых действий процесса для знаний k -го типа за задаваемое время $T_{\text{зад } k}$ предлагается определять по формуле

$$R_{\text{действий } k}(T_{\text{зад } k}) = G_{\text{наруш } k}(T_{\text{зад } k})/G_k(T_{\text{зад } k}), \quad (1)$$

где $G_{\text{наруш } k}(T_{\text{зад } k})$ и $G_k(T_{\text{зад } k})$ – соответственно количество случаев незавершения выполнения необходимых действий процесса и общее количество необходимых действий процесса, подлежащих выполнению за заданное время $T_{\text{зад } k}$ для знаний k -го типа согласно статистическим данным.

Показатель завершенности выполнения необходимых действий для знаний k -го типа $Z_{\text{действий } k}(T_{\text{зад } k})$ определен следующим образом

$$Z_{\text{действий } k}(T_{\text{зад } k}) = \begin{cases} 0, & \text{если условия завершения необходимых действий выполнены;} \\ R_{\text{действий } k}(T_{\text{зад } k}) \text{ по (1),} & \text{если условия не выполнены или не заданы.} \end{cases} \quad (2)$$

Условие завершения необходимых действий по знаниям k -го типа определено как условие непревышения максимально допустимого уровня $R_{\text{доп.действий } k}(T_{\text{зад } k})$, задаваемого для вероятности незавершения выполнения необходимых действий приобретения по знаниям k -го типа. Это условие выражается в форме: $R_{\text{действий } k}(T_{\text{зад } k}) \leq R_{\text{доп.действий } k}(T_{\text{зад } k})$. В выражении для обобщенного риска показатель завершенности выполнения необходимых действий для процесса приобретения знаний k -го типа $Z_{\text{действий } k}(T_{\text{зад } k})$ обозначен как $Z(\text{пр})_{\text{действий } k}(T_{\text{зад } k})$ – см. выражение (10).

Вероятность незавершения выполнения необходимых действий приобретения по всему множеству знаний различных типов согласно статистическим данным предлагается определять по формуле

$$R_{\text{действий }}(T_{\text{зад }}) = 1 - \sum_{k=1}^K W_k [1 - R_{\text{действий } k}(T_{\text{зад } k})] / \sum_{k=1}^K W_k, \quad (3)$$

где $T_{\text{зад }}$ – задаваемое суммарное время на реализацию процесса для всего множества знаний различных типов, включающее в себя все частные значения $T_{\text{зад } k}$ с учетом их наложений;

W_k – количество учитываемых поставок приобретаемых знаний k -го типа при множественных поставках, в выражении для обобщенного риска применительно к процессу приобретения использовано обозначение $W(\text{пр})_k$, $k=1, \dots, K(\text{пр})$ – см. выражение (10).

4.3 Каждый процесс приобретения знаний должен быть выполнен в задаваемые сроки. С точки зрения важности и срочности приобретаемых знаний и тяжести ущерба в случае нарушения сроков поставки приобретаемые знания могут быть условно сгруппированы по I типам, $I \geq 1$. В общем случае для каждого типа требования к своевременности поставки приобретаемых знаний формулируют в виде: срок поставки знаний i -го типа должен быть не более задаваемого $T_{\text{зад } i}$, $i = 1, \dots, I$. Неприемлемость нарушения задаваемых сроков поставки фиксируют в договорных условиях в виде штрафных санкций для поставщика, особых условий

страхования ответственности и иных обязательств, направленных на недопущение нарушений сроков поставки знаний.

При оценке риска вычисляют вероятность нарушения сроков однократной и множественных поставок для разнородных знаний.

На основе применения статистических данных вероятность нарушения сроков однократной поставки для знаний i -го типа за задаваемое время $T_{\text{зад } i}$ предлагается определять по формуле

$$R_{\text{св } i}(T_{\text{зад } i}) = N_{\text{наруш } i}(T_{\text{зад } i}) / N_i(T_{\text{зад } i}), \quad (4)$$

где $N_{\text{наруш } i}(T_{\text{зад } i})$ и $N_i(T_{\text{зад } i})$ – соответственно количество нарушений сроков поставки и общее количество поставок за заданное время $T_{\text{зад } i}$ для знаний i -го типа согласно статистическим данным.

Показатель выполнения сроков поставки для знаний k -го типа определен следующим образом

$$Z_{\text{срок } i}(T_{\text{зад } i}) = \begin{cases} 0, & \text{если условия сроков поставки выполнены;} \\ R_{\text{св } i}(T_{\text{зад } i}) & \text{по (4), если условия не выполнены или не заданы.} \end{cases} \quad (5)$$

Условие выполнения сроков поставки знаний k -го типа определено как условие непревышения максимально допустимого уровня $R_{\text{доп.св } i}(T_{\text{зад } i})$, задаваемого для вероятности нарушения сроков однократной поставки. Это условие выражается в форме: $R_{\text{св } i}(T_{\text{зад } i}) \leq R_{\text{доп.св } i}(T_{\text{зад } i})$. В выражении для обобщенного риска показатель выполнения сроков поставки для процесса приобретения знаний i -го типа $Z_{\text{срок } i}(T_{\text{зад } i})$ обозначен как $Z(\text{пр})_{\text{срок } i}(T_{\text{зад } i})$ – см. выражение (10).

Вероятность нарушения сроков поставки по всему множеству знаний различных типов, реализуемых в процессе согласно статистическим данным с учетом множественности поставок, характеризуемых исходными данными по каждому из типов знаний, предлагается определять по формуле

$$R_{\text{св}}(T_{\text{зад}}) = 1 - \sum_{i=1}^I M_i [1 - R_{\text{св } i}(T_{\text{зад } i})] / \sum_{i=1}^I M_i; \quad (6)$$

Здесь $T_{\text{зад}}$ – задаваемое суммарное время поставки всего множества знаний различных типов, включающее в себя все частные значения $T_{\text{зад } i}$ с учетом их наложений, M_i – количество учитываемых поставок знаний i -го типа при множественных поставках, в выражении для обобщенного риска применительно к процессу приобретения использовано обозначение $M(\text{пр})_i$, $i = 1, \dots, I(\text{пр})$ – см. выражение (10).

4.4 При реализации каждого процесса приобретаемые знания должны удовлетворять требованиям по качеству. Наличие недопустимого брака (аналитических ошибок, описок, необоснованных заключений и/или рекомендаций) в приобретаемых знаниях – это угроза возможного ущерба. В общем случае под выполнением требований по качеству понимается поставка знаний без брака или с допустимым уровнем брака, оговоренным в договорных условиях. С точки зрения нарушения качества приобретаемых знаний и тяжести возможного ущерба приобретаемые знания могут быть условно сгруппированы по J типам, $J \geq 1$. Неприемлемость нарушений задаваемых ограничений фиксируют в

договорных условиях в виде штрафных санкций для поставщика знаний, особых условий страхования ответственности и иных обязательств, направленных на недопущение брака.

При оценке риска вычисляют вероятность наличия брака при однократной и множественных поставках разнородных знаний.

На основе применения статистических данных вероятность наличия брака при однократной поставке знаний j -го типа за задаваемое время $T_{\text{зад } j}$ предлагается определять по формуле

$$R_{\text{брака } j}(T_{\text{зад } j}) = N_{\text{наруш } j}(T_{\text{зад } j})/N_j(T_{\text{зад } j}), \quad (7)$$

где $N_{\text{наруш } j}(T_{\text{зад } j})$ и $N_j(T_{\text{зад } j})$ – соответственно количество поставок с недопустимым браком и общее количество поставок за заданное время $T_{\text{зад } j}$ для знаний j -го типа согласно статистическим данным.

Показатель отсутствия брака в поставке знаний j -го типа определен следующим образом

$$Z_{\text{брака } j}(T_{\text{зад } j}) = \begin{cases} 0, & \text{если условия по отсутствию брака в поставке выполнены;} \\ R_{\text{брака } j}(T_{\text{зад } j}) \text{ по (7),} & \text{если условия не выполнены или не заданы.} \end{cases} \quad (8)$$

Условие отсутствия брака в приобретаемых знаниях k -го типа определено как условие непревышения максимально допустимого уровня $R_{\text{доп.брака } j}(T_{\text{зад } j})$, задаваемого для вероятности наличия брака в поставке. Это условие выражается в форме: $R_{\text{брака } j}(T_{\text{зад } j}) \leq R_{\text{доп.брака } j}(T_{\text{зад } j})$. В выражении для обобщенного риска показатель отсутствия брака для процесса приобретения знаний j -го типа $Z_{\text{брака } j}(T_{\text{зад } j})$ обозначен как $Z(\text{пр})_{\text{брака } j}(T_{\text{зад } j})$ – см. выражение (10).

Вероятность наличия брака по всему множеству знаний различных типов, реализуемых согласно статистическим данным с учетом множественности поставок и характеризующих исходными данными по каждому из типов знаний, предлагается определять по формуле

$$R_{\text{брака}}(T_{\text{зад}}) = 1 - \sum_{j=1}^J L_j [1 - R_{\text{брака } j}(T_{\text{зад } j})] / \sum_{j=1}^J L_j, \quad (9)$$

где $T_{\text{зад}}$ – задаваемое суммарное время поставки всего множества знаний различных типов, включающее в себя все частные значения $T_{\text{зад } j}$ с учетом их наложений;

L_j – количество учитываемых поставок знаний j -го типа при множественных поставках, в выражении для обобщенного риска применительно к процессу приобретения использовано обозначение $L(\text{пр})_j, j=1, \dots, J(\text{пр})$ – см. выражение (10).

4.5 Расчеты вероятностей нарушения надежности создания полезных знаний и распространения приобретенных или созданных полезных знаний о системе без учета требований по защите информации осуществляются аналогичным образом по собираемой статистике.

4.6 Обобщенный риск нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации оценивают с использованием расчетных вероятностей, описанных в 4.2-4.5.

Обобщенную вероятность $R_{\text{обобщен}}(T_{\text{зад}})$ нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации предлагается определять по формуле

$$\begin{aligned}
R_{\text{обобщен}}(T_{\text{зад}}) = & 1 - [1 - Z_{\text{полезн}}(T_{\text{зад}})] \cdot \\
& \cdot \left\{ \sum_{k=1}^{K(\text{пр})} W(\text{пр})_k [1 - Z(\text{пр})_{\text{действий } k}(T_{\text{зад } k})] \right. \\
& + \sum_{k=1}^{K(\text{созд})} W(\text{созд})_k [1 - Z(\text{созд})_{\text{действий } k}(T_{\text{зад } k})] + \\
& + \sum_{i=1}^{I(\text{пр})} M(\text{пр})_i [1 - Z(\text{пр})_{\text{сроки } i}(T_{\text{зад } i})] + \sum_{i=1}^{I(\text{созд})} M(\text{созд})_i [1 - Z(\text{созд})_{\text{сроки } i}(T_{\text{зад } i})] + \\
& + \sum_{j=1}^{J(\text{пр})} L(\text{пр})_j [1 - Z(\text{пр})_{\text{брака } j}(T_{\text{зад } j})] \\
& + \sum_{j=1}^{J(\text{созд})} L(\text{созд})_j [1 - Z(\text{созд})_{\text{брака } j}(T_{\text{зад } j})] \} / \left[\sum_{k=1}^{K(\text{пр})} W(\text{пр})_k \right. \\
& + \sum_{i=1}^{I(\text{пр})} M(\text{пр})_i \\
& + \sum_{j=1}^{J(\text{пр})} L(\text{пр})_j + \sum_{k=1}^{K(\text{созд})} W(\text{созд})_k + \sum_{i=1}^{I(\text{созд})} M(\text{созд})_i + \sum_{j=1}^{J(\text{созд})} L(\text{созд})_j \Big],
\end{aligned}
\tag{10}$$

где обозначения для аналогичны введенным в 4.2-4.4, $T_{\text{зад}}$ – задаваемое суммарное время, включающее в себя все частные значения $T_{\text{зад } k}$, $T_{\text{зад } i}$, $T_{\text{зад } j}$ (соответственно для приобретения, создания и распространения знаний) с учетом их наложений.

Если все условия по завершению необходимых действий процесса управления знаниями о системе, выполнению сроков поставки знаний, отсутствию брака в поставке приобретаемых и создаваемых знаний, распространению и применению полезных знаний выполнены, то вероятность нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации обращается в ноль, что означает, что риски не превышают допустимых. В ином случае требуется поиск мер снижения рисков с использованием предложенных и/или иных приемлемых методов.

4.7 В сопоставлении с возможным ущербом интегральный риск нарушения реализации процесса управления знаниями о системе с учетом требований по защите информации $R_{\text{интегр}}(T_{\text{зад}})$ для прогнозного периода $T_{\text{зад}}$ предлагается вычислять по формуле

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - [1 - R_{\text{обобщен}}(T_{\text{зад}})] \cdot [1 - R_{\text{наруш}}(T_{\text{зад}})], \tag{11}$$

где $R_{\text{обобщен}}(T_{\text{зад}})$ – вероятность нарушения надежности реализации процесса управления знаниями о системе в течение периода прогноза $T_{\text{зад}}$ без учета требований по защите информации, рассчитывается по 4.2-4.6;

$R_{\text{наруш}}(T_{\text{зад}})$ – вероятность нарушения требований по защите информации для процесса управления знаниями о системе в течение периода прогноза $T_{\text{зад}}$, может быть рассчитана доступными методами, например по ГОСТ Р 59341-2021.

Вывод

Предлагаемые методы позволяют анализировать на уровне вероятностных показателей различные риски для процесса управления знаниями о системе. Достоверность подтверждена на уровне реализации методов по предложениям авторов статьи в ГОСТ Р 59335-2021 «Системная инженерия. Защита информации в процессе управления знаниями о системе». Ожидается, что рациональное использование предложенных методов в жизненном цикле систем будет способствовать выявлению «узких мест» и снижению рисков при приобретении, создании и распространении полезных знаний о системе с учетом требований по защите информации.

Литература

1. Костокрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд. «Вооружение, политика, конверсия», 2008. – 404с.
2. Andrey Kostogryzov, Andrey Nistratov, George Nistratov Some Applicable Methods to Analyze and Optimize System Processes in Quality Management // InTech. 2012. P. 127–196. URL = <http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management>
3. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G. Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V. 1. P. 217–244. <http://www.scirp.org/journal/ajor/>
4. Andrey Kostogryzov, Pavel Stepanov, Andrey Nistratov, George Nistratov, Oleg Atakishchev and Vladimir Kiselev Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling // Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186–192. www.dropbox.com/s/a4zw1yds8f4ecc5/AMSM2016%20Full%20Proceedings.pdf?dl=0
5. Костокрызов А.И., Степанов П.В., Нистратов А.А., Григорьев Л.И., Червяков Л.М. Прогнозирование рисков для обеспечения качества информации в сложных системах // Системы высокой доступности №3, т.2, 2016, с. 25–37
6. Vladimir Artemyev, Andrey Kostogryzov, Jury Rudenko, Oleg Kurpatov, George Nistratov, Andrey Nistratov Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20–22, 2017, Milan, Italy, pp. 368–373
7. Vsevolod Kershenbaum, Leonid Grigoriev, Petr Kanygin and Andrey Nistratov / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, pp. 55–79. <http://dx.doi.org/10.5772/intechopen.74963>
8. Probabilistic Modeling in System Engineering. / By ed. A.Kostogryzov, - London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
9. Костокрызов А.И. Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта / БИТ. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019, сс. 220–229
10. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352–364. <https://www.springer.com/gp/book/9783030468941>

Methods of analysis for system knowledge management

Avdonin R.Y.¹⁰, Kostogryzov A.I.¹¹, Nistratov A.A.¹²

Abstract.

Methods are proposed that allow analyzing various risks in the acquisition, creation and dissemination of useful knowledge about the system, taking into account the requirements for information protection. The use of the proposed methods in the life cycle of systems will help to identify "bottlenecks" and reduce the integral risk of disrupting the process of system knowledge management.

Keywords: *analysis, protection of information, model, risk, knowledge management.*

¹⁰ Avdonin R.Y, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow

¹¹ Kostogryzov A.I, Dr.Sc., Prof., Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow

¹² Nistratov A.A., Ph.D., "Scientific&Technical Center Energobezopasnost", Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow

Оценка информационного риска методом декомпозиции и анализа сетевых и иерархических структур

Аносов С.С.¹³, Шахалов И.Ю.¹⁴

Аннотация. Оценка информационного риска рассмотрена как основная задача технико-экономического обоснования системы защиты информации. В основе рассматриваемого методического подхода лежит трехэтапная декомпозиция:

- декомпозиция сценария инцидента информационной безопасности на этапы возникновения и развития инцидента;
- декомпозиция этапа возникновения инцидента на способы и сценарии действия источника угрозы, являющаяся средством построения отображения из пространства факторов риска в пространство свойств защищаемых активов;
- декомпозиция этапа развития инцидента в форме взаимообусловленной системы защищаемых активов, являющаяся средством построения отображения из пространства свойств активов в пространство ущерба, причиняемого действием источника угрозы.

На основе методов анализа сетевых и иерархических систем получено отображение из пространства факторов риска в пространство уровней риска, тем самым выполнена формализация задачи оценки информационного риска, решаемая в процессе выбора варианта системы защиты информации, оптимального по технико-экономическому критерию.

Ключевые слова: факторы риска, источник угрозы, инцидент, актив, ущерб, система защиты.

Введение

Уровень информационного риска является ключевым показателем, используемым при проектировании и оценке эффективности системы защиты информации по технико-экономическому критерию [1-17]. Технико-экономическая эффективность W системы защиты информации определяется соотношением [1, 2, 9, 10]:

$$W = \frac{R^0 - R^S}{C^S}, \quad (1)$$

где R^0 – уровень информационного риска в отсутствии системы защиты (исходный риск); R^S – уровень информационного риска при наличии системы защиты (остаточный риск); $R^0 - R^S$ – величина риска, предотвращенного системой защиты; C^S – затраты на систему защиты (издержки).

Технико-экономическое обоснование системы защиты информации заключается в решении следующих задач:

формирование множества вариантов системы защиты $S = \{S_1, S_2, \dots\}$;

сопоставление ресурсоемкости C^S вариантов системы $S \in S$ и предотвращенного ими риска $R^0 - R^S$;

¹³ Аносов Сергей Сергеевич, начальник отдела, государственное унитарное предприятие «Научно-технический центр «Заря», г. Москва, Россия. E-mail: serg-anosov@mail.ru

¹⁴ Шахалов Игорь Юрьевич, доцент МГТУ им. Н.Э. Баумана, Акционерное общество «Научно-производственное объединение «Эшелон», г. Москва, Россия. E-mail: i-shahalov@npo-echelon.ru

выбор оптимального варианта системы защиты S^* среди множества вариантов S^w , удовлетворяющих критерию технико-экономической эффективности: $W > 1$.

В качестве критерия выбора варианта системы защиты применяется, как правило, один из следующих критериев:

наибольшее снижение риска при заданных ресурсных ограничениях C^* и предельно допустимом уровне остаточного риска R^* :

$$S^* = \underset{S \in S^w \wedge C^S \leq C^* \wedge R^S \leq R^*}{argmax} \{R^0 - R^S(C^S)\} = \underset{S \in S^w \wedge C^S \leq C^* \wedge R^S \leq R^*}{argmin} \{R^S(C^S)\}; \quad (2)$$

минимизация ресурсоемкости C^S системы защиты при заданном предельно допустимом уровне остаточного риска R^* :

$$S^* = \underset{S \in S^w \wedge R^S \leq R^*}{argmin} \{C^S\}. \quad (3)$$

В общем случае риск является многомерной величиной, характеризующейся вектором частных рисков причинения ущерба j -го вида $R = (R_1, R_2, \dots)$ [11, 12]:

$$R_j = \sum_k U_{jk} v_k, \quad (4)$$

где U_{jk} – возможный ущерб j -го вида при k -м сценарии инцидента; v_k – вероятность k -го сценария.

Модель развития инцидента

Связи в системе защищаемых активов (рис. 1) будем характеризовать весовыми коэффициентами, имеющими следующий смысл:

вес a_{ij} связи, направленной от актива A_i к активу A_j , означает относительный вклад актива A_i в свойства актива A_j по сравнению с вкладом других активов, также влияющих на свойства A_j ;

вес a_{ij}^* связи, направленной от актива A_i к ущербу U_j , означает относительный вклад актива A_i в величину ущерба U_j по сравнению с вкладом других активов, также влияющих на величину U_j .

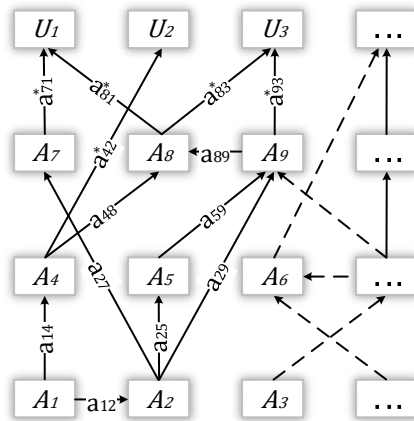


Рис. 1. Размеченный граф влияния активов

Относительное влияние, которое оказывают одни активы на свойства других, представляется векторами приоритетов, полученными на основе парных сравнений [13]. При проведении парных сравнений необходимо ответить на вопрос: для заданного элемента (актива или вида ущерба), на свойства которого оказывается влияние, и сравниваемой пары элементов (активов), оказывающих влияние, насколько сильнее влияние данного элемента пары по сравнению с влиянием другого элемента пары? На основании ответов формируются обратно-симметричные матрицы доминирования, из которых вычислением главных

собственных векторов выводятся векторы приоритетов $(a_{i_1j}, a_{i_2j}, \dots)$, ранжирующие множество элементов $\{A_{i_1}, A_{i_2}, \dots\}$, влияющих на элемент A_j , по относительной интенсивности этого влияния [14, 15].

Присвоим каждой вершине-активу параметр, определяющий степень ухудшения (утраты) свойств актива в результате действия источника угрозы. Множество таких параметров обозначим $\mathbf{P} = (p_1, p_2, \dots, p_m)$, где $p_i = 0$ в отсутствии влияния угрозы на свойства i -го актива и $0 < p_i \leq 1$ в условиях наличия такого влияния, m – количество активов в системе. Параметрам вершин-ущербов $(p_{m+1}, p_{m+2}, \dots, p_{m+n})$ присвоим значения максимальных ущербов соответствующих видов $\bar{U}_j \in \bar{\mathbf{U}} = (\bar{U}_1, \bar{U}_2, \dots, \bar{U}_n)$, возникающих в случае полной компрометации всех связанных с ними активов. Тогда отображение вектора параметров $\mathbf{P}$ в пространство ущербов $\mathbf{U} = (U_1, U_2, \dots, U_n)$, $\mathbf{P} \rightarrow \mathbf{U}$, определяет возможные негативные последствия и может быть задано следующей циклической схемой:

устанавливается общая нумерация вершин-активов $\{A_1, A_2, \dots, A_m\}$, вершин-ущербов $\{A_{m+1}, A_{m+2}, \dots, A_{m+n}\}$ и весовых коэффициентов a_{ij} : $i = \overline{1, m}$; $j = \overline{1, m+n}$;

для каждой i -й вершины графа, не имеющей входных связей, пересчитываются значения параметров тех вершин, которые подвержены влиянию с ее стороны, $\forall j \neq i: p_j = p_j + p_i a_{ij}$;

производится усечение графа удалением подмножества вершин, не имеющих входных связей;

до тех пор, пока множество вершин графа не пусто, осуществляется переход в начало цикла.

В результате реализации данной схемы значения параметров вершин-ущербов $(p_{m+1}, p_{m+2}, \dots, p_{m+n})$ будут равны ущербам $(U_{1k}, U_{2k}, \dots, U_{nk})$, возникающим в результате сценария инцидента, заданного вектором параметров $(p_1, p_2, \dots, p_m)$.

Рассмотренное отображение $\mathbf{P} \rightarrow \mathbf{U}$ определяет интегральное влияние ухудшения свойств активов, подвергшихся действию источника угрозы, на величину ущерба.

Модель возникновения инцидента

Будем полагать, что всевозможные угрозы заданы множеством $\mathbf{T} = \{T_1, T_2, \dots\}$, где каждая k -я угроза $T_k = (O_k, \mathbf{D}_k)$ определяется источником угрозы O_k и возможными способами действия источника угрозы $\mathbf{D}_k = (D_{1k}, D_{2k}, \dots)$. Способ действия источника угрозы D_{ik} , в свою очередь, характеризуется объектами, на которые может оказываться действие (активами, каналом и интерфейсом доступа к ним), используемыми уязвимостями объектов действия, свойствами активов $\mathbf{P}_{ik} \subset \mathbf{P}$, на которые оказывается действие, сценариями действия [4].

Представим действие источников угроз на активы в виде иерархической структуры (рис. 2):

на верхнем уровне иерархии располагаются источники угроз;

на втором уровне – возможные способы действия каждого источника угрозы;

на третьем уровне – возможные сценарии осуществления способов действия.

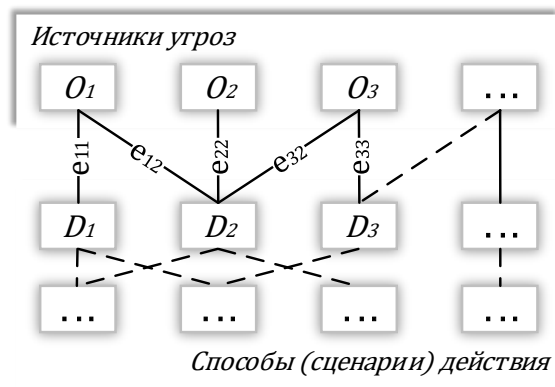


Рис. 2. Иерархия «источники угроз – способы действия»

Присвоим каждому источнику вектор параметров $\bar{P}_k = (\bar{p}_{1k}, \bar{p}_{2k}, \dots)$, где $0 \leq \bar{p}_{ik} \leq 1$ – потенциальные возможности k -го источника по ухудшению свойств (компрометации) i -го актива. Весовые коэффициенты связей в иерархии способов действия зададим вектором $e_{jl} = (g_{jl}, q_{jl})$, где $0 \leq g_{jl} \leq 1$. Применительно к связям между элементами первого и второго уровней иерархии («источники – способы») g_{jl} обозначает степень реализации потенциала j -го источника l -м способом действия, q_{jl} – вероятность действия j -го источника l -м способом, $\sum_l q_{jl} \leq 1$ – вероятность того, что j -м источником будет реализовываться хотя бы один из возможных способов действия. Для уровней иерархии, начиная со второго («способы – сценарии»), g_{jl} обозначает степень реализации потенциала j -го способа действия l -м сценарием действия; q_{jl} – вероятность реализации j -го способа действия l -м сценарием; $\sum_l q_{jl}$ – вероятность того, что j -й способ действия будет реализован хотя бы одним из возможных сценариев.

Учитывая, что параметры потенциальных возможностей источника угрозы $\bar{p}_{ik}$ и параметры компрометации свойств актива p_i относятся к одному и тому же активу (свойству актива), степень компрометации свойств i -го актива в результате действия k -го источника p_{ik} может быть определена с учетом всевозможных комбинаций «способ действия – сценарий действия»:

$$p_{ik} = \bar{p}_{ik} \sum_{j_1} g_{kj_1} q_{kj_1} \sum_{j_2} g_{j_1 j_2} q_{j_1 j_2} \dots \sum_{j_N} g_{j_{N-1} j_N} q_{j_{N-1} j_N}, \quad (5)$$

где N – количество уровней в иерархии «способы действия – сценарий действия».

Вероятность действия k -го источника угрозы на активы может быть определена как вероятность того, что хотя бы один из возможных способов действия будет реализован хотя бы одним из возможных сценариев:

$$v_k = \sum_{j_1} q_{kj_1} \sum_{j_2} q_{j_1 j_2} \dots \sum_{j_N} q_{j_{N-1} j_N}. \quad (6)$$

Выводы

Модели возникновения и развития инцидента являются элементами интересующего нас отображения из множества сценариев инцидентов в пространство ущербов $I \rightarrow U$, которое с учетом факторов риска и параметров моделей возникновения и развития инцидента $\theta = (\|a_{ij}\|, \|e_{lm}\|)$ может быть представлено в следующей обобщенной форме:

$$I \xrightarrow{\theta(S)} U. \quad (7)$$

Параметры θ моделей возникновения и развития инцидента устанавливаются на основе экспертных оценок применительно к одному из вариантов построения системы защиты S , что позволяет определять величину ущерба и уровень

остаточного риска R^S , обеспечиваемого этим вариантом, и при наличии информации о стоимости варианта системы защиты оценивать его эффективность по технико-экономическому критерию.

Таким образом, разработана методика, являющаяся инструментом оценки информационного риска и технико-экономического оценивания вариантов системы защиты информации на стадиях ее проектирования и эксплуатации. Выполненная декомпозиция процессов возникновения и развития инцидента информационной безопасности наряду с применением методов анализа сетевых и иерархических структур предоставляет возможность повышения точности оценки риска при снижении требований к квалификации экспертов, а также обеспечивает уровень формализации задачи оценки риска, достаточный для ее автоматизации [10].

Литература

1. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Концептуальная модель анализа риска безопасности информационных технологий // Вопросы кибербезопасности. 2020. № 2 (36). С. 2-10.
2. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Формализованная риск-ориентированная модель системы информационных технологий // Вопросы кибербезопасности. 2020. № 5 (39). С. 69-76.
3. 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.
4. Булдакова Т.И., Миков Д.А. Обеспечение согласованности и адекватности оценки факторов риска информационной безопасности // Вопросы кибербезопасности. 2017. № 3 (21). С. 8-15.
5. Гаськова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2 (30). С. 42-49.
6. Нащекин П.А. Теоретическое обоснование методики проектирования систем защиты информации в виртуальных средах и облачных платформах // Вопросы кибербезопасности. 2020. № 6 (40). С. 14-22.
7. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Академия АйТи: ДМК Пресс, 2004. 384 с.
8. Чукляев И.И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем // Вопросы кибербезопасности. 2016. № 4 (17). С. 61-71.
9. Аносов С.С., Аносов Р.С., Бывших Д.М. Вопросы системного и технико-экономического обоснования информационной безопасности в целях противодействия террористической деятельности // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму, 2020. № 3-4 (141-142). С. 92-102.
10. Казаков О.Д. Разработка методики технико-экономического обоснования внедрения системы защиты информации // Стратегия устойчивого развития экономики регионов: теория и практика: Материалы международной научно-практической конференции, Брянск, 24–26 марта 2015 года. – Брянск: Брянский ГАУ, 2015. – С. 142-147.
11. Боев А.С., Бывших Д.М., Коробейников А.С., Строкова Т.М. Анализ рисков при подготовке научно-технического и технологического задела инноваций // РИСК: Ресурсы. Информация. Снабжение. Конкуренция, 2013. № 3. С. 214–221.

12. Probabilistic Modeling in System Engineering. / By ed. A.Kostogryzov, - London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
13. Сабитова А.Т., Бакланова О.Е. Оценка рисков информационной безопасности // Вестник Восточно-Казахстанского государственного технического университета им. Д. Серикбаева. – 2020. – № 4. – С. 158-164. – DOI 10.51885/15614212_2020_4_158.
14. Луценко А.Д., Бывших Д.М., Шарапов А.И. Методика оценки относительной важности технологий создания специальных систем разведки и информационного обеспечения // Вооружение и экономика, 2008. № 3 (3). С. 31-49.
15. Саати Т.Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. Пер. с англ. / Науч. ред. А.В. Андрейчиков, О.Н. Андрейчикова. М.: ЛЕНАНД, 2019. 360 с.
16. Анализ методик автоматизированной оценки угроз и рисков информационной безопасности информационно-телекоммуникационных систем / Ю. В. Скоредова, Е. В. Гречишников, А. С. Кравченко, О. В. Ланкин // Вестник Воронежского института ФСИИ России. – 2017. – № 3. – С. 128-133.
17. Маковейчук К. А., Петренко С. А. Анализ условий и определение рисков использования облачных технологий в банковской сфере РФ // В сб.: Информационные системы и технологии в моделировании и управлении. IV Всероссийская научно-практическая конференция (с международным участием). Посвящается 75-летию Гуманитарно-педагогической академии (филиал) ФГАОУ ВО "КФУ им. В. И. Вернадского" в г. Ялте. - 2019. - С. 133-138.

Information risk assessment by decomposition and analysis of network and hierarchical structures

Anosov S.S.¹⁵, Shakhlov I.Yu.¹⁶

Abstract. *Information risk assessment is considered as the main task of the feasibility study of the information security system. The methodological approach under consideration is based on a three-stage decomposition:*

- *decomposition of the information security incident scenario into the stages of occurrence and development of the incident;*
- *decomposition of the incident occurrence stage into methods and scenarios of the threat source action, which is a means of constructing a mapping from the space of risk factors to the space of properties of protected assets;*
- *decomposition of the incident development stage in the form of a mutually dependent system of protected assets, which is a means of constructing a mapping from the space of asset properties to the space of damage caused by the action of the threat source.*

Based on the methods of analysis of network and hierarchical systems, a mapping from the space of risk factors to the space of risk levels is obtained, thereby formalizing the task of information risk assessment, which is solved in the process of choosing the optimal information security system according to the technical and economic criterion.

Keywords: *risk factors, threat source, incident, asset, damage, protection system.*

¹⁵ Sergey Anosov, State Unitary Enterprise «Scientific and Technical Center «Zarya», Moscow, Russia. E-mail: serg-anosov@mail.ru

¹⁶ Igor Shakhlov, Associate Professor of Bauman Moscow State Technical University, Scientific-Production Association Echelon Joint-Stock Company, Moscow, Russia. E-mail: i-shahlov@npoechelon.ru

Method for collecting architecture security-specific information for microservice-based systems

Barabanov A.V.¹⁷

Abstract. *The microservice architecture is being increasingly used for designing and implementing application systems in both cloud-based and on premise infrastructures. There are many security challenges need to be addressed in the application design and implementation phases. In order to address some security challenges, it is necessity to collect security-specific information on application architecture. The goal of this article is to provide a concrete proposal of approach to collect microservice-based architecture information to securing application that can be applicable in immature processes and agile development.*

Keywords: *microservices, microservice architectures, security, architecture artifacts, architecture documentation*

1. Introduction

During application development based on microservices architecture security architects/engineers usually face with the questions related with attack surface analysis, data leakage analysis and application components business/security functions verification [1, 2, 3] to build secure application and minimize number of vulnerabilities and threats [4, 5]. In most cases, existing application architecture documentation is not suitable to answer those questions. Moreover, usually in agile development practices source code and presentation slides are the only artifacts available for application security architect. Therefore, application security architect has to collect a necessity information and use it in secure software development activities. Various techniques [6, 7, 8] have been developed and applied to document microservice-based system architecture but in most cases, it can be applied in mature software development lifecycle processes and do not focus on application security aspects. In this paper we propose a novel approach to collect microservice-based architecture information and use it for securing application that can be applicable in immature processes and agile development.

2. Proposed method for collecting architecture security-specific information

Proposed method consists of several steps described below.

Step 1: Identify and describe application-functionality services

Application-functionality services implement one or several business process or functionality (e.g., storing customer details, storing and displaying product catalog). Collect information on the parameters listed below related to each application-functionality service:

- unique service name or ID;
- short description of business process or functionality implemented by the microservice;
- link to source code repository;
- development team which develops the microservice
- API definition (e.g., OpenAPI specification).

Step 2: Identify and describe infrastructure services

Infrastructure services including remote services may implement authentication,

¹⁷ Alexander Barabanov, Ph.D, CISSP, CSSLP, Advanced Software Technology Laboratory, Huawei, Moscow, Russia, barabanov.iu8@gmail.com

authorization, service registration and discovery, security monitoring, logging etc. Collect information on the parameters listed below related to each infrastructure service:

- unique service name or ID;
- short description of functionality implemented by the service (e.g., authentication, authorization, service registration and discovery, logging, security monitoring, API gateway);
- link to source code repository;
- link to the service documentation.

Step 3 Identify and describe data storages

Collect information on the parameters listed below related to each data storage:

- unique storage name or ID;
- software type, i.e. software that implements the data storage (e.g., PostgreSQL, Redis, Apache Cassandra).

Step 4: Identify and describe message queues

Messaging systems (e.g., RabbitMQ or Apache Kafka) are used to implement asynchronous microservices communication mechanism. Collect information on the parameters listed below related to each message queue: unique message queue name or ID and software type, i.e. software that implements the message queue (e.g., RabbitMQ, Apache Kafka).

Step 5: Identify and describe data assets

Identify and describe data assets that processed by system microservices/services. It is advisable firstly to identify assets, which are valuable from a security perspective (e.g., “User information”, “Payment”). Collect information on the parameters listed below related to each asset: unique asset name or ID and protection level, e.g., PII, confidential.

Step 6: Identify “service-to-storage” relations

Collect information on the parameters listed below related to each “service-to-storage” relation:

- service name (ID);
- storage name (ID);
- access type, i.e. specify access type, e.g. “Read” or “Read/Write”.

Step 7: Identify "service-to-service" synchronous communications

Collect information on the parameters listed below related to each “service-to-service” synchronous communication:

- caller service name (ID);
- called service name (ID);
- protocol/framework used, i.e. specify protocol/framework used for communication, e.g. HTTP (REST, SOAP), Apache Thrift, gRPC;
- shortly describe the purpose of communication (requests for query of information or request/commands for a state-changing business function) and data passed between services (if possible, in terms of assets defined above).

Step 8: Identify “service-to-service” asynchronous communications

Collect information on the parameters listed below related to each “service-to-service” asynchronous communication.

- publisher service name (ID);
- subscriber service name (ID);
- message queue (ID);
- shortly describe the purpose of communication (receiving of information or commands for a state-changing business function) and data passed between services (if

possible, in terms of assets defined above).

Step 8: Identify “asset-to-storage” relations

Collect information on the parameters listed below related to each “asset-to-storage” relation:

- Asset name (ID);
- Storage name (ID);
- Specify storage type for the asset, e.g. “golden source” or “cache”.

It is advisable to follow “architecture-as-a code” [9] practice and create graphical presentation of application architecture (building blocks and relations defined above) in form of services call graph or data flow diagram. In order to do that one can use special software tools (e.g. Enterprise Architect) or DOT language. An example of using DOT language to describe a simple microservice-based application architecture is the following:

```
digraph architecture {
    rankdir=LR;

    subgraph client_side_app {
        front_end -> {API_GW} [label = "HTTPS"]
    }

    subgraph api_gateways {
        API_GW -> {AuthN, ms_1, ms_2, ms_3} [label = "HTTP"]
    }

    subgraph microservices {
        ms_1 -> {DB} [label="JDBC"]
        ms_2 -> {Queue} [label="gRPC"]
        ms_3 -> {Queue} [label="gRPC"]
    }
}
```

That code can be transformed to the following graphical presentation (Figure 1).

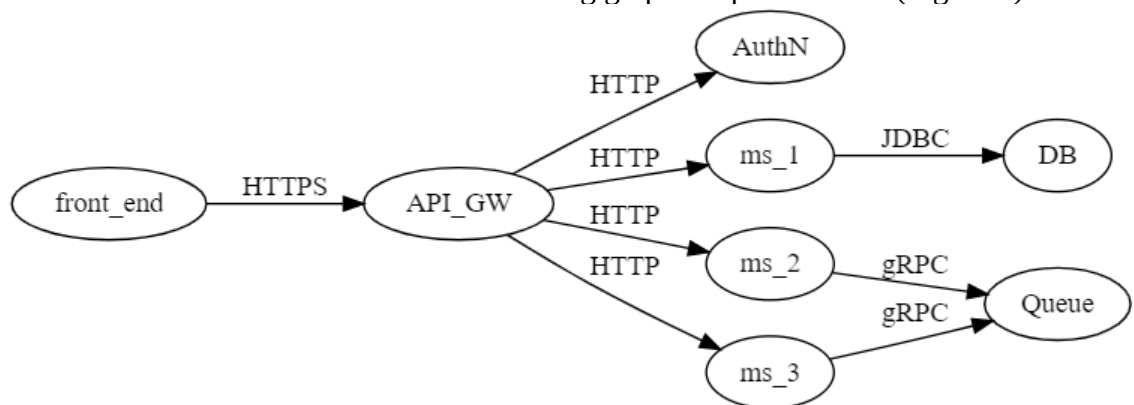


Fig.1. Example of using DOT language to describe microservice-based system architecture

3. Conclusion

In this paper, we presented a method for collecting architecture security-specific information for microservice-based systems that can be used even in immature software

development processes to secure application. Collected information may be useful for doing application security practices during defining security architecture: attack surface analysis, data leakage analysis, analysis of the application's high-level architecture, enforcement of the principle of least privilege and sensitive data identification and classification in secure software development lifecycle [10, 11, 12]. We tested our approach during development of microservice-based system in Oil & Gas automation and received a positive feedback. We also contributed that approach to OWASP Community in Cheat sheet series.

References

1. Alexander Barabanov, Alexey Markov, Andrey Fadin, Valentin Tsirlov, and Igor Shakhlov. 2015. Synthesis of secure software development controls. In Proceedings of the 8th International Conference on Security of Information and Networks (SIN '15). Association for Computing Machinery, New York, NY, USA, 93–97. DOI:<https://doi.org/10.1145/2799979.2799998>
2. M. Kleeaus and F. Matthes, "Challenges in Documenting Microservice-Based IT Landscape: A Survey from an Enterprise Architecture Management Perspective," 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC), Paris, France, 2019, pp. 11-20, doi: 10.1109/EDOC.2019.00012.
3. Barabanov A., Makrushin D., Authentication and authorization in microservice-based systems: survey of architecture patterns // Voprosy kiberbezopasnosti, №4 (38), 2020. pp 32-43. DOI: DOI: 10.21681/2311-3456-2020-04-32-43
4. Barabanov A.V., Markov A.S., Tsirlov V.L. Statistics of Software Vulnerability Detection in Certification Testing // Journal of Physics: Conference Series. 2018. V. 1015. P. 042033.
5. A. V. Barabanov, A. S. Markov, M. I. Grishin and V. L. Tsirlov, "Current Taxonomy of Information Security Threats in Software Development Life Cycle," 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT), Almaty, Kazakhstan, 2018, pp. 1-6, doi: 10.1109/ICAICT.2018.8747065.
6. B. Mayer and R. Weinreich, "An Approach to Extract the Architecture of Microservice-Based Software Systems," 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE), Bamberg, 2018, pp. 21-30, doi: 10.1109/SOSE.2018.00012.
7. G. Granchelli, M. Cardarelli, P. D. Francesco, I. Malavolta, L. Iovino and A. D. Salle, "Towards Recovering the Software Architecture of Microservice-Based Systems," in IEEE International Conference on Software Architecture Workshops. IEEE, Apr. 2017, pp. 46–53.
8. G. Granchelli, M. Cardarelli, P. D. Francesco, I. Malavolta, L. Iovino, and A. D. Salle, "MicroART: A Software Architecture Recovery Tool for Maintaining Microservice-Based Systems," in IEEE International Conference on Software Architecture Workshops. IEEE, Apr. 2017, pp. 298–302.
9. E. Yuan, "Architecture Interoperability and Repeatability with Microservices: An Industry Perspective," 2019 IEEE/ACM 2nd International Workshop on Establishing the Community-Wide Infrastructure for Architecture-Based Software Engineering (ECASE), Montreal, QC, Canada, 2019, pp. 26-33, doi: 10.1109/ECASE.2019.00013.
10. M. Ruggieri, T. Hsu and M. L. Ali, "Security Considerations for the Development of Secure Software Systems," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2019, pp. 1187-1193, doi: 10.1109/UEMCON47517.2019.8993081.
11. A. Ramirez, A. Aiello and S. J. Lincke, "A Survey and Comparison of Secure Software Development Standards," 2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges(51275), Copenhagen, Denmark, 2020, pp. 1-6, doi: 10.1109/CMI51275.2020.9322704.
12. R. A. Khan, S. U. Khan, H. U. Khan and M. Ilyas, "Systematic Mapping Study on Security Approaches in Secure Software Engineering," in IEEE Access, vol. 9, pp. 19139-19160, 2021, doi: 10.1109/ACCESS.2021.3052311

Метод сбора информации об архитектуре микросервисного приложения для решения задач безопасной разработки

А.В. Барабанов¹⁸

***Аннотация.** В настоящее время разработка программ на базе микросервисов является популярным архитектурным подходом, применяемым при создании систем, функционирующих в облачных средах или собственной инфраструктуре пользователя. Для решения задач безопасной разработки таких приложений инженеры по безопасной разработке должны собирать, актуализировать и использовать в работе информацию об архитектуре системы. В данной работе предложен метод сбора информации об архитектуре микросервисного приложения для решения задач безопасной разработки, который может быть использован в условиях использования гибкой методологии разработки и отсутствия ранее установленных процессов документирования архитектуры.*

***Ключевые слова:** микросервисная архитектура, безопасная разработка, документирование архитектуры.*

¹⁸ Александр Владимирович Барабанов, кандидат технических наук, CISSP, CSSLP, Лаборатория передовых программных технологий, компания Huawei, Москва, Россия. E-mail: barabanov.iu8@gmail.com

Исследование функционирования SIEM - систем с помощью различных корреляторов для бинарных последовательностей вида (1, -1) при условии, что случайные величины принимают свои значения с одинаковыми вероятностями

Басараб М.А.¹⁹, Троицкий И.И.²⁰, Онуфриева Е.В.²¹

Аннотация. Целью данной работы являлось исследование возможности использования корреляторов для функционирования SIEM - систем. SIEM - система является центральным звеном контроля информационной безопасности и работы средств защиты информации. Она глубоко интегрирована в инфраструктуру корпоративной сети, поэтому требует унификации поступающей в нее информации и ее перекрестного анализа в едином интерфейсе. В рамках данного исследования была решена задача оценки коэффициента корреляции двух бинарных последовательностей вида (1, -1) при условии, что случайные величины принимают свои значения с одинаковыми вероятностями $p = 1/2$, с помощью математического аппарата, представленного в данной работе.

Ключевые слова: SIEM – система, защита информации, корреляция событий безопасности, корреляционный анализ, коэффициент корреляции.

Введение

Одним из современных подходов к решению задач защиты информации корпоративных сетей, позволяющих обеспечивать безопасность систем любого уровня и набора устройств, являются системы управления информацией и событиями безопасности SIEM (Security information event management) [1]. Преимущество данных решений заключается в гибкости применения и независимости от набора спецификаций и платформ для конечной защищаемой инфраструктуры [2, 3].

Наибольшей вычислительной сложностью обладает операция корреляции событий безопасности [4, 5]. Суть этой операции заключается в определении причинно-следственных связей между поступающими на обработку событиями. Это позволяет выявлять вредоносную и аномальную активности, определять источник и цель атаки, обнаруживать многошаговые атаки, делать выводы об инцидентах безопасности и вырабатывать эффективные контрмеры [6-11]. В этом плане рассмотрим задачу оценки коэффициента корреляции событий [12].

Расчет оценки коэффициента корреляции двух бинарных последовательностей вида (1, -1)

Имеется 2 ряда бинарных данных:

$$x = \{1, -1, -1, \dots, 1\}, \quad x_i, \quad i = \overline{1, N}$$

¹⁹ Басараб Михаил Алексеевич, д.ф.-м.н., профессор, МГТУ им. Н.Э. Баумана, Москва, bmic@mail.ru

²⁰ Троицкий Игорь Иванович, к.т.н., доцент, МГТУ им. Н.Э. Баумана, Москва, iitroickiy@mail.ru

²¹ Онуфриева Евгения Валерьевна, старший преподаватель, МГТУ им. Н.Э. Баумана, Москва, evgeni.bmstu@yandex.ru

$$y = \{1, 1, -1, \dots, -1\}, \quad y_i, \quad i = \overline{1, N}$$

Известно, что коэффициент корреляции вычисляется по следующей формуле²²:

$$r = \frac{K_{xy}}{\sigma_x \cdot \sigma_y}, \quad (1)$$

где $K_{xy} = M[(x_i - m_x) \cdot (y_i - m_y)]$ – ковариация величин x и y ,

m_x и m_y – математические ожидания величин x и y ,

σ_x , σ_y – средние квадратические отклонения величин x и y .

Пусть x и y принимают значения 1 и -1 с вероятностью 1/2:

$$x = \begin{cases} 1, p = \frac{1}{2} \\ -1, p = \frac{1}{2} \end{cases}, \quad y = \begin{cases} 1, p = \frac{1}{2} \\ -1, p = \frac{1}{2} \end{cases}$$

$$\text{Найдем математическое ожидание величины } x: M[x] = 0, \quad (2)$$

$$\text{Вычислим математическое ожидание величины } x^2: M[x^2] = 1, \quad (3)$$

$$\text{Рассмотрим дисперсию величины } \hat{x}: D[x] = M[x^2] - \{M[x]\}^2 = 1 \quad (4)$$

$$\text{Аналогично, для величины } y: M[y] = 0, \quad M[y^2] = 1, \quad D[y] = 1 \quad (5)$$

Найдем средние квадратические отклонения величин x и y :

$$\sigma_x = \sigma_y = \sqrt{D[x]} = \sqrt{D[y]} = 1 \quad (6)$$

Следовательно, коэффициент корреляции величин x и y можно найти по

$$\text{формуле: } \hat{r} = M[x_i \cdot y_i] \quad (7)$$

Оценку коэффициента корреляции найдем по известной формуле²³:

$$r^* = \frac{\sum_{i=1}^n x_i \cdot y_i}{N} \quad (8)$$

где N – объем выборки.

Математическое ожидание оценки коэффициента корреляции:

²² Вентцель Е.С. Теория вероятностей. – М.: Физматлит, 1969. – 366 с.

²³ Пугачев В.С. Теория случайных функций и ее применение к задачам автоматического управления. – Москва: Физматлит, 1960. – 884 с.

$$M[r^*] = M\left[\frac{\sum_{i=1}^N x_i \cdot y_i}{N}\right] = \frac{1}{N} \sum_{i=1}^N M[x_i \cdot y_i] = \hat{r} \quad (9)$$

Дисперсия оценки коэффициента корреляции:

$$D[r^*] = D\left[\frac{1}{N} \sum_{i=1}^N x_i \cdot y_i\right] = \frac{1}{N^2} \sum_{i=1}^N D[x_i \cdot y_i] \quad (10)$$

Рассмотрим одно слагаемое из суммы:

$$D[x_i \cdot y_i] = M[x_i^2 \cdot y_i^2] - \{M[x_i \cdot y_i]\}^2 \quad (11)$$

$$\text{Поскольку } x_i^2 = y_i^2 = 1, \text{ то } D[x_i \cdot y_i] = 1 - \hat{r}^2 \quad (12)$$

$$\text{Следовательно, } D[r^*] = \frac{(1 - \hat{r}^2)}{N} \quad (13)$$

Рассмотрим случай, когда значение коэффициента корреляции $r_{xy} = 0$. В этом случае случайные величины X и Y являются некоррелированными.

Тогда для этого случая доверительный интервал будет равен:

$$P\left\{|r^*| < 3\sqrt{\frac{1}{N}}\right\} = 0,997$$

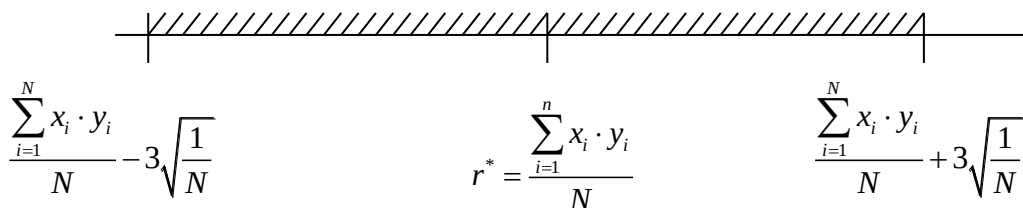
$$\text{Левая граница интервала будет равна: } \frac{\sum_{i=1}^N x_i \cdot y_i}{N} - 3\sqrt{\frac{1}{N}}.$$

$$\text{Правая граница интервала будет равна: } \frac{\sum_{i=1}^N x_i \cdot y_i}{N} + 3\sqrt{\frac{1}{N}}.$$

Здесь возможны три варианта:

- Ноль левее левой границы доверительного интервала, в этом варианте статистическая гипотеза не подтверждается.
- Ноль правее правой границы доверительного интервала, в этом варианте статистическая гипотеза также не подтверждается.
- Ноль внутри доверительного интервала, в этом варианте статистическая гипотеза о равенстве нулю коэффициента корреляции подтверждается и можно сказать, что случайные величины X и Y являются некоррелированными.

Построим доверительный интервал:



Выводы

В рамках данного исследования была решена задача оценки коэффициента корреляции двух бинарных последовательностей вида (1, -1) при условии, что случайные величины принимают свои значения с одинаковыми вероятностями $p = \frac{1}{2}$, с помощью математического аппарата, представленного в данной работе.

Список литературы

1. Пролетарский А.В., Митьковский А.А., Пономарев А.Д. Применение SIEM-системы для защиты информационной инфраструктуры предприятия // Динамика сложных систем - XXI век. 2018. Т. 12. № 4. С. 78-84.
2. Miller D. R. and etc. Security Information and Event Management (SIEM) Implementation. McGraw Hill, 2011. 430 p.
3. 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.
4. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. № 5 (24). С. 2-16.
5. Федорченко А. В., Котенко И. В. Корреляция информации в SIEM-системах на основе графа связей типов событий // Информационно-управляющие системы, 2018. – № 1. – С. 58-67.
6. Кузнецов А.В. Взаимосвязь процесса управления событиями с другими процессами управления предприятия // Вопросы кибербезопасности. 2017. № 5 (24). С. 17-22.
7. Кузнецов А.В., Ненашев С.М. Способ определения регистрируемых событий // Вопросы кибербезопасности. 2015. № 5 (13). С. 23-25.
8. Марков А. С., Фадин А. А. Конвергенция средств защиты информации // Защита информации. Инсайд. -2013. -№ 4. -С. 80-81.
9. Нашивочников Н.В., Большаков А.А., Николашин Ю.А., Лукашин А.А. Проблемные вопросы применения аналитических средств безопасности киберфизических систем предприятий ТЭК // Вопросы кибербезопасности. 2019. № 5 (33). С. 26-33.
10. Петренко С.А., Цирлов В.Л. Импортзамещение решений IDS И SIEM // Защита информации. Инсайд. 2017. № 5 (77). С. 46-51.
11. Рыболовлев Д.А., Карасёв С.В., Поляков С.А. Классификация современных систем управления инцидентами безопасности // Вопросы кибербезопасности. 2018. № 3 (27). С. 47-53.
12. Математические основы информационной безопасности/Басараб М.А., Булатов В.В., Булдакова, Т.И., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г., Медведев Н.В., Троицкий И.И., Чичварин Н.В. и др.: Под ред. Матвеева В.А. -М.: НИИ РИЛ МГТУ им.Н.Э.Баумана, 2013. -244 с.

The investigation of the operation of SIEM - systems using various correlators for binary sequences (1, -1) under condition, that random values take values with same probability

Basarab M.A.²⁴, Troickiy I.I.²⁵, Onufrieva E.V.²⁶

Annotation. *The objective of this research project is to investigate possibilities of using correlators for operation of SIEM (Security information and event management) software systems. SIEM – system is a central link of control of information security and information security operations. This system integrated into an organization's technology infrastructure, therefore, requires unification of all received information and it's cross-analysis in single interface. In this study a problem of estimation of a correlation coefficient of two binary sequences (1, -1) under condition, that random values take values with same probability of $p = 1/2$, was solved, using mathematical model, presented in this work.*

Keywords: *SIEM – system, information security, security event correlation, correlation analysis, correlation coefficient.*

²⁴ Basarab M.A., Dr.Sc., Professor, BMSTU, Moscow, bmic@mail.ru

²⁵ Troickiy I.I., Ph.D., Associate Professor, BMSTU, Moscow, iitroickiy@mail.ru

²⁶ Onufrieva E.V., Assistant Professor, BMSTU, Moscow, evgeni.bmstu@yandex.ru

Разработка учебного имитатора объединенной сети передачи данных категории специального назначения

Бельфер Р.А.²⁷, Кравцов А.В.²⁸

Аннотация. Сложностью алгоритмов построения учебного имитатора единой отечественной сети передачи данных, объединяющей независимые частные сети категории специального назначения, вызвано поэтапное создание имитаторов. Для первых двух версий имитаторов приводятся аппаратно-программные конфигурации и списки разработанных алгоритмов с указанием их описания в статьях ведущих российских научных журналах. Приведена в качестве примера конфигурация иерархической структуры третьей версии, которая позволяет имитировать работу объединенной сети в рамках всей страны. Изложены основные научно-практические направления по созданию учебного имитатора третьей версии.

Ключевые слова: имитатор объединенной сети, иерархическая структура, частная сеть, информационная безопасность, сеть передачи данных.

Введение

Преподавателями и студентами кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана совместно с Научно-исследовательским испытательным центром ЦНИИ ВКС с 2017 года проводится работа по созданию учебного лабораторного стенда (УЛС) аппаратно-программного имитатора сети передачи данных (ПД) специального назначения. Целью этой научно-практической работы – получение студентами знаний и опыта для создания отечественных сетей ПД категории специального назначения, к которым предъявляются высокие требования по надежности, информационной безопасности и другим характеристикам. В соответствии с п.16 ФЗ «О связи» [1] к категории специального назначения относятся сети «для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка». Актуальность построения действующих таких отечественных сетей подчеркивается в резолюции IV конференции «Информационные технологии на службе оборонно-промышленного комплекса России-2015» [2]. В этом документе отмечается недостаточная популяризация отечественных разработок в области телекоммуникационного оборудования, слабая поддержка российских производителей со стороны государства, отсутствие единой современной системы объединенных коммуникаций в сфере ОПК. Для сетей ПД данной категории характерна сложность алгоритмов и соответственно программное обеспечение их реализации. Как отмечается в документе, утвержденном Правительством РФ “Стратегия развития отрасли информационных технологий на 2014-2020 и на перспективу до 2025 года” конкурентным преимуществом России по сравнению с развитыми странами в области телекоммуникации является разработка ПО высокой сложности [3]. Сети ПД данной категории обычно создаются в течение весьма

²⁷ Бельвер Рувим Абрамович, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, a.belfer@yandex.ru

²⁸ Кравцов Александр Владимирович, начальник отдела НИИЦ (Москва) ЦНИИ ВКС, skyak78@gmail.com

длительного периода времени, в таких проектах задействованы большие научно-производственные коллективы высококвалифицированных специалистов. Настоящая работа посвящена результатам поэтапной разработке алгоритмов и ПО каждой из трех версий (аппаратно-программных или программных на одном компьютере) учебного имитатора сети ПД специального назначения с указанием. При этом отмечается основные направления продолжения разработок алгоритмов и ПО на указанных версиях имитатора и на новых версиях, подлежащих разработке.

Особенности сети ПД категории специального назначения по сравнению с сетями связи общего пользования (ССОП)

При разработке учебного имитатора сети ПД категории специального назначения учитываются особенности этих сетей по сравнению с сетями связи общего пользования (ССОП). К ним относятся:

- а) характеристики качества обслуживания отличаются от принятых в сетях связи общего пользования ССОП. Для них характерны высокие требования к количественным показателям качества обслуживания. Состав характеристик зависит от конкретной области использования сети ПД.

В учебном имитаторе сети ПД – это информационная безопасность, надежность, задержка сообщений, вероятность доставки сообщений.

- б) создаются отечественными специалистами на оборудовании отечественных разработок. Следует отметить, что многие технические решения в сетях связи общего пользования не могут быть использованы, так как не соответствуют требованиям поставленных задач создания отечественных сетей ПД специального назначения. Открытые отечественные и зарубежные стандартизированные протоколы не используются.

Решение задач обеспечения информационной безопасности в сетях ПД категории специального назначения отечественными не стандартизированными механизмами относится к специализированным отечественным научно-практическим организациям. В рамках учебного лабораторного стенда перед разработчиками имитатора сети ПД стоит другая задача - составить основные положения архитектуры ИБ объединенной сети ПД категории специального назначения. В некоторых случаях при проведении научно-исследовательских работ создания имитатора используются опубликованные работы и стандарты по ИБ зарубежных сетей ПД ССОП, Smart Grid и др.

- с) поставлена задача создания единой системы объединенных коммуникаций (объединенной сети) в государственных структурах, сети ПД, которых относятся к категории специального назначения. Каждая такая государственная структура может включать несколько частных (изолированных) сетей ПД. Эта задача стоит при создании учебного имитатора сети ПД. Об актуальности создания таких отечественных сетей ПД не только для ОПК говорит атака на внутренние сети ведомства МВД, которая имела место 12 мая 2017 года (газета "Московский Комсомолец", 15 мая, 2017г.).

- d) поставлена задача создания объединенной сети ПД специального назначения, предусматривающая информационное взаимодействие не только внутри государственных структур, но и между определенными оконечными пунктами разных частных сетей ПД (например, внутри МО и МВД РФ, а также между определенными оконечными пунктами частных сетей МО и МВД). Такие соединения будем называть смешанными;
- e) единая система объединенных коммуникаций позволит учитывать не только требования ОПК, но и других ведомств специального назначения (МВД и др.). Об актуальности создания таких отечественных сетей ПД для МВД говорит об атаке на внутренние сети ведомства МВД, которая имела место 12 мая 2017 года (газета "Московский Комсомолец", 15 мая, 2017г.).
- f) единую систему для нескольких областей применения с высокими показателями качества обслуживания позволяет создать коммутируемая сеть ПД из нескольких путей маршрутизации (пучка маршрутов) для передачи в одном соединении одного и того же сообщения (пакета данных и др.);
- g) в действующей сети ПД для обеспечения высоких требований ИБ, надежности и других показателей качества обслуживания необходимо использовать проводные каналы связи, а не беспроводные; для обеспечения надежности в разных путях маршрутизации одного соединения каналы должны принадлежать разным системам для отсутствия корреляции помех и отказов;
- h) большой объем программного обеспечения и сложность в отладке. Это относится к реализации функциям управления сетью, маршрутизации и др.;
- i) на данном этапе разработки имитатора сети ПД в УЛС принята коммутация пакетов данных по логическим адресам (на базе виртуальных каналов). Смена логических адресов при установлении каждого КВК способствует повышению защиты от угроз перехвата. Эта технология используется в сетях связи общего пользования X25, Frame Relay, ATM и в MPLS. Разработка отечественной первичной сети уплотненного волнового мультиплексирования DWDM (Dense Wave Division Multiplexing) для создания оптических магистралей, работающих на терабитных скоростях, дает основание для проведения научно-исследовательской работы для сравнения по технико-экономическим показателям имитаторов сети ПД специального назначения на коммутации каналов с настоящим направлением создания имитатора на коммутации пакетов. Это следует учесть в научно-исследовательских работах по созданию имитатора сети ПД.

Структурная схема и функции имитатора сети ПД первой версии

Имитатор сети ПД первой версии позволяет установить только одну группу изолированных между собой частных сетей ПД категории специального назначения для одного из государственных ведомств, указанных в п. 16 ФЗ «О связи». Приведенная на рис. 1 конфигурация имитатора сети ПД в УЛС позволяет создавать пучок маршрутов между оконечными пунктами, состоящий из четырех путей маршрутизации. Каждый путь маршрутизации включает три центра

коммутации пакетов (ЦКП). К двум оконечным ЦКП в каждом пути маршрутизации (ЦКП1.1, ЦКП3.1 и ЦКП1.2, ЦКП3.2) подключены оконечные пункты, а ЦКП2.1 и ЦКП2.2 являются транзитными. Доступ оконечных пунктов ($a, b, \dots, c$ и $d, e, \dots, f$) к центру коммутации пакетов удаленный. Оконечные пункты коммутируемых виртуальных каналов обмениваются данными одновременно по четырем путям маршрутизации.

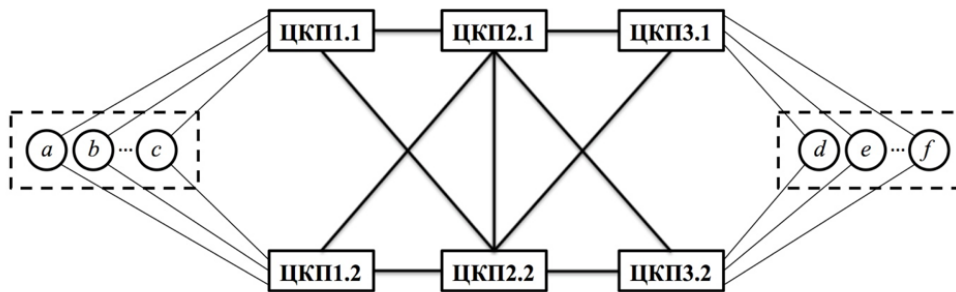


Рис.1. Конфигурация имитатора сети ПД первой версии

На рис. 2 показана аппаратная реализация абонентского участка первой версии имитатора сети ПД

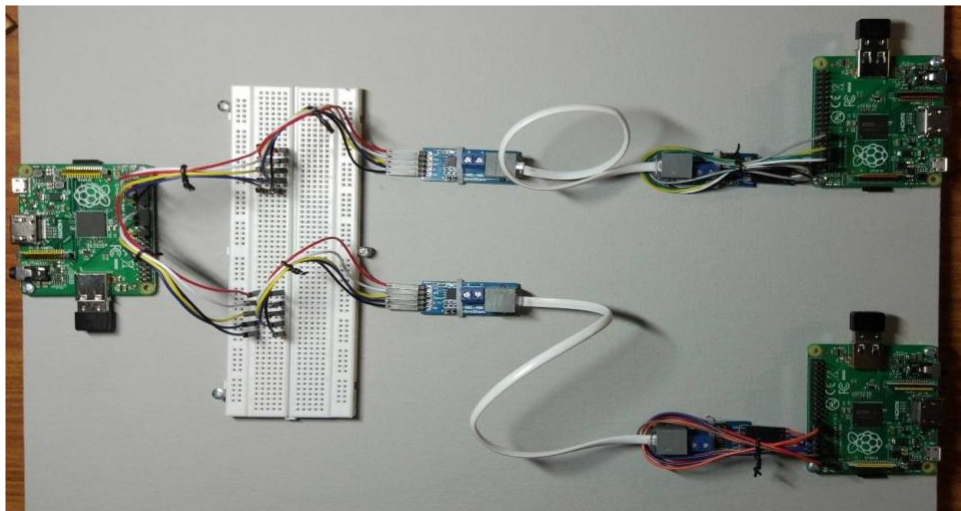


Рис.2 Аппаратная реализация абонентского участка первой версии имитатора сети ПД

В работах [4-6 и др.] приводятся разработанные алгоритмы первой версии имитатора:

- алгоритм функционирования защищенной сети ПД на базе виртуальных каналов с высокими требованиями к качеству обслуживания [4];
- алгоритм установления виртуального соединения на абонентском доступе передачи данных [5];
- алгоритм программного обеспечения взаимной аутентификации абонентского доступа [6]. В основу приведенного алгоритма принят стандартизированный протокол Европейского института стандартизации ETSI ETS 300 841 мультимедийной сети ISDN на базе инфраструктуры открытых ключей PKI (Public Key Infrastructure). Он был реализован, в

частности, на сети связи общего пользования немецкого оператора Deutschen Telecom. Рассматривается одноуровневая и двухуровневая иерархия сертификатов с общим центром сертификации

Структурная схема и функции имитатора сети ПД второй версии

Имитатор сети ПД второй версии экономически более целесообразен по сравнению с имитатором первой версии за счет создания объединенной (единой) сети, включающей несколько групп изолированных частных сетей (ЧС) имитатора сети специального назначения. На рис. 3 приведена конфигурация имитатора сети ПД второй версии, которая отличается от первой версии введением Центра эксплуатации сети (ЦЭС) и единого Удостоверяющего центра УЦ (CA, Certificate Authority). Функции ЦЭС и УЦ приведем ниже. На рис. 4 показана аппаратная реализация абонентских участков, транспортной сети и ЦЭС этого имитатора.

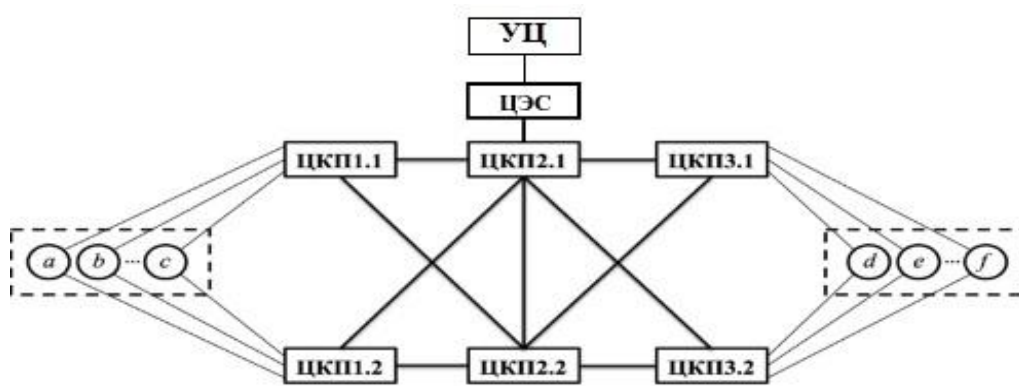
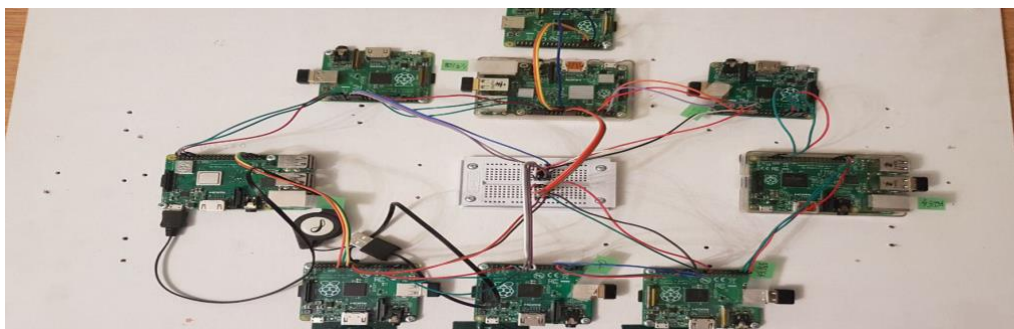


Рис.3. Конфигурация имитатора сети ПД второй версии

На рис. 4 показана аппаратная реализация абонентского участка и транспортной сети второй версии имитатора сети ПД



Имитатор сети ПД второй версии экономически более целесообразен по сравнению с имитатором первой версии за счет создания объединенной (единой) сети, включающей в себя несколько групп изолированных частных сетей (ЧС) имитатора сети специального назначения. Каждая такая группа ЧС относится к категории сетей специального назначения определенного государственного ведомства из указанных в ФЗ «О связи».

Первые две версии имитатора являются учебными и созданы студентами с неполной аппаратно-программной реализацией алгоритма в плане, как аппаратуры, так и программного обеспечения.

В [7] показано, что причиной отказов работоспособности системы общеканальной сигнализации ОКС№7 сети связи общего пользования ISDN (после более 20 лет ее создания и пуска в эксплуатацию [8]) является сложность принятого автоматизированного децентрализованного алгоритма маршрутизации. Это вызвано простоями функционирования сегментов сети во время коррекции таблиц маршрутизации при неисправности устройств сети. Разработаны менее сложные алгоритмы формирования маршрутов и их коррекцию в сетях ПД специального назначения за счет использования ЦЭС для централизованной принудительной маршрутизации («от источника»). В [9,10] приведены алгоритмы такой маршрутизации в отсутствии неисправных устройств имитатора сети при установлении КВК. В [11] так же приводятся примеры процедур установления КВК централизованной принудительной маршрутизацией при неисправности устройств имитатора сети. Все эти процедуры относятся к управлению сетью, которые включают также приведенные в [11] контроль за состоянием устройств имитатора сети ПД, ввод в рабочее состояние восстановленного канала имитатора сети ПД, локализацию неисправного устройства.

Кратко изложим результаты некоторых работ по учебному имитатору сети ПД второй версии с частичной реализацией аппаратно-программной реализацией:

В работах приводятся разработанные алгоритмы второй версии имитатора:

- алгоритм взаимной аутентификации между устройствами каждого абонентского доступа (оконечный пункт – ЦКП) и между смежными ЦКП. Алгоритм построен на использовании двух механизмов – РКІ и механизма аутентификации на основе идентификатора устройств изложен в работе [12]. В основу алгоритма положена работа иностранных специалистов [13] для сетей ПД усовершенствованной инфраструктуры счета AMI (Advanced Metering Infrastructure) модернизированной энергосистемы Smart Grid;
- алгоритм защищенного установления соединения на абонентском доступе имитатора объединенной сети ПД специального назначения [9];
- в транспортной части имитатора объединенной сети алгоритмы установления коммутируемых виртуальных каналов, разъединение соединения. Указанные алгоритмы приводятся на примере двух КВК разных частных сетей. Алгоритмы предусматривают обеспечение надежности и информационной безопасности [10].
- алгоритмы передача пакета данных/подтверждение в имитаторе объединенной сети специального назначения на примере передачи по двух КВК разных частных сетей. Алгоритмы предусматривают обеспечение надежности и информационной безопасности [14];
- алгоритм защищенного установления соединения установления в объединенном имитаторе объединенной сети ПД специального назначения между оконечными пунктами разных частных сетей [15];
- алгоритм формирования очередей таблиц маршрутизации нескольких КВК на примере двухчастных сетей объединенной сети ПД категории специального назначения. Приводится пример коррекции очереди свободных блоков, очереди свободных номеров и очереди таблицы маршрутизации при разъединении одного из КВК [1];

- алгоритм управления учебным имитатором сетей передачи данных специального назначения [13]. Показано, что выбор централизованного управления маршрутизацией «от источника» (принудительная маршрутизация) объясняется менее сложным алгоритмом по сравнению с используемой в сети X.25 децентрализованной маршрутизацией.

Структурная схема и функции имитатора сети ПД третьей версии

Первые две версии учебного имитатора сети ПД специального назначения не позволяют имитировать работу объединенной сети ПД специального назначения в рамках страны с оконечными пунктами частных сетей, расположенными в территориально удаленных федеральных субъектах. Для решения этой проблемы в третьей версии имитатора положен принцип иерархической двухуровневой структуры, принятый в междугородной сети связи общего пользования сети ТФОП/ISDN в РФ [17-19] и в других странах (например, в Германии на мультимедийной сети Дойче Телеком, предоставляющую возможность всем пользователям получить услугу шифрования при передаче речи или данных). На рис. 5. приведен пример иерархической структуры объединенной сети ПД специального назначения страны, использующий принцип междугородной сети ССОП. ТФОП/ISDN.

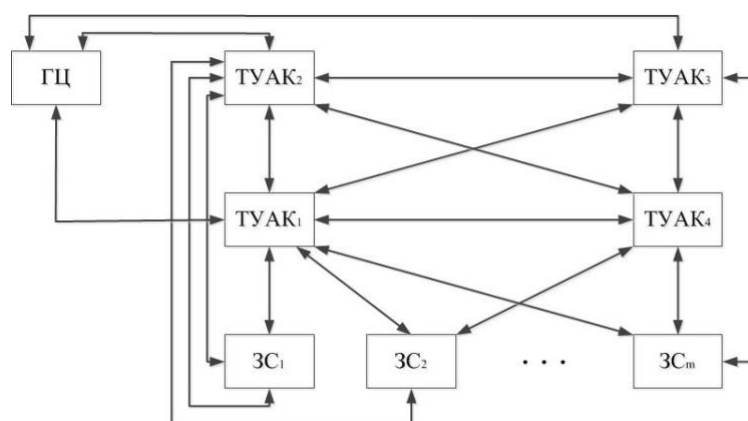


Рис. 5. Пример иерархической структуры сети ПД специального назначения страны

Нижний уровень включает территориально расположенные в разных местах страны зонные сети (ЗС). Каждая такая ЗС включает оконечные пункты (ОП) нескольких или одной частной сети, узлы коммутации УК (ЦКП) и центр эксплуатации ЦЭС. Территориальное расположение каждой ЗС, состав устройств (оконечных пунктов и ЦКП) и топология ЗС определяется в процессе проектирования сети ПД. При разработке в учебном лабораторном стенде аппаратно-программного имитатора такой иерархической сети ПД определяется число ЗС, состав моделируемых устройств в них, схемы конфигурации. Имитатор второй версии учебного имитатора объединенной сети ПД (рис.5), на котором проводятся работы, можно рассматривать в качестве примера одной из зонных сетей. Каждая ЗС соединена с узлами коммутации верхнего уровня, которые являются транзитными и служат для взаимодействия оконечных пунктов разных ЗС. Коммутация осуществляется по принципу междугородной сети ТФОП/ISDN

с помощью нескольких транзитных узлов автоматической коммутации (ТУАК), соединенных «каждый с каждым». На рис. 5 показаны четыре ТУАК - ТУАК₁, ТУАК₂, ТУАК₃, ТУАК₄. Для выполнения высоких требований по надежности, задержке и другим показателям каждая ЗС должна быть соединена с тремя или четырьмя ТУАК (на рис. 5 показано с тремя) каналами связи в разных системах уплотнения, обеспечивающих отсутствие в них корреляции помех. Число ТУАК и каналов связи между ЗС и ТУАК определяется при разработке имитатора сети ПД.

На верхнем уровне установлены также головной центр ГЦ, включающие не показанные входящие в них головные центры эксплуатации каждой частной сети ГЧС (ГЧС₁, ГЧС₂ ... ГЧС_n) и общий центр эксплуатации ОЦЭ для всех частных сетей. Головной центр частной сети предназначен для установления КВК и обмена сообщениями через узлы коммутации ТУАК с оконечными пунктами этой ЧС, расположенными в зонах сетях. Необходимо так же обеспечить установление КВК и обмен сообщениями между оконечными пунктами, принадлежащие одной из ЧС и расположенные в одной или разных ЗС. ОЦЭ предназначен для установления КВК и обмена сообщениями с оконечными пунктами разных ЧС и расположенными в разных ЗС.

Функциональные задачи иерархической сети специального назначения

Приведем некоторые из основных функций объединенной сети ПД категории специального назначения иерархической структуры с обеспечением высоких показателей качества обслуживания (надежность, информационная безопасность и др.).

1. Установление трех типов соединений КВК (одноадресного, многоадресного или широковещательного) между головным центром эксплуатации частной сети и оконечным пунктом той же ЧС в одной из ЗС. Передача сообщений по установленным КВК, разъединение КВК.
2. Установление трех типов соединений КВК (одноадресного, многоадресного или широковещательного) между оконечными пунктами, расположенными в разных или одной ЗС и принадлежащих одной и той же ЧС. Для выполнения этой функции может потребоваться предварительное установление соединения между головным центром эксплуатации частной сети и оконечными пунктами. Передача сообщений по установленным КВК.
3. Реализация указанных пунктов 1 и 2 требует выполнение функций обеспечения необходимых показателей качества обслуживания (надежность, информационная безопасность и др.).
4. безопасность и др.).

На рис. 6 приведен пример иерархической структуры учебного имитатора сети ПД специального назначения, включающий пустые зональные сети, которые подлежат заполнению устройствами (оконечные пункты частных сетей и узлы коммутации

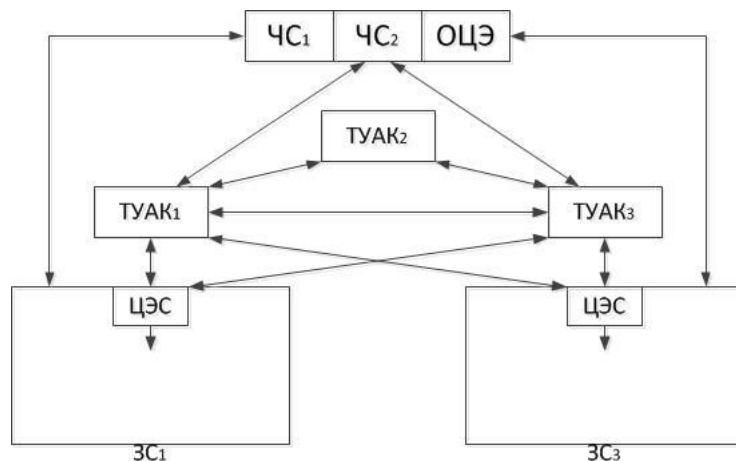


Рис.6. Пример имитатора сети третьей версии без устройств в зонах сетях

В состав имитатора входят:

- первая и третья зональные сети (ЗС₁ и ЗС₃). Имитатор второй версии может быть одной из ЗС;
- три транзитных узла автоматической коммутации (ТУАК₁, ТУАК₂, ТУАК₃), представляющие полносвязную сеть связи. Для обеспечения надежности устанавливаемых соединений ЗС₁ и ЗС₂ подключены ко всем трем ТУАК имитатора;
- головные центры частных сетей ЧС₁ и ЧС₂ (ГЧС₁, ГЧС₂). ГЧС₁ и ГЧС₃ подключены непосредственно к отдельным входам транзитного узла автоматической коммутации ТУАК₂;
- общий центр эксплуатации ОЦ предназначен для управления сетью (в развитие управления сетью в зональных сетях [11]), а также для установления КВК и обмена сообщениями с оконечными пунктами разных ЧС и расположенными в разных ЗС.

Каждый из ГЧС₁, ГЧС₂ и ОЦ подключены отдельными входами к ТУАК₂, что обеспечивает высокую надежность на участках верхнего уровня иерархической структуры имитатора сети.

Основные научно-практические направления по созданию имитатора третьей версии

Учитывая сложность изложенных выше функциональных задач иерархической сети ПД специального назначения, изложим ограниченные процедуры для решения в третьем варианте учебного имитатора.

1. Определить конфигурацию имитатора сети, включающую устройства (оконечные пункты частных сетей и узлы коммутации транспортной части) зональных сетей, транзитные узлы автоматической коммутации ТУАКи, головные центры частных сетей ГЧСы, общий центр эксплуатации ОЦ;
2. Одновременно с разработкой аппаратно-программного имитатора сети реализовать чисто программный имитатор на базе одного компьютера со всеми входящими в него устройствами;
3. Разработать на основе зарубежных работ или стандартов для других сетей не отечественной разработки алгоритм взаимной аутентификации между

взаимодействующими ТУАКаи и взаимодействующими ТУАК-ЗС (точнее ЦЭС ЗС);

4. Разработать алгоритм формирования канальных ключей для шифрования/дешифрации сообщений разных частных сетей на приведенных в предыдущем п.3 общих участках;
5. Разработать алгоритм установления защищенного КВК между головным центром частной сети (ГЧС) - несколько ТУАК - ЦЭС зонной сети - транспортная сеть этой ЗС - конечный пункт (ОП) этой частной сети (ЧС);
6. Разработать алгоритм защищенной передачи пакета данных по установленному КВК (в предыдущем пункте 5);
7. Разработать алгоритм установления защищенного КВК между ОП одной из ЗС – транспортная сеть этой ЗС - ЦЭС этой ЗС - несколько ТУАК - ЦЭС другой ЗС - транспортная сеть этой ЗС – ОП. Оба ОП установленного КВК принадлежат одному и тому же ЧС;
8. Разработать алгоритм защищенной передачи пакета данных по установленному КВК (в предыдущем пункте 7);
9. Разработать алгоритм установления защищенного КВК между конечными пунктами, принадлежащими разным ЧС и находящимися в разных ЗС.

Выводы

Сложность построения учебного имитатора единой отечественной сети передачи данных, объединяющей независимые частные сети категории специального назначения, некоторых государственных ведомств требует разработку алгоритмов в несколько этапов. На каждом из них создается следующая усовершенствованная версия учебного имитатора. Для приведенных первых двух версий имитаторов приводятся аппаратно-программные конфигурации и списки разработанных алгоритмов с указанием их описания в статьях ведущих российских научных журналах по телекоммуникациям. Приведена в качестве примера конфигурация иерархической структуры третьей версии, которая позволяет имитировать работу объединенной сети в рамках страны. Изложены основные научно-практические направления по созданию учебного имитатора третьей версии.

Проведения студентами научно-исследовательских практических работ по созданию имитатора сети ПД категории специального назначения дает им получение знаний и опыта для того, чтобы, придя после окончания вуза использовать на производстве по построению действующей сети на отечественном оборудовании.

Список литературы

1. Федеральный закон Российской Федерации «О связи» № 126-ФЗ от 07.07.2003 (редакция от 05.01.2018 г.).
2. Резолюция конференции «Информационные технологии на службе оборонно-промышленного комплекса России 2015» // Connect. – 2015. – № 9. – С. 78-88
3. Стратегия развития отрасли информационных технологий на 2014-2020 и на перспективу до 2025 года”. Утверждена распоряжением Правительства РФ 1.11.2013 г. № 2036-р.
4. Матвеев В.А., Басараб М.А., Бельфер Р.А., Кравцов А.В., Мерзляков Д.И. Алгоритм функционирования УЛС защищенной сети ПД на базевиртуальных

- каналов с высокими требованиями к качеству обслуживания. // "Электросвязь", 2017. № 8. С. 57–62.
5. М.А. Басараб, Р.А. Бельфер, Е.В. Глинская, А.В. Кравцов. Алгоритм ПО установления коммутируемого виртуального канала на абонентском доступе имитатора сети ПД с учетом обеспечения информационной безопасности // ПЕРВАЯ МИЛЯ. 2017. №8. С.64-69.
 6. Р.А. Бельфер, Е.В. Глинская, А.В. Кравцов. Алгоритм программного обеспечения аутентификации абонентского доступа имитатора сети ПД учебного лабораторного стенда. // ПЕРВАЯ МИЛЯ. 2018. №1. С.64-68.
 7. Басараб М.А., Р.А. Бельфер Р.А., Глинская Е.В., Кравцов А.В. Сравнение процедур коррекции маршрутизации в имитаторе сети ПД специального назначения и в ОКС7. // REDS: ТЕЛЕКОММУНИКАЦИОННЫЕ УСТРОЙСТВА И СИСТЕМЫ. № 4. 2020. С. 43-47.
 8. Rufa G. Developments in Telecommunications. With a Focus on SS7 Network Reliability //Springer, 2009. – 277 p
 9. Басараб, М.А., Р.А. Бельфер, А.В. Кравцов, Т.П. Алгоритм защищенного установления соединения на абонентском доступе имитатора объединенной сети ПД специального назначения. // Первая миля. – 2019. – № 8. – С. 46-51.
 10. Басараб М.А., Р.А. Бельфер Р.А., Глинская Е.В., Кравцов А.В. Алгоритм безопасного установления/разъединения соединения на транспортном участке объединенной сети ПД спецназначения // Первая миля. – 2020. – № 2. – С. 22-25.
 11. Басараб М.А., Бельфер Р.А., Кравцов А.В. Управление учебным имитатором зонных сетей передачи данных специального назначения. // Электросвязь. № 1. 2021. С. 51-56.
 12. Басараб, М.А., Р.А. Бельфер, А.В. Кравцов, Т.П. Никулина Алгоритм аутентификации и формирования разовых ключей в имитаторе лабораторного стенда объединенной сети ПД специального назначения // Первая миля. – 2019. – № 2. – С. 62-68
 13. Sangji Lee; Jinsuk Bong; Sunhee Shin; Yongtae Shin. A security mechanism of Smart Grid AMI network through smart devicemutual authentication. The International Conference on Information Networking 2014 (ICOIN2014).- 2014. - pp 592 – 595.
 14. Басараб, М.А., Р.А. Бельфер, А.В. Кравцов, В.Г. Орлов. Алгоритмы передачи данных в имитаторе объединенной сети специального назначения. // Телекоммуникации и информационные технологии, – 2019. – № 2. – С. 76-81.
 15. Басараб М.А., Бельфер Р.А., Кравцов А.В. Маршрутизация в объединенном имитаторе сети ПД специального назначения между оконечными пунктами разных частных сетей // Электросвязь. № 3. 2019. С. 51-53
 16. Басараб М.А., Бельфер Р.А., Кравцов А.В. Архитектура очередей таблиц маршрутизации объединенной сети ПД категории специального назначения // Электросвязь. № 2. 2019. С. 33-37.
 17. Гольдштейн Б.С, Соколов Н.А., Яновский Г.Г. Сети связи. «БХВ» Петербург. 2011. 400с.
 18. Басараб М.А., Бельфер Р.А., Кравцов А.В. Учебные имитаторы объединенной сети ПД спецназначения и задачи имитатора иерархической структуры // Электросвязь. – 2020. – № 3. – С. 62-68.
 19. Васинев Д.А. Применение операционных систем с открытым исходным кодом в коммуникационном оборудовании для сетей с коммутацией пакетов // Вопросы кибербезопасности. 2016. № 4 (17). С. 36-44.

Development of a training simulator of a united data transmission network of a special purpose category

Belfer R.A.²⁹, Kravcov A.V.³⁰

Abstract. *The complexity of the algorithms for constructing an educational simulator of a unified domestic data transmission network that unites independent private networks of a special-purpose category is caused by the phased creation of simulators. For the first two versions of simulators, hardware and software configurations and lists of developed algorithms are provided with an indication of their description in articles of leading Russian scientific journals. As an example, the configuration of the hierarchical structure of the third version is given, which allows simulating the operation of the interconnected network throughout the country. The main scientific and practical directions for creating an educational simulator of the third version are stated.*

Keywords: *united network simulator, hierarchical structure, private network, information security, data transmission network.*

²⁹ Belfer Ruvim, Ph.D., Bauman Moscow State Technical University, Moscow, a.belfer@yandex.ru

³⁰ Kravcov Alexander, the head of department, Research Institute (Moscow) Central Research Institute of VKS, skyak78@gmail.com

Методика оценки угроз безопасности информации

Бондарев В.В.³¹

Аннотация. Проведен анализ нового методического документа ФСТЭК России, посвященного оценке угроз безопасности информации. Особое внимание уделено практике реализации требований этого документа для специалистов в области ИБ, которые занимаются анализом потенциальных угроз для важных объектов информационной инфраструктуры.

Ключевые слова: информационная безопасность; защита информации; угроза безопасности информации; модель угроз; информационная система; автоматизированная система управления; информационно-телекоммуникационные сети.

Введение. Как известно, новый методический документ, определяющий методику оценки угроз безопасности информации, был подписан ФСТЭК России 5 февраля 2021 г.³²

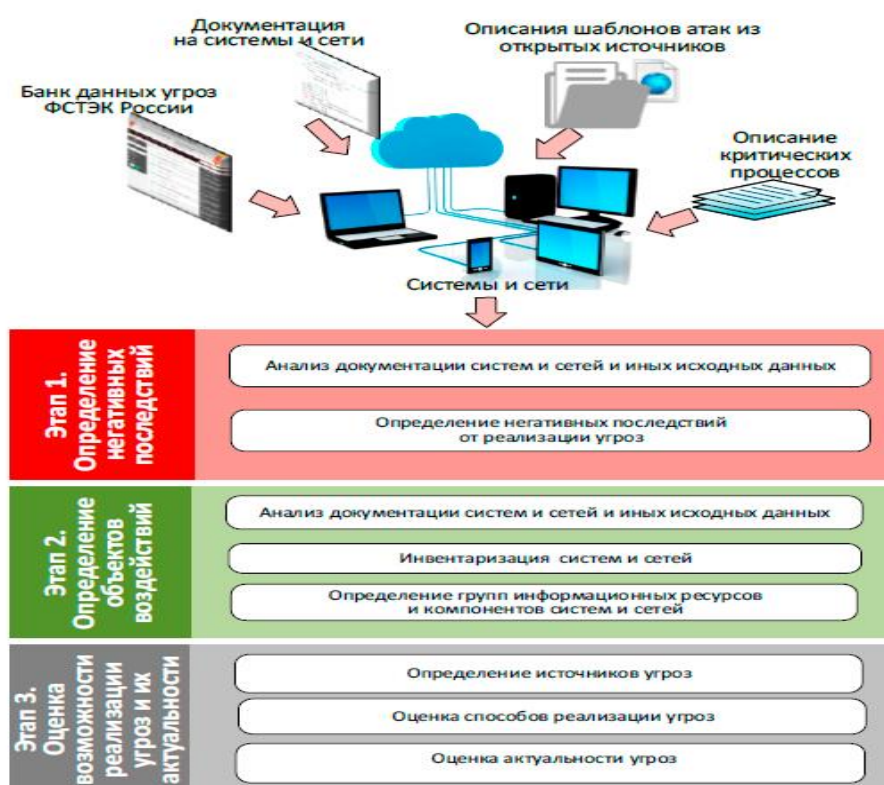


Рисунок 2. Общая схема проведения оценки угроз безопасности информации

Методика работает со следующими типами объектов:

³¹ Бондарев Валерий Васильевич, к.в.н., доцент, МГТУ имени Н.Э. Баумана, Москва, bondarevvv@mail.ru

³² Методический документ Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

- информационные системы (ИС);
- автоматизированные системы управления;
- информационно-телекоммуникационные сети;
- информационно-телекоммуникационные инфраструктуры центров обработки данных;
- облачные инфраструктуры.

Также методика применима для следующих областей:

- информационные системы персональных данных;
- информационные системы управления производством, используемые организациями оборонно-промышленного комплекса;
- муниципальные и государственные ИС;
- значимые объекты критической информационной инфраструктуры РФ;
- критически важные, потенциально опасные объекты с автоматизированными системами управления производственными и технологическими процессами.

Новая методика ориентирована на оценку угроз безопасности, которые обусловлены действиями нарушителей, и поэтому не включает в себя ряд факторов, не зависящих от человека:

- угрозы безопасности, связанных с природными явлениями и стихийными бедствиями;
- угрозы безопасности криптографических средств защиты;
- угрозы безопасности, связанных с техническими каналами утечки данных.

Можно, конечно, много говорить о достоинствах нового документа. Но даже его поверхностный анализ приводит к неутешительным выводам.

В методике, которая изначально должна быть риск-ориентированной, отсутствует понятие вероятности реализации негативного события [10]. То есть ущерб (негативные последствия) мы оцениваем, а их вероятность – нет. Есть деление на угрозы возможные и актуальные. Но ведь наличие хотя бы одного сценария делает угрозу актуальной [1-5]. Тогда разницы между возможными и актуальными нет, так как сложно представить угрозу, для которой не было в современной организации хотя бы одного сценария реализации. А значит мы опять все возможные угрозы делаем актуальными, не имея возможности их сократить.

Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования систем и сетей [5-10].

ФСТЭК России обязывает реализовывать не дискретный процесс моделирования (раз в три года перед аттестацией), а непрерывный. То есть учитывать появление новых уязвимостей, влияющих на возможности реализации угроз, а также новых тактик. Поэтому необходимо разрабатывать средства автоматизации моделирования. И эти средства автоматизации должны будут

подгружать новые данные об угрозах и т.п. с сайта регулятора. Кстати, поддержание модели угроз в актуальном состоянии в свою очередь ставит вопрос о непрерывной перееаттестации.

Классификация источников угроз противоречит ранее выпущенным ГОСТам ФСТЭК и в методике вообще нет отсылок ранее принятых ТК362 ГОСТов. Эти ГОСТы классифицируют и систематизируют многие вопросы, рассматриваемые в методике, - нарушителей, источники угроз, мотивы, потенциал и т.п. По сути, сейчас любой нарушитель является актуальным. А ведь существует ГОСТ 18045 с потенциалом нападения. Невозможно ответить на вопрос, как влияет определяемый уровень возможностей нарушителя, его категория, виды, риски и т.п. на определение актуальных угроз? Все равно все скатывается к определению возможных сценариев угроз, которые непонятно как связать с нарушителями и их возможностями.

Ну и наконец, главное. Как выбрать меры по нейтрализации угроз/обработке рисков? Известно, что одни угрозы/риски мы будем уменьшать, другие принимать, третьи передоверять или отказываться от вида деятельности, которая порождает конкретную угрозу/риск. Но ведь у нас все угрозы/нарушители актуальны (смотри выше).

Выводы

1. Разработать модель угроз по новой методике очень сложно, если вообще возможно. В реальной жизни положения данной методике для большинства организаций неприменимы [1-5].

2. Необходимо доработать/обновить банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) сведениями о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

3. Необходима разработка средств автоматизации моделирования.

4. Было бы крайне полезно, чтобы регулятор разработал акции по использованию разработанного продукта. В эти рекомендации, в первую очередь, необходимо включить готовые частные модели угроз. Был бы отличный пример работы документа и многие вопросы снялись бы автоматически.

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. Бондарев В.В. Возможный подход к оценке средств защиты информации // В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019. С. 38-41.

3. Бондарев В.В. Возможный подход к оценке средств защиты информации // В сборнике: Безопасные информационные технологии (БИТ-2016). Сборник трудов Седьмой Всероссийской научно-технической конференции. Под редакцией В.А. Матвеева. 2016. С. 77-79.

4. Бондарев В.В. Учебно-материальная база подготовки специалиста в области информационной безопасности // В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019. С. 42-

45.

5. Бондарев В.В. Функционально-системный подход в подготовке специалиста в области информационной безопасности // В сборнике: Безопасные информационные технологии. Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 63-67.

6. Климов С.М., Поликарпов С.В., Рыжов Б.С., Тихонов Р.И., Шпырня И.В. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий // Вопросы кибербезопасности. 2019. № 6 (34). С. 37-48.

7. Массель А.Г. Методика анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов // В сборнике: Информационные и математические технологии в науке и управлении. Ответственный редактор Л.В. Массель. 2015. С. 186-195.

8. Нащекин П.А. Теоретическое обоснование методики проектирования систем защиты информации в виртуальных средах и облачных платформах // Вопросы кибербезопасности. 2020. № 6 (40). С. 14-22.

9. Соловьев С.В., Язов Ю.К. Информационное обеспечение деятельности по технической защите информации // Вопросы кибербезопасности. 2021. № 1 (41). С. 69-79.

10. Probabilistic Modeling in System Engineering. / By ed. A.Kostogryzov, - London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.

Method information security threat assessments

Bondarev V.V.³³

Abstract. *The analysis of the new methodological document of the FSTEC of Russia, dedicated to the assessment of threats to information security, is carried out. Particular attention is paid to the practice of implementing the requirements of this document for specialists in the field of information security, who are engaged in the analysis of potential threats to important objects of information infrastructure.*

Keywords: *information security; protection of information; threat to information security; threat model; Information system; automated control system; information and telecommunication networks.*

³³ Bondarev Valery, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, bondarevvv@mail.ru

Подход к повышению оперативности обработки исполняемых файлов специалистами по компьютерной криминалистике

Бураков А.Г.³⁴, Полосухин Н.В.³⁵

***Аннотация.** Исследование посвящено разработке подхода к обработке подозрительных исполняемых файлов в рамках работы специалиста по компьютерной криминалистике с целью повышения оперативности их обработки за счет автоматизации отдельных задач анализа. Авторами разработан способ детектирования вредоносного программного обеспечения на основе эвристического анализа в среде эмуляции. В результате проведенных исследований достигнуто существенное снижение времени работы аналитика при расследовании инцидентов, обусловленных вредоносным программным обеспечением. Представлено сравнение эффективности обнаружения вредоносного кода существующими средствами анализа файлов и разрабатываемого программного модуля.*

***Ключевые слова:** эвристический анализ, среда виртуализации, машинное обучение, анализ дампов памяти, монитор обращений.*

Введение

В настоящее время растет количество новых образцов вредоносного программного обеспечения, равно как и количество инцидентов информационной безопасности. В процессе проведения оперативных мероприятий по реагированию на инциденты сотрудниками изымается большое количество жестких дисков, машинных носителей информации, снимаются дампы оперативной памяти.

Специалистам по компьютерной криминалистике необходимо исследовать различные артефакты, извлеченные из доказательной базы. Однако среди таких артефактов могут быть вредоносные файлы, что ставит перед специалистом задачу определения вредоносной активности в обнаруженных подозрительных артефактах.

Постановка задачи

Целью данного исследования является разработка программного модуля, способного автоматизировано анализировать подозрительные артефакты инцидента информационной безопасности с извлечением конкретных индикаторов компрометации и работать в изолированных локально-вычислительных сетях, а также повышающего оперативность работы специалиста по информационной безопасности.

Описание модуля статического анализа

Вначале работы модуль определяет тип загруженного объекта. Тип объекта определяется мажоритарным принципом [1] с использованием утилит *FILE*, *BINWALK*, *TRID*, *STRINGS*. Определение типа объекта необходимо для формирования решения о применении методов эвристического анализа и компьютерного зрения.

После определения типа, объект поступает на сопоставление с *YARA*

³⁴ Бураков Александр Геннадьевич, Академия ФСО России, г. Орёл, burakov2298@mail.ru

³⁵ Полосухин Никита Владимирович, Академия ФСО России, г. Орёл, lolnoobnick@gmail.com

правилами [2]. При обнаружении совпадения с правилами, относящимися к вредоносному программному обеспечению, анализ прекращается с выводом в файл отчета описания YARA правила.

Далее объект поступает на модуль статического анализа методом компьютерного зрения. Для корректной работы модуля были определены эмпирические границы размера анализируемых объектов: не менее 5 кБ и не более 1,5 МБ. Модуль преобразует объект в RGB изображение [3], которое поступает на вход глубокой сверточной нейронной сети для анализа. Нейронная сеть позволяет разделять только исполняемые объекты (типа *EXE*, *DLL*) на два класса: вредоносные и легитимные. Качество классификации составляет 98,16%.

Если анализируемый объект был определен как исполняемый, то после анализа нейронной сетью объект поступает на выделение индикаторов компрометации методом статического анализа с помощью утилиты PESTudio. Утилита позволяет выделить специфические индикаторы [4] анализируемого объекта, при этом принимается решение о наличии аномалий на основе встроенных правил.

Описание модуля поведенческого анализа

Запуск поведенческого анализа зависит от результатов статического анализа. Если в результате статического анализа не было выявлено ни одного подозрительного индикатора или вредоносный объект был однозначно идентифицирован (например, с помощью YARA правил), то запуск модуля поведенческого анализа является опциональным и производится по решению специалиста. Если были обнаружены подозрительные индикаторы, но объект не был однозначно идентифицирован, то запуск модуля поведенческого анализа происходит автоматически. Поведенческий анализ [5] проходит в среде виртуализации и содержит в себе два этапа.

На первом этапе анализ производится с помощью утилиты Windows Process Monitor (ProcMon). Process Monitor – это расширенный инструмент мониторинга для Windows, который в реальном времени отображает активность файловой системы, реестра и процессов / потоков. Главное преимущество данного средства – анализ живой системы и представление оперативного отчета. Для работы с данной утилитой необходимо предварительно указать файл конфигурации, который подготавливается аналитиком для фиксации только необходимых событий, таких как: создание новых процессов, активность файловой системы, доступ к реестру и создание сетевых соединений [6]. Вывод подвергается эвристическому анализу по соответствующим индикаторам Журнал вывода ProcMon подвергается фильтрации и создается промежуточный отчет с необходимыми полями о функционировании ВПО.

На втором этапе происходит анализ дампа оперативной памяти виртуальной машины, снятого после исполнения подозрительного объекта. Для выделения эвристик используется фреймворк volatility и сравнительный анализ "чистого" и "зараженного" дампа [7]. Для каждого объекта генерируется уникальный вектор эвристик, вычисляются хэш-функция таблицы импорта исполняемых файлов, а также нечеткие хэш-функции ssdeep и TLSH [8, 9]. После этого происходит сравнение вычисленных хэш-значений с имеющимися и с помощью алгоритма случайного леса [10] происходит отнесение вектора эвристик к одному из 5 классов: стилеры, загрузчики, шифровальщики, бэкдоры, другие вредоносные файлы. Помимо общего вектора эвристик генерируется подробный отчет о

различиях с "чистой" системой и о всех подозрительных действиях, зарегистрированных в дампе оперативной памяти.

Оценка эффективности

Для оценки эффективности созданный модуль был сравнен с подобными существующими решениями, а также были оценены временные затраты на его работу.

Для сравнения с существующими системами была сформирована выборка из 70 вредоносных объектов и 30 легитимных объектов. Согласно практическому исследованию качества обнаружения ВПО (табл. 1), разрабатываемый программный модуль обеспечивает качества детектирования ВПО на уровне 90%. Такое качество связано с тем, что у отдельных образцов ВПО присутствует защита от исполнения в среде эмуляции.

Таблица 1.

Сравнение различных средств анализа объектов

Средство анализа объектов	Метод обнаружения	Доступность	Стоимость	Целевая система	Ошибки 1 рода, %	Ошибки 2 рода, %	Корректное детектирование ВПО (positive), %	Недетектирование неВПО (false negative), %
Авторский модуль	compl.	local	free to use	Windows	11	3	89	97
Anubis sandbox	beh.	web	licensed	Windows	30	0	70	100
Cuckoo sandbox	compl.	web	free to use	Any	10	0	90	100
Kaspersky	compl.	local	licensed	Any	4	17	96	83
VirusTotal	compl.	web	free to use*	Any	1	3	99	97
Any.Run	compl.	web	free to use*	Windows	4	0	96	100
Joe sandbox	compl.	web	licensed	Any	1	0	99	100
VxStream	beh.	web	free to use	Windows	21	0	79	100
Malwr	compl.	web	free to use	Windows	10	0	90	100

Для оценки временной эффективности модуля было проанализировано 10 объектов вредоносного ПО специалистом ИБ и с помощью представленного программного модуля. Этапы анализа соответствовали этапам работы созданного модуля. Для каждого этапа замерялось время работы и усреднялось по количеству испытаний (рис. 1).

Верхняя граница времени работы $t_{\max}$ достигается при анализе такого файла,

что модуль статического анализа считает исследуемый файл подозрительным, а *ProcMon* не позволяет однозначно детектировать вредоносную активность, при этом $t_{\max}$ рассчитывается как:

$$t_{\max} = t_{\text{type}} + t_{\text{static}} + t_{\text{yara}} + t_{\text{ProcMon}} + t_{\text{volatility}} + t_{\text{report}} \Leftrightarrow \text{suspicious}(\text{file}) == \text{True}, \quad (1)$$

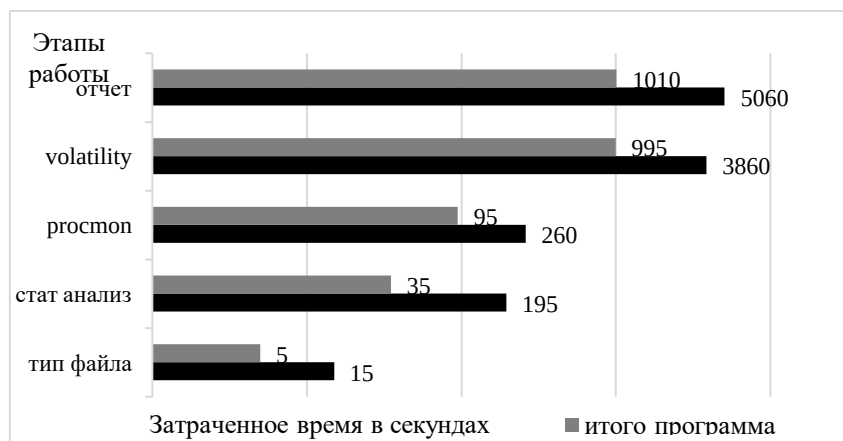


Рис. 1. Сравнение среднего времени работы аналитика

Выводы

В результате работы представлен способ значительного повышения оперативности работы специалиста по компьютерной криминалистике. Разработан способ обнаружения ВПО на основе методов машинного зрения, в комбинации с сигнатурным анализом на основе YARA правил. Полученные результаты в сравнении с существующими системами анализа файлов обусловлены фактом защиты некоторых образцов ВПО от исполнения в среде эмуляции. Таким образом, направлением дальнейших исследований является повышение качества детектирования вредоносного кода за счет перехода от виртуальной машины, используемой в качестве изолированной программной среды, на решения на основе реальных ОС.

Научный руководитель: Козачок Александр Васильевич, докт. техн. наук, Академия ФСО России, г.Орёл, a.kozackok@academ.msk.rsnet.ru.

Литература

1. Karampidis K., Kavallieratou E., Papadourakis G. Comparison of classification algorithms for file type detection a digital forensics perspective //Polibits. – 2017. – Т. 56. – С. 15-20.
2. Naik N. et al. Embedding fuzzy rules with YARA rules for performance optimisation of malware analysis //2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). – IEEE, 2020. – С. 1-7.
3. Rathore H. et al. Malware detection using machine learning and deep learning //International Conference on Big Data Analytics. – Springer, Cham, 2018. – С. 402-411.
4. Kozachok A. V., Kozachok V. I. Construction and evaluation of the new heuristic malware detection mechanism based on executable files static analysis //Journal of Computer Virology and Hacking Techniques. – 2018. – Т. 14. – №. 3. – С. 225-231.

5. Марков А.С., Матвеев В.А., Фадин А.А., Цирлов В.Л. Эвристический анализ безопасности программного кода // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2016. № 1. С. 98–111. DOI: 10.18698/0236-3933-2016-1-98-111.
6. Hampton N., Baig Z., Zeadally S. Ransomware behavioural analysis on windows platforms //Journal of information security and applications. – 2018. – Т. 40. – С. 44-51.
7. Tien C. W. et al. Memory forensics using virtual machine introspection for Malware analysis //2017 IEEE Conference on Dependable and Secure Computing. – IEEE, 2017. – С. 518-519.
8. Moia V., Henriques M. A. A comparative analysis about similarity search strategies for digital forensics investigations //Proceedings of the Thirty-Fifth Brazilian Symposium on Telecommunications and Signal Processing. – 2017. – С. 462-466.
9. Oliver J., Cheng C., Chen Y. TLSH--a locality sensitive hash //2013 Fourth Cybercrime and Trustworthy Computing Workshop. – IEEE, 2013. – С. 7-13.
10. Lin W. et al. An ensemble random forest algorithm for insurance big data analysis //Ieee access. – 2017. – Т. 5. – С. 16568-16575.

An approach of efficiency increasing of digital forensics specialist

Burakov A.G.³⁶, Polosukhin N.V.³⁷

Abstract. *The study of the approach of processing suspicious files within the work of a specialist in digital forensics in order to minimize the average time of work is being carried out. A method for detecting malicious software (malware) based on heuristic analysis in an emulation environment has been developed. The principle of operation of the software tool modules, the algorithm of their work is described. As a result of the work, a significant reduction in the processing time of the information security analyst was achieved at the stage of carrying out received files during the operational activities in the time of the incident investigation. Comparison of the detection of malicious code with existing file analysis systems and the developed software module is given.*

Keywords: *heuristic analysis, sandbox, machine learning, memory dump, access monitor.*

³⁶Burakov Aleksandr Gennadievich, Academy of the Federal Guard Service, Russia, Oryol, burakov2298@mail.ru

³⁷Polosukhin Nikita Vladimirovich, Academy of the Federal Guard Service, Russia, Oryol, lolnoobnick@gmail.com

Алгоритм поиска седловой точки в игровой задаче выбора программных средств защиты информации для серверов вычислительной сети

Быков А.Ю.³⁸, Гришунин М.В.³⁹, Федоров Е.Г.⁴⁰, Маркова И.А.⁴¹

Аннотация. Представлена игровая постановка задачи двух игроков: защитника и нападающего. Защитник осуществляет выбор программных средств защиты информации для серверов вычислительной сети с учетом важности обрабатываемой информации, а нападающий выбирает возможные типы атак. Математическая постановка задачи является дискретно-непрерывной игрой, множество решений защитника дискретно, а множество решений нападающего непрерывно. Игра является игрой с нулевой суммой, в качестве показателя качества используется ущерб защитника. Защитник при заданном решении нападающего решает задачу булевого программирования, а нападающий при заданном решении защитника задачу линейного программирования. Предложен алгоритм поиска седловой точки в смешанной стратегии для защитника, в чистой для нападающего, основанный на сведении непрерывной задачи нападающего к дискретной. Алгоритм основан на идеях метода Брауна-Робинсона, но без явного построения матрицы игры. Для снижения вычислительных ресурсов процессора, требуемых для работы алгоритма, предложено после того, как на заданном числе шагов не получено новое решение, не решать оптимизационные задачи, а искать решения методом перебора среди найденных ранее решений.

Ключевые слова: защита информации, дискретно-непрерывная игра, игра с нулевой суммой, булево программирование, линейное программирование, смешанная стратегия, чистая стратегия.

Введение

При решении различных задач в области защиты информации часто используются математические модели из теории игр. Чаще всего рассматривается игра двух игроков: защитника и атакующего, но может быть и более двух игроков. Некоторые примеры подобных задач приведены в [1-9].

Другие математические модели, используемые при защите информации, рассмотрены в [10-12].

Ниже рассматривается дискретно-непрерывная игра для выбора программных средств, устанавливаемых на серверах сети с целью защиты информации.

1. Постановка задачи

Базисные множества

1. $S = \{s_1, s_2, \dots, s_n\}$ – множество серверов в распределённой вычислительной системе, $N = \{1, 2, \dots, n\}$ – множество индексов этих серверов.

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

³⁹ Гришунин Максим Вадимович, МГТУ им. Н.Э. Баумана, Москва, grishunin-mv@ya.ru

⁴⁰ Федоров Евгений Георгиевич, МГТУ им. Н.Э. Баумана, Москва, fedorov.evg.msu@gmail.com

⁴¹ Маркова Ирина Александровна, МГТУ им. Н.Э. Баумана, Москва, gurina.irina.94@gmail.com

2. $A = \{a_1, a_2, \dots, a_m\}$ – множество типов атак (реализаций угроз безопасности) в защищаемой системе, $M = \{1, 2, \dots, m\}$ – множество индексов этих атак.
3. $\Pi = \{\pi_1, \pi_2, \dots, \pi_\lambda\}$ – множество служебных процессов, которые могут быть запущены на серверах для обеспечения безопасности, $\Lambda = \{1, 2, \dots, \lambda\}$ – множество индексов этих процессов.
4. $R^{(3)} = \{r_1^{(3)}, r_2^{(3)}, \dots, r_{l^{(3)}}^{(3)}\}$ – множество ограниченных ресурсов стороны защиты, $L^{(3)} = \{1, 2, \dots, l^{(3)}\}$ – множество индексов этих ресурсов.

Множество ресурсов R делится на два непересекающихся подмножества $R^{(3)} = R^{(ч)} \cup R^{(о)}$, $R^{(ч)}$ – множество частных ресурсов для серверов, $R^{(о)}$ – множество общих ресурсов для серверов. Для частных и общих ресурсов введем отдельную нумерацию: $L^{(ч)} = \{1, 2, \dots, l^{(ч)}\}$, $L^{(о)} = \{1, 2, \dots, l^{(о)}\}$ – множества индексов частных и общих ресурсов, соответственно.

5. $R^{(н)} = \{r_1^{(н)}, r_2^{(н)}, \dots, r_{l^{(н)}}^{(н)}\}$ – множество ограниченных ресурсов стороны нападения, $L^{(н)} = \{1, 2, \dots, l^{(н)}\}$ – множество индексов этих ресурсов.

Параметры элементов множеств и отношений между ними

1. $w_{ij} \geq 0, \forall i \in N, j \in M$ – оценка ущерба защитника на i -ом сервере при успешной для нападающего реализации j -го типа атаки.
2. $p_{jk} \in [0, 1], \forall j \in M, k \in \Lambda$ – вероятность (или возможность) предотвращения j -ой атаки (реализации угрозы) при использовании k -го процесса на любом из серверов.
3. $v_{jik}^{(ч)} \geq 0, \forall j \in L^{(ч)}, k \in \Lambda, i \in N$ – значение j -го частного ресурса требуемого для работы k -го процесса i -ом сервере.
4. $V_j^{(ч)} \geq 0, \forall j \in L^{(ч)}, i \in N$ – максимальное значение j -го частного ресурса на i -ом сервере, которое может быть использовано для служебных процессов.
5. $v_{jik}^{(о)} \geq 0, \forall j \in L^{(о)}, k \in \Lambda, i \in N$ – значение j -го общего ресурса требуемого для работы k -го процесса i -ом сервере.
6. $V_j^{(о)} \geq 0, \forall j \in L^{(о)}$ – максимальное значение j -го общего ресурса для всех серверов, которое может быть использовано для служебных процессов.
7. Некоторые вычислительные процессы (приложения) объединим в однотипные группы, из группы имеет смысл устанавливать только одно приложение, в каждой группе. $G = \{1, 2, \dots, g\}$ – индексы этих групп. Для определения таких групп введем булеву матрицу $B_{\langle \lambda \times g \rangle} \|b_{ki}\|, \forall k \in \Lambda, i \in G, b_{ki} = 1$, если k -ое приложение входит в i -ую группу, $b_{ki} = 0$ – в противном случае.
8. $v_{kij}^{(н)} \geq 0, \forall k \in L^{(н)}, j \in M, i \in N$ – значение k -го ресурса стороны нападения, необходимого для проведения j -го типа атаки i -ый сервер.

9. $V_k^{(H)} \geq 0, \forall k \in L^{(H)}$ – максимальное значение объема k-го ресурса стороны нападения, используемое для проведения всех типов атак.

Искомые переменные

Для стороны защиты введем булеву переменную $x_{ki} \in \{0, 1\}, \forall k \in \Lambda, i \in N$, $x_{ki} = 1$, если k-ый процесс запущен i-ом сервере, $x_{ki} = 0$ – в противном случае, переменные образуют вектор $\vec{X}$.

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

Показатель игроков

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

$$U(\vec{X}, \vec{Y}) = \sum_{i \in N} \sum_{j \in M} w_{ij} y_{ij} - \sum_{i \in N} \sum_{j \in M} w_{ij} \max_{k \in \Lambda} \{p_{jk} x_{ki}\} y_{ij} = \sum_{i \in N} \sum_{j \in M} w_{ij} y_{ij} (1 - \max_{k \in \Lambda} \{p_{jk} x_{ki}\}). \quad (1)$$

Ограничения

Ограничения на использование частных ресурсов на каждом сервере:

$$\sum_{k \in \Lambda} v_{jik}^{(ч)} x_{ki} \leq V_{ji}^{(ч)}, \forall j \in L^{(ч)}, i \in N. \quad (2)$$

Ограничения на использование общих ресурсов для всех серверов:

$$\sum_{i \in N} \sum_{k \in \Lambda} v_{jik}^{(o)} x_{ki} \leq V_j^{(o)}, \forall j \in L^{(o)}. \quad (3)$$

Ограничения на то, что на любом сервере нельзя устанавливать более одного приложения из каждой группы:

$$\sum_{k \in \Lambda} b_{kj} x_{ki} \leq 1, \forall i \in N, j \in G. \quad (4)$$

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

$$\sum_{i \in N} \sum_{j \in M} v_{kij}^{(H)} y_{ij} \leq V_k^{(H)}, \forall k \in L^{(H)}. \quad (5)$$

2. Алгоритм поиска седловой точки

По аналогии с [8], так как нападающий решает задачу ЛП, и решение этой задачи находится в вершине многогранника допустимых решений, число этих вершин конечное, то непрерывную задачу можно свести к дискретной, если рассматривать в качестве решений вершины многогранника. В этом случае поставленную задачу можно свести к матричной игре, в которой седловая точка в смешанных стратегиях существует всегда. Идея метода Брауна-Робинсона для поиска решения в смешанных стратегиях основана на последовательном решении задач каждым из игроков при этом используется суммарный накопленный выигрыш или проигрыш. При многократном решении таких задач оценивается вероятность появления каждого из решений, эти оценки вероятностей и задают смешанную стратегию. По аналогии с [8] для нападающего, множество решений

которого непрерывно, необходимо вычислять среднее $\bar{Y}$ среди множества получаемых решений. Для защитника получаем оценки вероятностей для получения каждого из решений.

Пусть $\vec{Y}^{(1)}, \vec{Y}^{(2)}, \dots, \vec{Y}^{(g)}$ – последовательность решений, получаемых нападающим при оптимизации показателя (1), тогда защитник должен решать задачу минимизации на $(g + 1)$ -ом шаге показателя:

$$U_3^{(g+1)}(\vec{X}) = \sum_{e=1}^g U(\vec{X}, \vec{Y}^{(e)}) = \sum_{e=1}^g \sum_{i \in N} \sum_{j \in M} w_{ij} y_{ij}^{(e)} \left(1 - \max_{k \in A} \{p_{jk} x_{ki}\}\right), \quad (6)$$

где $y_{ij}^{(e)}$ компоненты вектора $\vec{Y}^{(e)}$.

Пусть $\vec{X}^{(1)}, \vec{X}^{(2)}, \dots, \vec{X}^{(g)}$ – последовательность решений, получаемых защитником при оптимизации показателя (1), тогда нападающий должен решать задачу максимизации на $(g + 1)$ -ом шаге показателя:

$$U_n^{(g+1)}(\vec{Y}) = \sum_{e=1}^g U(\vec{X}^{(e)}, \vec{Y}) = \sum_{e=1}^g \sum_{i \in N} \sum_{j \in M} w_{ij} y_{ij} \left(1 - \max_{k \in A} \{p_{jk} x_{ki}^{(e)}\}\right), \quad (7)$$

где $x_{ki}^{(e)}$ компоненты вектора $\vec{X}^{(e)}$.

Задача с показателем (6) является задачей булевого программирования для защитника. Так как показатель (6) линейный по компонентам вектора $\vec{Y}^{(e)}$, то при оптимизации вместо первой суммы по векторам $\vec{Y}^{(0)}, \vec{Y}^{(1)}, \dots, \vec{Y}^{(g)}$ можно использовать среднюю точку среди этих векторов. Задача с показателем (7) является задачей линейного программирования для нападающего.

Средняя точка для нападающего имеет вид:

$$\vec{Y}^{(cp)} = \frac{1}{g} \sum_{e=1}^g \vec{Y}^{(e)}. \quad (8)$$

Сформулируем алгоритм поиска седловой точки.

Шаг 0. Полагаем, что вектор $\vec{Y}^{(сум)} = \|0, 0, \dots, 0\|^T$ (суммарный вектор для вычисления суммы $\sum_{e=1}^g \vec{Y}^{(e)}$), $\vec{X}^{(0)} = \|0, 0, \dots, 0\|^T$ – начальное решение защитника, может быть выбрано любое решение, словарь (map) векторов $\vec{X}$ пуст. Ключом этого словаря является вектор $\vec{X}^{(k)}$, а значением число появлений векторов $\vec{X}$ на различных шагах алгоритма.

Шаг k ($k=1, 2, 3, \dots$). Находим $\vec{Y}^{(k)}$ при полученном на текущем шаге словаре (map) векторов $\vec{X}$, решая ЗЛП для нападающего, максимизирую показатель (7) (при $k=1$ максимизируем показатель (1) при $\vec{X} = \vec{X}^{(0)}$). Значение показателя качества нападающего при этом обозначим $U_n^{(k)}(\vec{Y}^{(k)})$, полагаем $\vec{Y}^{(сум)} = \vec{Y}^{(сум)} + \vec{Y}^{(k)}$, $\vec{Y}^{(cp)} = \frac{\vec{Y}^{(сум)}}{k}$.

Находим $\vec{X}^{(k)}$ при заданном $\vec{Y}^{(cp)}$, решая задачу булевого программирования для защитника с показателем (6). Значение показателя качества при этом обозначим $U_3^{(k+1)}(\vec{X}^{(k)})$, найденное $\vec{X}^{(k)}$ включаем в словарь (map) решений защитника.

Начиная со 2-го шага проверяем критерий остановки. Если он выполняется, то завершаем работу алгоритма, полученное решение нападающего – $\vec{Y}^{(cp)}$, по словарю (map) полученных векторов $\vec{X}$ вычисляем оценки вероятностей для каждого вектора $\vec{X}$ в словаре, это будет решение защитника в смешанных стратегиях. Пара решений защитника и нападающего определяет приближенную седловую точку. Если критерий остановки не выполняется, то переходим к

следующему шагу.

В качестве критерия остановки можно использовать условие $\left| \frac{U_n^{(k)}(\vec{y}^{(k)})}{k-1} - \frac{U_3^{(k+1)}(\vec{x}^{(k)})}{k} \right| < \varepsilon$, где ε - некоторое относительно малое положительное значение, определяющее погрешность алгоритма.

Описанный алгоритм при определенной размерности задачи требует значительных вычислительных ресурсов, так как на каждом шаге приходится защитнику решать задачу булевого программирования с экспоненциальной вычислительной сложностью.

Как показали вычислительные эксперименты, получаемые решения на определенном шаге начинают повторяться, т.е. на заданном относительно большом числе шагов не получены новые решения, как для защитника, так и для нападающего (решения нападающего также можно сохранять в словаре), в этом случае можно прекратить решение оптимизационных задач, а искать решения методом перебора среди уже найденных ранее решений, подобный подход был использован в [9].

Выводы

Проведены вычислительные эксперименты, которые продемонстрировали работоспособность алгоритма, предложен способ снижения вычислительной трудоемкости алгоритма за счет перехода от решения оптимизационных задач к поиску решений среди ранее найденных после того, как решения на заданном числе шагов будут повторяться.

Использование предложенного алгоритма позволяет при использовании программных средств защиты в случае ограничений на различные ресурсы существенно снижать ущерб стороны защиты от различных типов атак.

Достоверность полученных результатов подтверждается корректностью математической постановки задачи, явной содержательной интерпретацией, как постановки задачи, так и получаемых решений, а также проверкой получаемых решений на выполнение требуемых критериев.

Литература

1. Fanyu Kong, Yufeng Zhou, Bin Xia, Li Pan, Limin Zhu. A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment. IEEE Access. 2019. Vol. 7. P. 161822-161830. DOI: 10.1109/ACCESS.2019.2950731
2. Hengwei Zhang, Lv Jiang, Shirui Huang, Jindong Wang, Yuchen Zhang. Attack-Defense Differential Game Model for Network Defense Strategy Selection. IEEE Access. 2018. Vol. 7. P. 50618-50629. DOI: 10.1109/ACCESS.2018.2880214
3. Liang Xiao, Dongjin Xu, Narayan B. Mandayam, H. Vincent Poor. Attacker-Centric View of a Detection Game against Advanced Persistent Threats. IEEE Transactions on Mobile Computing. 2018. Vol. 17. Iss. 11. P. 2512-2523. DOI: 10.1109/TMC.2018.2814052
4. Shana Moothedath, Dinuka Sahabandu, Joey Allen, Andrew Clark, Linda Bushnell, Wenke Lee, Radha Poovendran. A Game-Theoretic Approach for Dynamic Information Flow Tracking to Detect Multistage Advanced Persistent Threats. IEEE Transactions on Automatic Control. 2020. Vol. 65. Iss. 12. P. 5248-5263. DOI: 10.1109/TAC.2020.2976040
5. Dayong Ye, Tianqing Zhu, Sheng Shen, Wanlei Zhou. A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries. IEEE Transactions on Information Forensics and Security. 2020. Vol. 16. P. 569-584. DOI: 10.1109/TIFS.2020.3016842

6. Rui Zhang, Quanyan Zhu. FlipIn : A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things. IEEE Transactions on Information Forensics and Security. 2019. Vol. 15. P. 2026-2041. DOI: 10.1109/TIFS.2019.2955891
7. Boyu Gao;Libao Shi. Modeling an Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a Cyber-Physical Power System. IEEE Access. 2020. Vol. 8. P. 30322-30331. DOI: 10.1109/ACCESS.2020.2973030
8. Быков А.Ю., Крыгин И.А., Гришунин М.В., Маркова И.А. Об одном алгоритме поиска седловой точки для непрерывных линейных игр применительно к задачам защиты информации [One saddle point search algorithm for continuous games applied to information security problems] // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2020, № 4 (133), С. 58-74. DOI: 10.18698/0236-3933-2020-4-58-74
9. Быков А.Ю., Гришунин М.В., Крыгин И.А. Игровая задача выбора защищаемых объектов и исследование алгоритма поиска седловой точки на основе модификации метода Брауна-Робинсона // Вопросы кибербезопасности. 2019. № 2 (30). С. 2-12. DOI: 10.21681/2311-3456-2019-2-2-12
10. Ключарев П.Г. Графы Пайзера в задачах криптографии и обработки информации. Сборник трудов Десятой международной научно-технической конференции «Безопасные информационные технологии» (БИТ-2019) / Под. ред. А.А.Александрова. – М.: МГТУ им. Н.Э.Баумана, 2019. С. 176-179.
11. Пономаренко Г.С., Ключарёв П.Г. Определение обфускации JavaScript-программ с помощью раскрасок на абстрактных синтаксических деревьях // Математика и математическое моделирование. 2020. № 2. С. 1-24. DOI: 10.24108/mathm.0220.0000218.
12. Вишневский А.С., Ключарев П.Г. Обнаружение целенаправленных атак веб-ориентированной обманной системой, основанной на алгоритме антиклассификации // Нейрокомпьютеры: разработка, применение. 2020. Т. 22. № 3. С. 5-17. DOI: 10.18127/j19998554-202003-01.

Saddle point search algorithm in the game task of selecting information protection software for network servers

Bykov A.Yu.⁴², Grishunin M.V.⁴³, Fedorov E.G.⁴⁴, Markova I.A.⁴⁵

Abstract. The game formulation of the problem of two players is presented: a defender and an attacker. The defender selects the information security software for the computer network servers, taking into account the importance of the processed information, and the attacker selects the possible types of attacks. The mathematical formulation of the problem is a discrete-continuous game, the set of solutions of the defender is discrete, and the set of solutions of the attacker is continuous. The game is a zero-sum game, with the defender's damage used as a quality indicator. The defender, given the attacker's solution, solves the Boolean programming problem, and the attacker, given the defender's solution, solves the linear programming problem. An algorithm for finding the saddle point in a mixed strategy for the defender, in a pure strategy for the attacker, based on reducing the continuous problem of the attacker to a discrete one, is proposed. The algorithm is based on the ideas of the Brown-Robinson method, but without explicit construction of the game matrix. To reduce the computational resources of the processor required for the operation of the algorithm, it is proposed that after a given number of steps a new solution is not obtained, not to solve optimization problems, but to search for solutions by brute force among the previously found solutions. An example of solving the problem is given.

Keywords: information security, discrete-continuous game, zero-sum game, boolean programming, linear programming, mixed strategy, pure strategy

⁴²Aleksandr Bykov, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, abykov@bmstu.ru

⁴³Maxim Grishunin, Bauman Moscow State Technical University, Moscow, grishunin-mv@ya.ru

⁴⁴Evgenij Fedorov, Bauman Moscow State Technical University, Moscow, fedorov.evg.msu@gmail.com

⁴⁵Markova Irina, Bauman Moscow State Technical University, Moscow, gurina.irina.94@gmail.com

Некоторые методические замечания к российским криптографическим стандартам ГОСТ Р 34.10 и ГОСТ Р 34.12

Варфоломеев А.А.⁴⁶

Аннотация

Приведены замечание в отношении определения понятия «эллиптическая кривая» в стандарте ГОСТ Р 34.10 – 2012 и замечание к описанию процесса зашифрования в алгоритме Магма стандарта ГОСТ Р 34.12 - 2015.

Ключевые слова: криптография, криптографический стандарт, эллиптическая кривая.

Введение

К настоящему времени в России разработан и применяется целый ряд криптографических стандартов (например, [1-4]). История изучения и использования их насчитывает уже несколько лет. Тем не менее к их изложению можно сделать ряд замечаний, которые позволят сделать их лучше. Здесь будут сделаны замечания к двум стандартам, ГОСТ Р 34.10 – 2012⁴⁷ и ГОСТ Р 34.12 - 2015⁴⁸.

Замечания к ГОСТ Р 34.10 - 2012.

На странице 6 сказано:

«Эллиптической кривой E , определенной над конечным простым полем F_p (где $p > 3$ - простое число), называется множество пар чисел (x, y) , x, y из F_p , удовлетворяющих **тождеству** (выделено мной)

$$y^2 \equiv x^3 + ax + b \pmod{p}, \quad (1)$$

где a, b из F_p и $4a^3 + 27b^2$ не сравнимо с нулем по модулю p ».

Вместе с тем известно, что «Тождество – равенство двух аналитических выражений, справедливое для любых допустимых значений входящих в него букв».

«Для обозначения $\equiv$ применяется знак $\equiv$, введенный Б. Риманом (1857)».

См. например, Математический энциклопедический словарь. Но для обозначения бинарного отношения сравнимости целых чисел по модулю тоже используется подобный знак $\equiv$. Видимо это и ввело в заблуждение авторов текста стандарта, и они вместо термина «сравнение» использовали термин «тождество».

Кроме того, не указано в этом определении эллиптической кривой, относится ли к ней «нулевая точка», как названа в стандарте «точка на бесконечности». Именно эта точка является нейтральным элементом в группе точек кривой по операции сложения.

Замечания к ГОСТ Р 34.12 - 2015.

При описании алгоритма блочного шифрования с длиной блок $n=64$

⁴⁶ Варфоломеев Александр Алексеевич, канд. физ.-мат. н, доцент, МГТУ им. Н.Э. Баумана

⁴⁷ ГОСТ Р 34.10 – 2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

⁴⁸ ГОСТ Р 34.12 – 2015 Информационная технология. Криптографическая защита информации. Блочные шифры.

(называемого «Магма») на странице 10 сказано

Алгоритм зашифрования в зависимости от значений итерационных ключей $K_i \in V_{32}$, $i = 1, 2, \dots, 32$, реализует подстановку $E_{K1}, \dots, K_{32}$, заданную на множестве V_{64} в соответствии с равенством

$$E_{K1}, \dots, K_{32}(a) = G^*[K_{32}]G[K_{31}] \dots G[K_2]G[K_1](a_1, a_0), \quad (19)$$

где $a = a_1 \| a_0 \in V_{64}$, $a_0, a_1 \in V_{32}$.

В указанном равенстве в левой части преобразование действует на векторном пространстве V_{64} , в то время как справа аргументом является элемент декартового произведения векторных пространств $V_{32} \times V_{32}$.

Правильно переписать соотношение (19) в виде

$$E_{K1}, \dots, K_{32}(a) = G^*[K_{32}]G[K_{31}] \dots G[K_2]G[K_1] R(a),$$

где преобразование $R: V_{64} \rightarrow V_{64} \times V_{64}$ действует следующим образом $(a_1 \| a_0) \rightarrow (a_1, a_0)$. Преобразование R является взаимно однозначным, и обратное к нему преобразование обозначим через $S: V_{64} \times V_{64} \rightarrow V_{64}$, оно задается соотношением $(a_1, a_0) \rightarrow (a_1 \| a_0)$.

Точно также надо переписать формулу (20) в виде

$$D_{K1}, \dots, K_{32}(a) = G^*[K_1]G[K_2] \dots G[K_{31}]G[K_{32}] R(a),$$

где $a = a_1 \| a_0 \in V_{64}$, $a_0, a_1 \in V_{32}$.

Обозначим через $P: V_{32} \times V_{32} \rightarrow V_{32} \times V_{32}$ преобразование $P(a_1, a_0) \rightarrow (a_0, a_1)$. Очевидно, что $P^2 = I$ (I – тождественное преобразование), или $P^{-1} = P$.

Для преобразований G и G^* из стандарта (формулы (16) и (17) соответственно) и введенных преобразований R , $S = R^{-1}$ и P легко показать справедливость следующих утверждений.

Утверждение 1.

$$G^* = S P G.$$

Утверждение 2.

$$P G [K_i] P = G^{-1} [K_i] \text{ для всех } i \text{ от } 1 \text{ до } 32.$$

Из этих двух утверждений следует корректность преобразований зашифрования и расшифрования.

Утверждение 3.

$$D_{K1}, \dots, K_{32}(E_{K1}, \dots, K_{32}(a)) = a \text{ для всех } a = a_1 \| a_0 \in V_{64}, a_0, a_1 \in V_{32}$$

Действительно,

$$\begin{aligned} D_{K1}, \dots, K_{32}(E_{K1}, \dots, K_{32}(a)) &= \\ S P G[K_1]G[K_2] \dots G[K_{31}]G[K_{32}] R (S P G [K_{32}]G[K_{31}] \dots G[K_2]G[K_1] R(a)) &= \\ = S P G[K_1]G[K_2] \dots G[K_{31}]G[K_{32}] P G[K_{32}]G[K_{31}] \dots G[K_2]G[K_1] R(a) &= \\ = S P G[K_1]P P G[K_2] \dots G[K_{31}]P P G[K_{32}] P G[K_{32}]G[K_{31}] \dots G[K_2]G[K_1] R(a) &= \\ = S G^{-1}[K_1] \dots G^{-1}[K_{32}] G[K_{32}]G[K_{31}] \dots G[K_2]G[K_1] R(a) = S R(a) = a. \end{aligned}$$

Вывод

При следующих версиях стандартов ГОСТ Р 34.10 – 2012 и ГОСТ Р 34.12 – 2015 необходимо учесть предложенные выше исправления.

Литература

1. Бабенко Л.К., Санчес Россель Х.А. Исследование симметричной схемы цифровой подписи, разработанной на базе алгоритма "ГОСТ Р 34.12-2015" // Вопросы кибербезопасности. 2018. № 2 (26). С. 52-58.
2. Варфоломеев А.А. О схемах "анонимной цифровой подписи" и схемах цифровой подписи, обеспечивающих анонимность // Вопросы кибербезопасности. 2015. № 1 (9). С. 44-48.
3. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. 2015. №2(10). С. 2–10.
4. Комарова А.В., Менщиков А.А., Коробейников А.Г. Анализ и сравнение алгоритмов цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 // Вопросы кибербезопасности. 2017. №1(19). С 51-55.

Some methodological remarks on Russian cryptographic standards GOST R 34.10 and GOST R 34.12

Varfolomeev A.A.⁴⁹

Abstract.

A remark on the definition of the concept of "elliptic curve" in the GOST R 34.10 - 2012 standard and a remark on the description of the encryption process in the Magma algorithm of the GOST R 34.12 - 2015 standard are given.

Keywords: *cryptography, cryptographic standard, elliptic curve.*

⁴⁹ Varfolomeev A.A, associated professor, Ph.D., Bauman Moscow State Technical University, Moscow

Асимптотическая устойчивости модели динамического конфигурирования структуры вычислительных сетей

Ворончихин И.С.⁵⁰, Соколовский С.П.⁵¹

Аннотация. Предлагаются принципиально новые подходы к построению систем безопасности вычислительных сетей, с целью формирования у злоумышленника ложного представления о составе, структуре и алгоритмах функционирования вычислительной сети посредством управления ее структурно-функциональными характеристиками. Разработана математическая модель динамического конфигурирования структурно-функциональных характеристик вычислительной сети в условиях ведения злоумышленником сетевой разведки. Предлагается провести оценку асимптотической устойчивости (существование финальных вероятностей и соответственно стационарного процесса) разработанной модели к вариациям исходных данных. Полученные результаты позволяют находить оптимальные режимы динамического конфигурирования структурно-функциональных характеристик вычислительных сетей для различных ситуаций.

Ключевые слова: сетевая разведка, вычислительные сети, компьютерная атака, маскирование структуры сети, технология движущейся цели.

Введение

На текущий момент свойство однородности структуры современных вычислительных сетей (ВС) наделяет злоумышленника преимуществом при использовании вычислительного ресурса для реализации компьютерных атак (КА). Предлагаются принципиально новые подходы к построению систем безопасности ВС, с целью формирования у злоумышленника ложного представления о составе, структуре и алгоритмах функционирования вычислительной сети посредством управления ее структурно-функциональными характеристиками (СФХ) [1-3].

При математической постановке задачи на моделирование динамического конфигурирования СФХ ВС определена главная задача – за счет вариации параметров динамической конфигурации СФХ ВС скрыть состав, структуру и алгоритмы функционирования ВС от сетевой разведки (СР) и перевести ВС в заранее заданную конфигурацию при реализации противником КА [4, 5].

Под динамической конфигурацией СФХ ВС понимается такое управление сетевыми параметрами и взаимосвязями элементов ВС, при котором длительность их стационарного состояния изменяется адаптивно, и может быть установлено таким, что будет меньше длительности времени сбора противником информации о составе, структуре и алгоритмах функционирования ВС [1, 2]. Периодичность динамической конфигурации СФХ задается декларативно и может быть меньшей, равной или большей значения времени сетевого сканирования средств СР злоумышленника, в зависимости от их технических характеристик [6].

⁵⁰ Ворончихин Иван Сергеевич, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, 5.00@mail.ru

⁵¹ Соколовский Сергей Петрович, к.т.н, доцент, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, ssp.vrn@mail.ru

Модель динамического конфигурирования вычислительных сетей

Разработана модель динамического конфигурирования СФХ ВС в условиях СР. Моменты возможных переходов моделируемой системы из состояния в состояние неопределенны, случайны и происходят под действием потоков событий, характеризующиеся их интенсивностями λ , характеризующими среднее число событий, приходящееся на единицу времени [7, 8].

Сценарий перехода моделируемой системы из состояния в состояние под воздействием потоков событий с различными интенсивностями представлен на рис.1, где S_1 – начальное состояние моделируемой системы (состояние покоя системы).

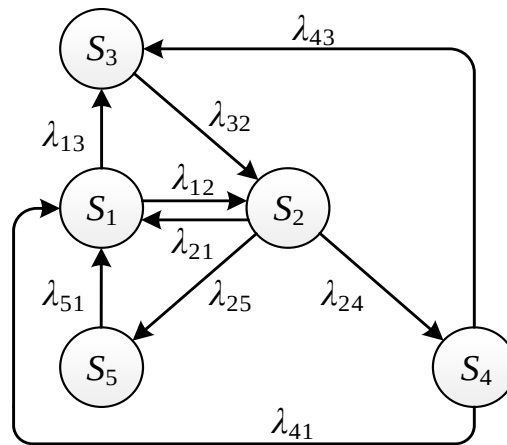


Рис.1. Граф состояний функционирования ВС

По размеченному графу состояний (рис.1) строится математическая модель ее функционирования (1).

$$\left. \begin{aligned} \frac{dp_1(t)}{dt} &= \lambda_{21}p_2(t) + \lambda_{51}p_5(t) - \lambda_{12}p_1(t) + \lambda_{41}p_4(t) - \lambda_{13}p_1(t), \\ \frac{dp_2(t)}{dt} &= \lambda_{12}p_1(t) + \lambda_{32}p_3(t) - \lambda_{21}p_2(t) - \lambda_{24}p_2(t) - \lambda_{25}p_2(t), \\ \frac{dp_3(t)}{dt} &= \lambda_{13}p_1(t) - \lambda_{32}p_3(t) + \lambda_{43}p_4(t), \\ \frac{dp_4(t)}{dt} &= \lambda_{24}p_2(t) - \lambda_{43}p_4(t) - \lambda_{41}p_4(t), \\ \frac{dp_5(t)}{dt} &= \lambda_{25}p_2(t) - \lambda_{51}p_5(t). \end{aligned} \right\} \quad (1)$$

В качестве метода решения системы линейных дифференциальных уравнений выбран классический метод четвертого порядка – метод Рунге-Кутты с фиксированным шагом интегрирования [6, 9-11].

Оценим асимптотическую устойчивость (существование финальных вероятностей и соответственно стационарного процесса) модели к вариациям исходных данных, задавая граничные значения в условиях функционирования ВС, для этого определим диапазон возможных значений интенсивностей λ_i

определяющих различные ситуации конфигурирования ВС.

Определим диапазон возможных значений интенсивностей λ_i , определяющих различные ситуации конфигурирования ВС.

В исходной ситуации ВС функционирует без воздействия средств СР, в штатном режиме, СФХ сетевым устройствам распределены, осуществляется информационный обмен. По истечению времени аренды СФХ сетевых устройств ВС они штатно изменяются в ручном или автоматическом режиме администратором.

Рассмотрим ситуацию, когда ВС функционирует в условиях воздействия средств СР. Средства СР обнаружены штатными средствами защиты ВС. СФХ сетевым устройствам распределены, осуществляется информационный обмен. По истечению времени аренды СФХ сетевых устройств ВС они изменяются автоматическим или администратором. При отсутствии возможности увеличения интенсивности заявок на внештатное конфигурирование СФХ сетевых устройств ВС, чтобы предотвратить вскрытие средствами СР СФХ сетевых устройств ВС, штатные средства защиты наращивают интенсивность потока заявок на обнаружение средств СР и оценку результативности обнаружения средств СР.

Модель позволяет вскрыть зависимость процесса динамического конфигурирования СФХ ВС от потоков воздействий, оценивать качество обслуживания клиентов, обоснованно выбирать алгоритмы защиты ВС от перегрузки и оптимально использовать ресурс сервера.

Условием эргодичности однородного марковского процесса с непрерывным временем является отрицательность действительной части корней характеристического уравнения матрицы коэффициентов (то есть собственных чисел матрицы) [1, 6, 12].

Для поиска допустимого интервала варьирования значений интенсивностей $\lambda_{24}=x$ и $\lambda_{32}=y$, при которых процесс обладает свойством эргодичности, определены зависимости действительной части собственных чисел матрицы коэффициентов от данных интенсивностей в ситуации, представленные в графическом виде на Рисунке 2.

Как видно из рис.2 в рассматриваемом диапазоне значений $\lambda_{24} \in [0; 2000]$, $\lambda_{32} \in [0; 2000]$ действительные части собственных чисел матрицы, характеризующей систему дифференциальных уравнений Колмогорова, принимают отрицательные значения, следовательно, цепь Маркова с непрерывным временем при рассматриваемых значениях интенсивностей потоков событий, асимптотически устойчива (эргодична).

Далее, рассмотрим использование модели при вариациях исходных данных, определяющих вышеприведенную ситуацию.

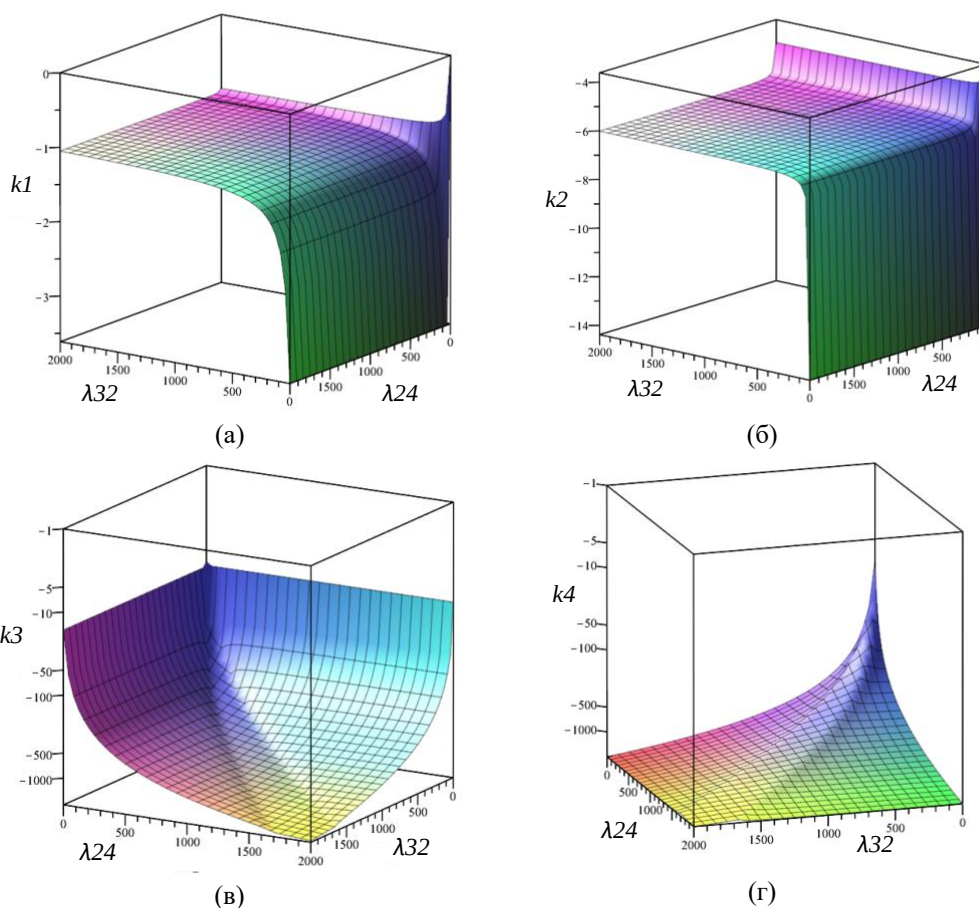


Рис.2. Зависимости действительной части собственных чисел (k_1 (а), k_2 (б), k_3 (в), k_4 (г)) от варьируемых интенсивностей потоков событий применительно к моделируемой ситуации, при варьировании значений интенсивности λ

При $t \rightarrow \infty$ в моделируемой системе устанавливается стационарный режим, когда ВС случайным образом меняет свои состояния и ее вероятности $p_1(t), p_2(t), \dots, p_5(t)$ уже не зависят от времени и равны финальным (предельным) вероятностям (рис.3).

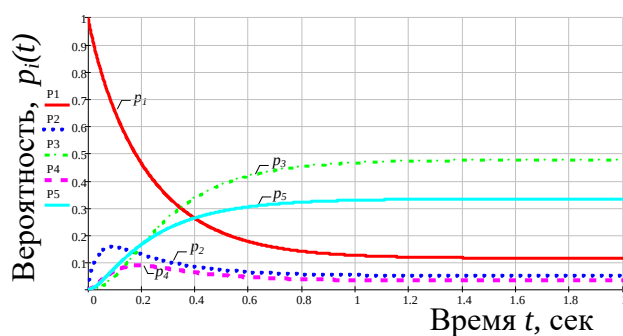


Рис.3. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие исследуемой ситуации

Аналогичным образом производятся расчеты для других ситуаций конфигурирования СФХ вычислительной сети.

Выводы

Внедрение предлагаемых научных решений позволит при выборе диапазонов варьирования интенсивностей потоков событий, решить вопрос оценки ограничений на данные параметры, то есть определения эргодичности и устойчивости случайного процесса, при различных значениях входных параметров.

Таким образом, разработанная математическая модель марковского процесса обладает асимптотической устойчивостью в широком диапазоне варьируемых значений интенсивностей потоков событий в рамках рассматриваемых ситуаций конфигурирования СФХ ВС в условиях применения злоумышленником средств СР.

Литература

1. Ворончихин И.С., Иванов И.И., Максимов Р.В., Соколовский С.П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 92-101. DOI: 10.21681/2311-3456-2019-6-92-101.
2. Соколовский С.П., Ворончихин И.С., Королев В.А., Тимошенко В.К. Разработка программного комплекса средств динамической конфигурации структурно-функциональных характеристик вычислительных сетей. Сборник XXIV Международной научно-практической конференции «Решетневские чтения» / под общ. ред. Ю.Ю. Логинова – Красноярск.: СибГУ им. ак. М.Ф. Решетнева, 2020. Том 2. С. 545-547.
3. Соколовский С.П., Ворончихин И.С., Гритчин А.Д. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров. Сборник XXIII Международной научно-практической конференции «Решетневские чтения» / под общ. ред. Ю.Ю. Логинова – Красноярск.: СибГУ им. ак. М.Ф. Решетнева, 2019. Том 2. С. 447-448.
4. Максимов Р.В., Соколовский С.П., Ворончихин И.С., Гритчин А.Д., Боядкин М.С., Игнатенко А.В. Способ защиты вычислительных сетей // Патент на изобретение RU 2726900, опубл. 16.07.2020, Бюл. № 7, 33 с.
5. Максимов Р.В., Орехов Д.Н., Соколовский С.П., Барабанов В.В., Ефремов А.А., Ворончихин И.С. // Патент на изобретение RU 2696330, опубл. 01.08.2019, Бюл. № 22, 30 с.
6. Максимов Р.В., Соколовский С.П., Ворончихин И.С. // Патент на изобретение RU 2716220, опубл. 06.03.2020, Бюл. № 20, 49 с.
7. Максимов Р.В., Соколовский С.П., Ворончихин И.С. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей // Информатика и автоматизация. 2020. № 5 (2020). С. 1018-49. DOI: 10.15622/ia.2020.19.5.
8. Maximov R., Krupenin A., Sharifullin S., Sokolovsky S. Innovative Development of Tools and Technologies to Ensure the Russian Information Security and Core Protective Guidelines // Voprosy kiberbezopasnosti [Cybersecurity issue], 2019, N 1 (29), pp. 10-17. DOI: 10.21681/2311-3456-2019-1-10-17.
9. Ворончихин И.С. Динамическое изменение структурно-функциональных характеристик информационной системы в целях снижения эффективности сетевой разведки // Безопасные информационные технологии: сб. тр. конференции Десятая Междунар. науч.-технич. конф. «Безопасные информационные технологии». – М. 2019. С. 81-87.
10. Шерстобитов Р. С., Шарифуллин С. Р., Максимов Р. В. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и

безопасности. 2018. № 4. С. 136-175. URL: <http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf>.

11. Максимов Р.В., Соколовский С.П., Чернолес В.П., Шарифуллин С.Р. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. №3 (233). С. 28-35.

12. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50-99. DOI: 10.24411/2410-9916-2019-10403

Asymptotic stability of the dynamic configuration structure model of the computer networks

Voronchikhin I.S.⁵², Sokolovsky S.P.⁵³

Abstract: *fundamentally new approaches to the construction of computer network security systems are proposed in order to form a false idea of the composition, structure and algorithms of the computer network functioning by controlling its structural and functional characteristics. A mathematical model of dynamic configuration of the structural and functional characteristics of a computer network under the conditions of conducting network intelligence by an attacker is developed. It is proposed to evaluate the asymptotic stability (the existence of final probabilities and, accordingly, a stationary process) of the developed model to the variations of the initial data. The obtained results allow us to find optimal modes of dynamic configuration of the structural and functional characteristics of computer networks for various situations.*

Keywords: *network intelligence, computer networks, computer attack, masking network structure, moving target defense technology.*

УДК 004.65+004.438.5

⁵² Ivan Voronchikhin, Ph.D. Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia, 5.00@mail.ru

⁵³ Sergey Sokolovsky, Ph.D., Associate Professor, Doctoral Student, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia, ssp.vrn@mail.ru

Модель защиты сервиса электронной почты от сетевой разведки управлением параметрами передачи сообщений

Горбачев А.А.⁵⁴, Соколовский С.П.⁵⁵

***Аннотация.** Приведен анализ информационных угроз и средств защиты сервиса электронной почты. Разработана математическая модель по оценке вероятностно-временных характеристик режимов управления параметрами сетевых соединений клиентов и сервера электронной почты с учетом асимптотической устойчивости и робастности. Приведены расчеты показателей эффективности и вероятностно-временных характеристик процесса взаимодействия средств защиты с потенциальным злоумышленником. Новизна представленной модели заключается в использовании математического аппарата однородных цепей Маркова с непрерывным временем с целью выбора оптимального режима управления параметрами сетевого соединения средствами защиты сервиса электронной почты в условиях сетевой разведки с учетом свойств асимптотической устойчивости и робастности.*

***Ключевые слова:** случайный процесс, цепь Маркова, сетевая ловушка, компьютерная атака, робастность, устойчивость.*

Введение

В связи с популярностью сервиса электронной почты возникла проблема активизации деятельности злоумышленников по проведению массовых и целевых атак, посредством которой может быть реализована деятельность рекламного характера, фишинг, внедрение вредоносного программного обеспечения, кража интеллектуальной собственности, мошенничество, нарушение доступности сервиса электронной почты. Сетевая разведка является наиболее важным этапом подготовки компьютерных атак [1-6].

Сетевая разведка проводится с целью добывания информации о составе, структуре, алгоритмах функционирования, местоположении, принадлежности элементов системы электронной почты, анализа хранимых, обрабатываемых данных и осуществляется для поиска потенциальных целей, их уязвимостей и направлений сосредоточения усилий при реализации компьютерных атак или иных злонамеренных воздействий [9-11].

Повышение защищенности сервиса электронной почты достигается за счет имитации канала связи с плохим качеством посредством использования возможностей протокола SMTP по контролю сетевого соединения сервера с клиентом на различных этапах почтовой транзакции, обеспечивающей значительное использование вычислительного ресурса злоумышленника, предотвращение и (или) затруднение проведения сетевой разведки и распределенных компьютерных атак.

Анализ информационных угроз и применяемых средств защиты

⁵⁴ Горбачев Александр Александрович, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, druzhochek123@yandex.ru

⁵⁵ Соколовский Сергей Петрович, кандидат технических наук, доцент, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, ssp.vrn@mail.ru

сервиса электронной почты

Предпосылками формирования информационных угроз сервиса электронной почты являются [12-15]:

популярность сервиса электронной почты в ходе электронной переписки между рядовыми пользователями, организациями, институтами различных ведомств;

открытость архитектуры и уязвимости сетевых протоколов прикладного уровня, на которых функционирует сервис электронной почты;

использование не декларированных возможностей аппаратного и программного обеспечения средств вычислительной техники, обеспечивающих функционирование сервиса электронной почты;

совершенствование средств и методов ведения сетевой разведки и компьютерных атак на инфраструктуру сервиса электронной почты за счет роста мобильности и количества конечных устройств.

Обеспечение конфиденциальности и целостности передаваемой информации осуществляется за счет использования средств криптографической защиты сервиса электронной почты, таких как стандарты S/MIME, PGP. Проверка содержимого электронных сообщений на предмет спама и вредоносного программного обеспечения реализуется средствами фильтрации, антивирусной защиты, аутентификации. Применение традиционных средств анализа содержимого электронных сообщений, криптографической защиты информации и аутентификации в полной мере не позволяют обеспечить защиту от массовых и целевых атак, основанных на методах: подмены IP-адресов отправителей (spoofing), DDOS и DOS-атаках, фишинге, распространения спама и вредоносного программного обеспечения, NDR-атаках (Non Delivery Report attack), петлях системы электронной почты (mail loops) [16-20].

Сущность управления параметрами сетевого соединения сервиса электронной почты состоит в регулировании длительности ответных откликов сервера за счет направления промежуточных ответных откликов, разбиения ответного отклика на фрагменты и их отправки через различные промежутки времени, а также направлении злоумышленнику заведомо ложных сообщений о временной или постоянной недоступности сервиса электронной почты.

Модель защиты сервиса электронной почты от сетевой разведки управлением параметрами передачи сообщений

Формализованная постановка задачи включает в себя определение вида математической модели описываемого процесса, основных параметров и ограничений.

Вероятностно-временные характеристики эффективности функционирования сервиса электронной почты в условиях сетевой разведки позволяет определить моделирование системы с использованием математического аппарата случайных процессов. В модели используется однородная цепь Маркова с непрерывным временем (марковский процесс с дискретными состояниями и непрерывным временем). Однородность марковского процесса обусловлена стационарностью случайного процесса в широком смысле слова, характеризующаяся независимостью математического ожидания (интенсивностей простейших потоков событий), дисперсии случайного процесса от параметра (времени) и зависимостью

корреляционной функции процесса только от величины промежутка времени.

Определяемые параметры и ограничения:

минимизация вероятности передачи злоумышленником вредоносного электронного сообщения как параметр эффективности:

$$\langle MIP, Z \rangle \rightarrow \min P_{ABD} = \lim P_{ABD}(t) | P_{ABD} \in P_i, i = 1, 2, \dots, h, \quad (1)$$

максимизация вероятности удержания злоумышленника и доступности сервиса электронной почты:

$$\langle MIP, Z \rangle \rightarrow \min P_{ABD} = \lim P_{ABD}(t) | P_{ABD} \in P_i, i = 1, 2, \dots, h, \quad (2)$$

где, Z – множество внутренних параметров модели,

$$Z \subseteq \{S_i, A_{ij}, p_i(0)\}, \quad (3)$$

где, $S_i = \{S_1, \dots, S_h\}$ – множество моделируемых состояний системы,

$$S_i = \{S_1, \dots, S_h\}, \quad (4)$$

A_{ij} – интенсивности простейших потоков событий (заявок) в ней,

$$A_{ij} = \{\lambda_{11}, \lambda_{12}, \dots, \lambda_{ij}\}, \quad (5)$$

MIP – множество входных параметров модели, параметров динамического контроля сетевого соединения сервером электронной почты,

$$MIP \subseteq \{I_{cmax}, L_{cmax}, T, d, u, m, y\}, \quad (6)$$

I_{cmax} – максимальное значение количества подключений клиента сервера электронной почты;

$$I_{cmax} = [1, 2, \dots, n], \quad (7)$$

$p_i(0)$ – распределение вероятностей пребывания системы в состояниях в начальный момент времени;

$$p_i(0) = \{p_1(0), p_2(0), \dots, p_i(0)\}, \quad (8)$$

I_{cmax} – максимальное значение количества подключений клиента сервера электронной почты;

$$I_{cmax} = [1, 2, \dots, n], \quad (9)$$

L_{cmax} – максимальное значение количества подключений клиента сервера электронной почты;

$$L_{cmax} = [1, 2, \dots, 10000], \quad (10)$$

T – значение времени задержки промежуточных откликов клиенту сервиса электронной почты, секунд;

$$T = [1, 2, \dots, 10], \quad (11)$$

d – общее количество промежуточных откликов, которые будут направлены клиенту сервиса электронной почты ответным сообщением;

$$d = [1, 2, \dots, R], \quad (12)$$

u – общее количество ответных откликов на команды отправителя сообщений, содержащих коды ошибок;

$$u = [1, 2, \dots, U], \quad (13)$$

m – общее количество фрагментов, на которые разбиваются ответные отклики, направляемые клиенту;

$$m = [1, 2, \dots, G], \quad (14)$$

y – значение времени задержки между отправкой фрагментов откликов клиенту сервиса электронной почты, секунд;

$$y = [1, 2, \dots, 15], \quad (15)$$

Полученная модель представляет собой цепь Маркова с непрерывным временем, которая может быть представлена с помощью ориентированного графа (рис. 1).

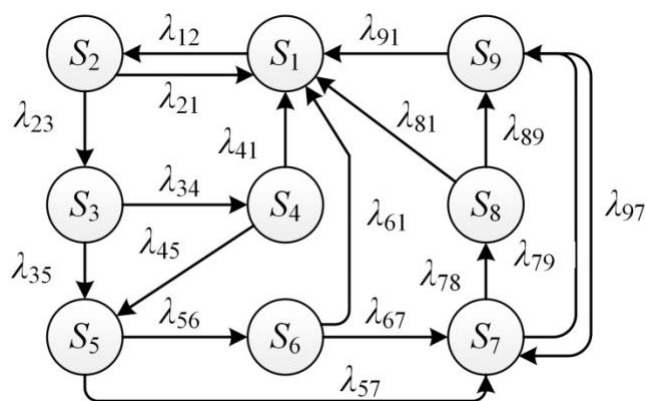


Рис.1. Ориентированный граф состояний сервиса электронной почты в условиях сетевой разведки

Искомые показателями являются вероятностно-временные характеристики случайного процесса: вектор функций безусловных вероятностей $p_i(t)$ нахождения системы в состояниях S_i в любой момент времени, вектор финальных вероятностей p_i (в случае, если случайный процесс обладает свойством эргодичности).

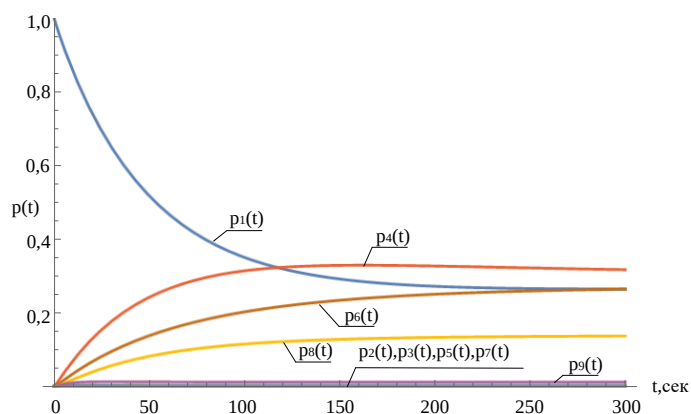


Рис.2. Графическая форма представления решения СДУ Колмогорова для рассматриваемой системы S

Вектор функций $p_i(t)$ является решением системы обыкновенных дифференциальных уравнений (СОДУ) Колмогорова, составленного в соответствии с графом (рис. 1), а p_i решением системы линейных алгебраических уравнений (СЛАУ) Колмогорова с учетом условия нормировки $\sum p_i = 1$. Решение СОДУ осуществляется аналитическими или численными методами в зависимости от размерности матрицы интенсивностей и требований к скорости вычислений (рис. 2).

Важным критерием корректности математической модели является ее устойчивость, то есть чувствительность искомых вероятностно-временных характеристик к погрешностям исходных данных и их стабилизация с течением времени (асимптотическая устойчивость).

Робастность модели (обусловленность, корректность) характеризует возмущение выходных характеристик относительно возмущения входных параметров. Одной из характеристик робастности моделей, описанных СЛАУ, является число обусловленности $cond(B, \infty)$, рассчитанное для векторной нормы Чебышева инфинитезимальной матрицы интенсивностей B , являющейся

линейным оператором СЛАУ (рис. 3). Высокие значения $cond(B, \infty) > 10^4 \dots 10^5$ числа обусловленности характеризуют высокую чувствительность финальных вероятностей к изменению интенсивности воздействия злоумышленника λ_{12} , что-либо предъявляет повышенные требования к точности определения исходных данных либо снижает надежность полученных с помощью модели результатов.

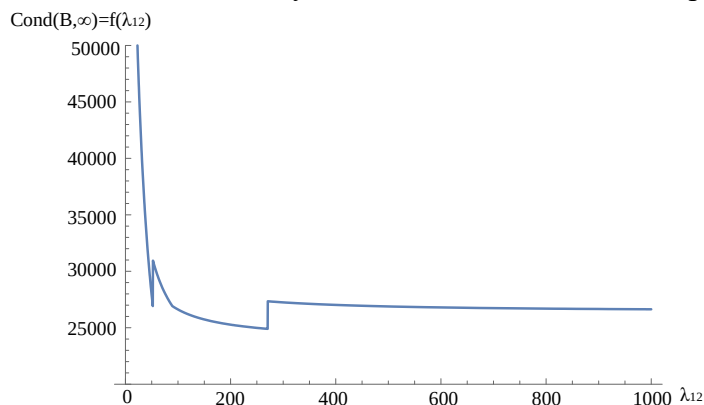


Рис.3. Зависимость числа обусловленности матрицы – линейного оператора СЛАУ Колмогорова моделируемой системы S от интенсивности потока заявок λ_{12} .

Промежуточные результаты показывают, что по мере увеличения величины задержки между промежуточными откликами на первом этапе почтовой транзакции и фрагментами на втором этапе увеличивается вероятность удержания злоумышленника, но по мере приближения значения задержки к тайм-ауту разрыва соединения злоумышленника (около 1 минуты), вероятность удержания стабилизируется ($p_4(t) + p_6(t) < 0,40$). Также с ростом средней суммарной длительности задержки с одной стороны уменьшается вероятность успешной передачи вредоносного сообщения злоумышленником ($p_9(t) < 0,01$), а с другой стороны снижается доступность сервиса электронной почты для легитимных пользователей ($p_1(t) < 0,60$).

Выводы

Использование разработанной математической модели в структуре средств защиты сервиса электронной почты обеспечит повышение защищенности серверов передачи почты от сетевой разведки и компьютерных атак за счет управления параметрами сетевых соединений в ходе почтовой транзакции.

Оценка робастности и асимптотической устойчивости модели позволит установить требования к качеству исходных данных и интерпретации результатов расчетов.

Литература

1. Кучуров В.В., Максимов Р.В., Шерстобитов Р.С. Модель и методика маскирования адресации корреспондентов в киберпространстве // Вопросы кибербезопасности. 2020. № 6 (40). С. 2-13.
2. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50-99.
3. Ворончихин И.С., Иванов И.И., Максимов Р.В., Соколовский С.П. Маскирование структуры распределённых информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 92-101.
4. Крупенин А.В., Соколовский С.П., Хорев Г.А., Калач А.В. Маскирование идентификаторов канального уровня средств проактивной защиты интегрированных сетей

связи специального назначения // Вестник Воронежского института ФСИН России. 2018. № 3. С. 81–89.

5. Maximov R.V., Krupenin A.V., Sharifullin S.R., Sokolovsky S.P. Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines // Вопросы кибербезопасности. 2019. № 1 (29). С. 10–17.

6. Максимов Р.В., Соколовский С.П., Шарифуллин С.Р., Чернолес В.П. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. № 3 (233). С. 28–35.

7. Соколовский С.П., Ворончихин И.С. Обоснование задач динамического конфигурирования информационных систем для обеспечения их безопасности // Радиоэлектронная борьба в современном мире: сб. тр. участников I Всерос. научно-методич. конф. «Радиоэлектронная борьба в современном мире». – Воронеж. 2019. С. 300–304.

8. Соколовский, С.П. Концептуализация проблемы проактивной защиты интегрированных информационных систем / С.П. Соколовский, Д.Н. Орехов // Научные чтения имени профессора Н.Е. Жуковского: сб. тр. участников VIII Междунар. научно-практической конф. "Научные чтения имени профессора Н.Е. Жуковского" (Краснодар, 20–21 декабря 2017 г.). – Краснодар, 2017. – С. 47–52.

9. Максимов Р.В., Соколовский С.П., Ворончихин И.С. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей // Цифровые информационно-телекоммуникационные технологии. 2020. Т. 19. № 5. С. 1090–1121. DOI: 10.15622/ia2020.19.5.7.

10. Sokolovsky S.P., Telenga A.P., Voronchikhin I.S. Moving target defense for securing Distributed Information Systems // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции / под редакцией Д.Н. Борисова. – Воронеж.: ВГУ, 2019. С. 639–643.

11. Соколовский С.П., Ворончихин И.С., Гритчин А.Д. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров // Решетневские чтения: сб. тр. участников XXIII Междунар. науч.-практич. конф., посвященной памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева «Решетневские чтения». – Красноярск. 2019. Ч.2. С. 447–448.

12. Усов Н.А., Соколовский С.П. Моделирование процесса функционирования устройства выявления несанкционированных воздействий на информационную телекоммуникационную систему // Информатика: проблемы, методология, технологии. Материалы XV Международной научно-методической конференции. 2015. С. 224–227.

13. Соколовский С.П., Усов Н.А. Применение адаптивных нечетких систем в вопросах разработки средств выявления несанкционированных воздействий на информацию // Информатика: проблемы, методология, технологии. Материалы XVI Международной научно-методической конференции. Под редакцией Тюкачева Н.А. 2016. С. 259–264.

14. Душкин А.В., Соколовский С.П. Нейросетевая реализация модуля выявления несанкционированных воздействий на информационную телекоммуникационную систему специального назначения // Информация и безопасность. 2010. № 1. С. 123–126.

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

16. Maximov R. V., Ivanov I. I., Sharifullin S. R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). (Moscow, 6–7 December 2017) – Moscow, Bauman Moscow Technical University, 2017. P. 83–87.

17. Iskolnyy B. B., Maximov R. V., Sharifullin S. R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT

2017). (Moscow, 6-7 December 2017) – Moscow, Bauman Moscow Technical University, 2017. P. 59-65.

18. Maximov R. V., Sokolovsky S. P., Gavrilov A. L. Hiding computer network proactive security tools unmasking features // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). (Moscow, 6-7 December 2017) – Moscow, Bauman Moscow Technical University Publ., 2017. P. 88-92.

19. Максимов Р. В., Соколовский С. П., Орехов Д. Н. Особенности детектирования и способы маскирования демаскирующих признаков средств проактивной защиты вычислительных сетей // Радиолокация, навигация, связь: Сборник трудов XXIV Международной научно-технической конференции. Том 2. – Воронеж: ООО «Вэлборн», 2018. С. 169-179

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

A model for protecting an email service from network intelligence by managing message transmission parameters

Gorbachev A. A.⁵⁶, Sokolovsky S. P.⁵⁷

Abstract. *The analysis of information threats and means of protection of e-mail is given. A mathematical model for evaluating the probabilistic-temporal characteristics of managing transmission parameters modes in e-mail, taking into account the asymptotic stability and robustness is developed. Calculations of efficiency indicators and probabilistic-time characteristics of the process of interaction of security tools with a potential attacker are given. The novelty of the presented model consists in the use of the mathematical apparatus of homogeneous Markov chains with continuous time in order to select the optimal mode of managing transmission parameters by means of protecting the e-mail service in the conditions of network intelligence, taking into account the properties of asymptotic stability and robustness.*

Keywords: *random process, Markov chain, network trap, computer attack, robustness, stability.*

⁵⁶ Gorbachev Alexandr Alexandrovich, Krasnodar higher military school named after army General S. M. Shtemenko, Krasnodar, druzhocek123@yandex.ru

⁵⁷ Sokolovsky Sergey Petrovich, PhD. of Engineering Sciences, Associate Professor, Krasnodar higher military school named after army General S. M. Shtemenko, Krasnodar, ssp.vrn@mail.ru

Зависимость среднего числа решений в задаче о ранце от параметров области ограничений

Леонтьев В.К.⁵⁸, Гордеев Э.Н.⁵⁹

Аннотация. Задача о рюкзаке (задача о ранце) используется во многих математических моделях, в том числе и в области информационной безопасности. Решение задачи (нахождение оптимальной загрузки рюкзака) или даже ответ на вопрос о существовании допустимого решения – это NP-полная проблема. В связи с этим актуален вопрос о нахождении мощности множества допустимых решений или оценок этой мощности. В работе анализируются комбинаторные аспекты этой проблемы на основе метода производящих функций. Получены формулы и оценки для числа допустимых решений и среднего числа допустимых решений зависимости от коэффициентов вектора ограничений. На их основе могут быть построены вычислительные алгоритмы нахождения указанных величин. Все это может быть использовано для оценки адекватности и качества исходной математической модели.

Ключевые слова: задача о рюкзаке, допустимые решения, производящие функции, оценки числа решений, NP-полнота.

Введение

Задача о рюкзаке с булевыми переменными имеет вид:

$$\begin{aligned} \sum_{j=1}^n c_j x_j &\rightarrow \max; \\ \sum_{i=1}^n a_i x_i &\leq b, \end{aligned} \quad (1)$$

где $x=(x_1, \dots, x_n)$ – n -мерный булевский вектор.

Везде в дальнейшем будем считать, что все параметры рассматриваемой задачи – неотрицательные целые числа.

Множество допустимых решений этой задачи V_b – это множество булевых векторов, удовлетворяющих неравенству

$$\sum_{i=1}^n a_i x_i \leq b. \quad (2)$$

Объем V_b – это число $|V_b|$ допустимых решений задачи (2).

Это классическая задача комбинаторной оптимизации (см. [1], [2]). Данная работа является продолжением исследований, проведенных в [3], [4]. Различные аспекты

⁵⁸ Леонтьев Владимир Константинович, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, vkleontiev@yandex.ru. Грант РФФИ 20-01-00645.

⁵⁹ Гордеев Эдуард Николаевич, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, werhorn@gmail.com. Грант РФФИ 20-01-00645.

задачи о рюкзаке, связанные с тематикой данной работы, изучались, например, в [2], [5], [6].

Везде в дальнейшем будем считать, что все параметры рассматриваемой задачи, числа $c_1, \dots, c_n$; $a_1, \dots, a_n$; b – неотрицательные целые числа.

Производящие функции для числа допустимых решений

Вначале непосредственно выразим объем допустимых решений с помощью

производящей функции для $P_b(z_1, \dots, z_n) = \sum_{x \in V_b} z_1^{a_1 x_1} z_2^{a_2 x_2} \dots z_n^{a_n x_n}$. В [4] доказана лемма.

Лемма 1. Справедлива формула

$$\sum_{b=0}^{\infty} P_b(z_1, \dots, z_n) u^b = \frac{(1 + (z_1 u)^{a_1}) \dots (1 + (z_n u)^{a_n})}{1 - u}. \quad (3)$$

Следствие. Пусть $0 < \rho < 1$. Тогда для объема области допустимых решений имеет место равенство.

$$|V_b| = \frac{1}{2\pi i} \oint_{|u|=\rho} \frac{(1 + u^{a_1}) \dots (1 + u^{a_n})}{(1 - u) u^{b+1}} du. \quad (4)$$

Среднее число допустимых решений

Рассмотрим теперь вопрос о среднем значении объема допустимых решений. Пусть

$$|\overline{V_b}| = \frac{1}{(b+1)^n} \sum_{\substack{\{a_1, \dots, a_n\} \\ 0 \leq a_i \leq b, 1 \leq i \leq n}} |V_b|. \quad (5)$$

Напомним, что переменные у нас булевы. Число b фиксировано, фиксирована также размерность n . Поэтому каждый коэффициент вектора ограничений меняется от 0 до b , т.е. принимает $n+1$ значение. Отсюда и следует (5).

Конечно, вопрос о среднем числе допустимых значений носит, скорее, теоретический характер. Однако, он проливает свет на комбинаторику задачи при исследовании взаимозависимости b и n .

Ниже мы приводим несколько утверждений, дающих различные формулы (алгоритмы расчета) среднего числа допустимых решений. В качестве

иллюстрации использования метода производящих функций представлены и их доказательства.

Теорема 1. Справедлива формула

$$|\overline{V_b}| = \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k C_b^{n-k} (b+2)^k. \quad (6)$$

Доказательство. Непосредственно из (4) и (5) имеем

$$|\overline{V_b}| = \frac{1}{(b+1)^n} \frac{1}{2\pi i} \oint_{|u|=\rho} \left\{ \frac{\sum_{a_1=1}^b (1+u^{a_1}) \dots \sum_{a_n=1}^b (1+u^{a_n})}{(1-u)u^{b+1}} \right\} du.$$

Далее заметим, что, во-первых,

$$\sum_{a_k=0}^b (1+u^{a_k}) = 2 + (1+u) + \dots + (1+u^b) = 2 + b + \frac{u-u^{b+1}}{1-u}.$$

$$\text{Во-вторых, } (1-u^b)^{n-k} = 1 - C_{n-k}^1 u^b + C_{n-k}^2 u^{2b} - \dots = \sum_{i=0}^{n-k} (-1)^i C_{n-k}^i u^{ib}.$$

Поэтом далее имеем

$$\begin{aligned} |\overline{V_b}| &= \frac{1}{(b+1)^n} \frac{1}{2\pi i} \oint_{|u|=\rho} \left\{ \frac{\left(b+2 + \frac{u-u^{b+1}}{1-u} \right)^n}{(1-u)u^{b+1}} \right\} du = \frac{1}{(b+1)^n} \frac{1}{2\pi i} \oint_{|u|=\rho} \left\{ \frac{\left((b+2)(1-u) + u(1-u^b) \right)^n}{(1-u)^{n+1} u^{b+1}} \right\} du = \\ &= \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k (b+2)^k \frac{1}{2\pi i} \oint_{|u|=\rho} \left\{ \left(\frac{u}{1-u} \right)^{n-k} \frac{(1-u^b)^{n-k}}{u^{b+1}} \frac{1}{1-u} \right\} du. \end{aligned}$$

$$\text{Теперь заметим, что } (1-u^b)^{n-k} = 1 - C_{n-k}^1 u^b + C_{n-k}^2 u^{2b} - \dots = \sum_{i=0}^{n-k} (-1)^i C_{n-k}^i u^{ib}. \quad (7)$$

Поэтому из (7) следует:

$$\frac{1}{2\pi i} \oint_{|u|=\rho} \left\{ \frac{(1-u)^{-n+k-1} (1-u^b)^{n-k}}{u^{b+1+k-n}} \right\} du = \frac{1}{2\pi i} \oint_{|u|=\rho} \left\{ \frac{(1-u)^{-n+k-1}}{u^{b+1+k-n}} \right\} du = (-1)^{b+k-n} C_{-(n-k+1)}^{b+k-n}.$$

После очевидных преобразований получаем

$$(-1)^{b+k-n} C_{-n+k-1}^{b+k-n} = (-1)^{b+k-n} C_{-(n-k+1)}^{b+k-n} = C_b^{b+k-n} = C_b^{n-k}. \quad (8)$$

Но теперь из (7) и (8) следует утверждение леммы.

Теорема доказана.

Посмотрим на это выражение с другой стороны.

Теорема 2. Справедлива формула

$$|\overline{V_b}| = \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k C_{b+k}^b (b+1)^{n-k}. \quad (9)$$

Доказательство. Применим метод коэффициентов к вычислению суммы

$$|\overline{V_b}| = \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k C_b^{n-k} (b+2)^k. \text{ Получим цепочку соотношений:}$$

$$\begin{aligned} |\overline{V_b}| &= \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k (b+2)^k \underset{u}{Coef} \left\{ (1+u)^b u^{-b+n-k-1} \right\} = \frac{1}{(b+1)^n} \underset{u}{Coef} \left\{ \frac{(1+u)^b}{u^{b-n+1}} \sum_{k=0}^n C_n^k \left(\frac{b+2}{u} \right)^k \right\} = \\ &= \frac{1}{(b+1)^n} \underset{u}{Coef} \left\{ \frac{(1+u)^b}{u^{b-n+1}} \left(1 + \left(\frac{b+2}{u} \right)^n \right) \right\} = \frac{1}{(b+1)^n} \underset{u}{Coef} \left\{ \frac{(1+u)^b}{u^{b+1}} (u+b+2)^n \right\} = \\ &= \frac{1}{(b+1)^n} \underset{u}{Coef} \left\{ \frac{(1+u)^b}{u^{b+1}} ((1+u) + (b+1))^n \right\} = \\ &= \frac{1}{(b+1)^n} \underset{u}{Coef} \left\{ \frac{\sum_{k=0}^n C_n^k (1+u)^k (b+1)^{n-k}}{u^{b+1}} \right\} (1+u)^b = \\ &= \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k (b+1)^{n-k} \underset{u}{Coef} \left\{ \frac{(1+u)^{b+k}}{u^{b+1}} \right\} (1+u)^b = \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k C_{b+k}^b (b+1)^{n-k}. \end{aligned}$$

Теорема доказана.

Примеры

1. Пусть $n=b=2$, тогда имеем 9 ограничений: 1) $x_1+x_2 \leq 2$; 2) $2x_1+x_2 \leq 2$; 3) $x_1+2x_2 \leq 2$; 4) $2x_1+2x_2 \leq 2$. И еще 4 с одной переменной, а также с двумя нулевыми коэффициентами при переменных. Последние 5 имеют по четыре решения, а для первых четырех имеем: $|V_1|=4$; $|V_2|=3$; $|V_3|=3$; $|V_4|=3$. Непосредственно получаем: $|\overline{V_b}| = 33/9 = 11/3$.

То же получаем из (9).

$$\begin{aligned} |\overline{V_b}| &= \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k C_{b+k}^b (b+1)^{n-k} = \frac{1}{3^2} \sum_{k=0}^2 C_2^k C_{2+k}^2 3^{2-k} = \\ &= \frac{1}{3^2} (C_2^0 C_2^2 3^2 + C_2^1 C_3^2 3^1 + C_2^2 C_4^2 3^0) = 33/9 = 11/3. \end{aligned}$$

2. Пусть b – любое, а $n=3$. Вид ограничений очевиден. Непосредственный подсчет $|\overline{V_b}|$ затруднителен, а из (9) сразу получаем:

$$|\overline{V_b}| = \frac{1}{(b+1)^n} \sum_{k=0}^n C_n^k C_{b+k}^b (b+1)^{n-k} = \frac{1}{(b+1)^3} \sum_{k=0}^3 C_3^k C_{b+k}^b (b+1)^{n-k} =$$

$$= \frac{1}{(b+1)^3} ((b+1)^3 + 3(b+1)^3 + 3(b+2)(b+1)^2 / 2 + (b+1)(b+1)(b+1) / 6).$$

Это асимптотически равно $5\frac{2}{3}$.

Вывод

Метод производящих функций может быть успешно применен для анализа задач, имеющих «комбинаторную» природу. В приведенном исследовании с его помощью получены новые формулы для числа допустимых решений и среднего числа допустимых решений в задаче о ранце.

Они могут быть улучшены и уточнены при рассмотрении уравнений не общего, а специального вида. Именно такие задачи и возникают в конкретных прикладных областях, в частности в математических моделях информационной безопасности, учитывающих реальные особенности исходных постановок.

Поэтому изложенные здесь результаты могут быть базисом для дальнейших исследований.

Достоверность результатов следует из корректности определений и доказательств теорем.

Литература

1. Пападимитриу Х., Стайглиц С. Комбинаторная оптимизация. М.: Мир. 1989. 512 с.
2. Горшков С.П., Тарасов А.В. Сложность решения систем булевых уравнений. М.: Курс. 2017. 192 с.
3. Леонтьев В.К., Гордеев Э.Н. Производящие функции в задаче о ранце// Доклады Академии наук. 2018. Т. 481. № 5. С. 478 – 480. DOI: 10.31857/S086956520002139-5.
4. Леонтьев В.К., Гордеев Э.Н. О некоторых комбинаторных свойствах задачи о рюкзаке// Журнал вычислительной математики и математической физики. 2019. Т. 59. № 8. С. 1439-1447. DOI: <https://doi.org/10.1134/S0044466919080076>.
5. Леонтьев В.К. Булевы полиномы и линейные преобразования// ДАН. 2009. Т. 425. №3. С. 320-322.
6. Леонтьев В.К. Комбинаторика и информация. Часть 1. Комбинаторный анализ. М.: МФТИ, 2015. 174 с.

Dependence of the average number of solutions in the knapsack problem on the parameters of the constraint domain

Leontiev V.K.⁶⁰, Gordeev E.N.⁶¹

Abstract. *The knapsack problem is used in many mathematical models, including in the field of information security. Solving a problem (finding the optimal backpack load) or even answering the question about the existence of a valid solution is an NP-complete problem. In this regard, the question of finding the power of the set of acceptable solutions or estimates of this power is relevant. The paper analyzes the combinatorial aspects of this problem based on the method of generating functions. Formulas and estimates for the number of acceptable solutions and the average number of acceptable solutions depending on the coefficients of the constraint vector are obtained. On their basis, computational algorithms for finding these values can be constructed. All this can be used to assess the adequacy and quality of the original mathematical model.*

Keywords: *knapsack problem, feasible solutions, generating functions, estimates of the number of solutions, NP-completeness.*

⁶⁰ Leontiev Vladimir, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, vkleontiev@yandex.ru. RFBR grant 20-01-00645.

⁶¹ Gordeev Eduard, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, werhorn@gmail.com. RFBR grant 20-01-00645.

Анализ засекреченных сигналов телефонных шифраторов

Горшков Ю.Г.⁶²

Аннотация. Рассмотрены характеристики зарубежных телефонных шифраторов коммерческого применения. Приводится структура засекреченных сигналов линейных передач. Проведено сравнение частотно-временных характеристик сонограмм засекреченных сигналов, полученных с использованием преобразования Фурье и многоуровневого вейвлет-преобразования. Представлены возможности программных средств «Sound Edit» и «WaveView-MWA» при решении задач анализа сложных нестационарных сигналов. Впервые приводятся примеры построения вейвлет-сонограмм засекреченных сигналов с высоким частотно-временным разрешением.

Ключевые слова: телефонный шифратор, засекреченный сигнал, многоуровневый вейвлет-анализ, сонограмма.

Введение

Для защиты переговоров на каналах сети общего пользования (ТфОП) телефонные шифраторы за рубежом находят применение с 70-х годов прошлого столетия. К 1980 году разработкой, производством и сбытом «скремблеров» коммерческого применения в США, Англии и ряде стран Западной Европы задействованы десятки компаний. Отдельные компании, такие как Crypto AG [1] поставляли шифртехнику, в том числе телефонные шифраторы, более чем 100 странам мира.

Несмотря на то, что на каналах ТфОП все большее применение находят дискретные телефонные шифраторы, интерес к аналоговым системам засекречивания за рубежом достаточно высок [2]. Если дискретные шифраторы предназначены исключительно для засекречивания речевых сигналов, то аналоговые решения незаменимы при защите всего набора акустических биомедицинских сигналов в системах телемедицины [3]. В связи с этим исследования, направленные на изучение опыта построения «скремблеров» ведущими зарубежными компаниями, а также создания новых программных средств высокоточного анализа засекреченных аналоговых сигналов, следует отнести к актуальным.

1. Методы преобразования речевого сигнала. По зарубежной классификации аналоговая аппаратура (Scramblers) включает следующие виды засекречивающих преобразований [4]: 1. Frequency-Domain Scramblers (FDS) - частотные преобразования; 2. Time-Domain Scramblers (TDS) - преобразования во временной области; 3. Time-Frequency Scrambling (TFS) - частотно-временные преобразования; 4. Encryption by using Pseudo-Noise Sequences (ENS) - шифрование с использованием псевдошумовых последовательностей.

В отечественной литературе встречаются: частотные, временные и частотно-временные преобразования [5-7].

1.1. Частотные преобразования. Наибольшее применение находят: - частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и

⁶² Горшков Юрий Георгиевич, к.т.н., доцент, МГТУ им. Н.Э. Баумана, Москва, y.gorshkov@pro-echelon.ru

фильтра); - разбиение полосы частот речевого сигнала на несколько поддиапазонов, частотная инверсия спектра в каждом относительно средней частоты поддиапазона; - перестановка полос в частотной области.

На рис. 1 представлен внешний вид телефонного шифратора **ACS-2** (Research Electronics Inc. (REI), Algood (Tennessee, USA). На рис. 2 - **DV-505** Datotek, Dallas (Texas, USA).



Рис. 1. Шифратор **ACS-2**



Рис. 2. Шифратор **DV-505**

Основные характеристики. ACS-2. Преобразования – кольцевая динамическая инверсия; - время установления защищенного сеанса связи 2.5 сек; - частотный диапазон 300 – 2750 Гц; - количество ключей 13122.

DV-505. Пятиполосные частотно-временные преобразования; - частотный диапазон 200 – 3000 Гц; - общее число ключей 18.000.000, вырабатываемых «rolling code key generator» и «key generator», построенный на регистрах сдвига с нелинейной обратной связью (non-linear feedback shift registers, NLFSR).

Инженерно-криптографические решения, реализованные в шифраторе **DV-505** закреплены патентами: US 3.781.473 Random digital code generator; US 3.886.313, US 4.013.837, US 4.020.285 Voice security method and system [8].

1.2. Преобразования во временной области. Используются: - временные Шифраторы с временными перестановками в период 1974 -1980 годы и позднее в ряде стран Западной Европы находят широкое применение. К ним относятся Cryptophon 1100 (Brown Boveri and Company, BBC, Switzerland) и малогабаритная версия BBC Vericrypt 1100 [9]. Количество ключей 10.000.000. Генератор псевдослучайных чисел (pseudo-random number generator, PRNG), период 8.5 час. Синхронизация шифраторов обеспечивается пилот-сигналом с частотой 1830 Гц $\pm$ 100 Гц.

1.3. Частотно-временные преобразования. Наиболее распространенное семейство шифраторов с частотно-временными преобразованиями CRM-008, HC-230/HC-235 (рис. 3) Crypto AG (Hagelin, Switzerland) [10]. Мощность ключевой системы: 10 в 32-й степени.

На рис. 4, 5 и 6 представлены структура засекреченного сигнала, блок-схема шифратора и преобразования речевого сигнала в частотно-временной области.



Рис. 3. Шифратор **HC-230/HC-235**

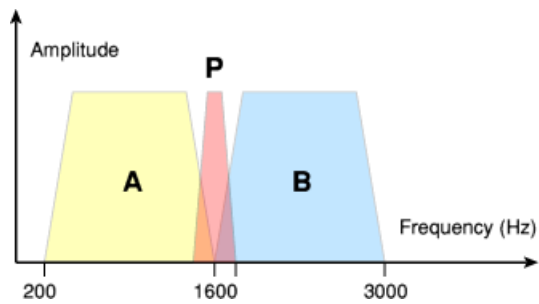


Рис. 4. Структура засекреченного сигнала

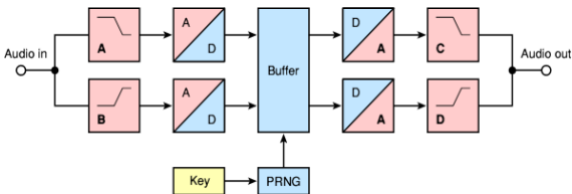


Рис. 5. Блок-схема шифратора

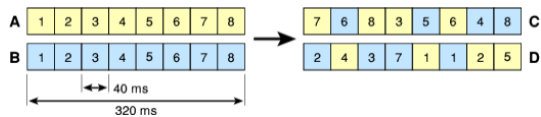


Рис. 6. Преобразования сигнала

2. Анализ засекреченных сигналов. На примере демонстрационных записей телефонного шифратора **Cryptophon 1100** оценим возможности частотно-временного разрешения полученных сонограмм (изображений «видимый звук») с использованием распространенного звукового редактора на основе преобразования Фурье и разработанных на кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана программных средств многоуровневого вейвлет-анализа нестационарных сигналов «WaveView-MWA».

2.1. Анализ на основе преобразования Фурье. Для получения сонограмм использовалась программа звукового редактора «Sound Edit» («Эталон», Россия). На рис. 7 и 8 представлены Фурье-сонограммы открытого и засекреченного речевого сигнала.

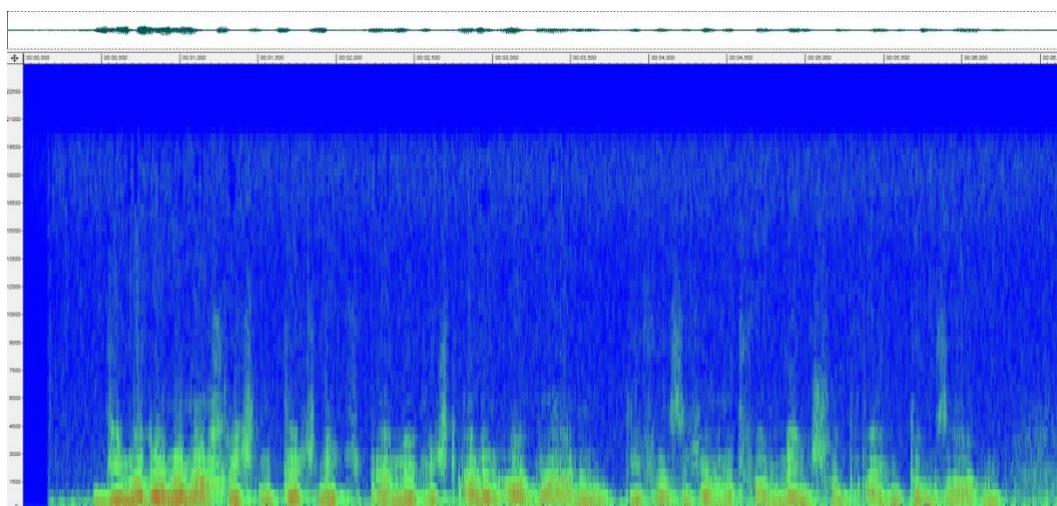


Рис. 7. Фурье-сонограмма открытого речевого сигнала

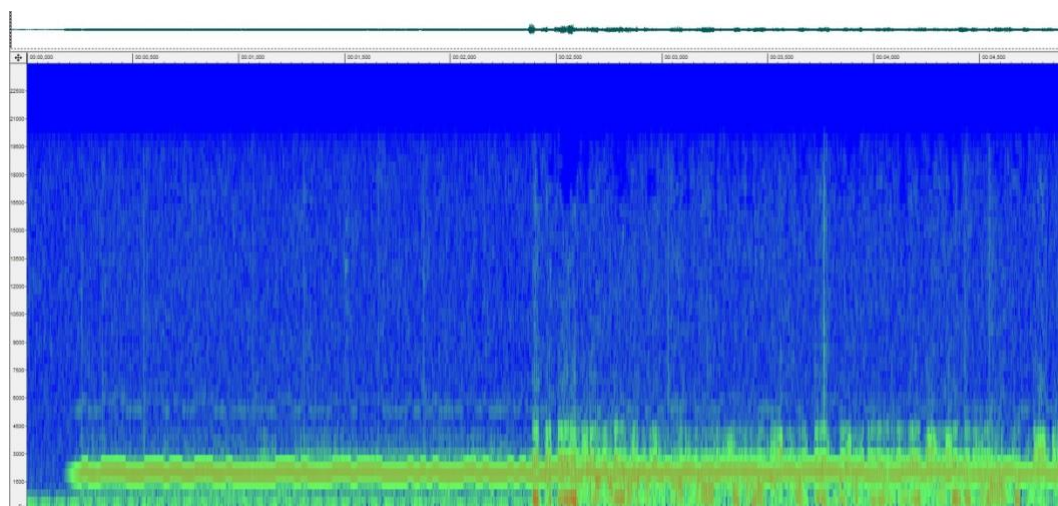


Рис. 8. Фурье-сонограмма засекреченного речевого сигнала

Звуковой редактор «Sound Edit» обеспечивает предварительную обработку и анализ звуковых файлов с использованием преобразования Фурье: построение сонограмм; амплитудное и спектральное отображение звуковых данных; редактирование (удаление фрагмента аудиозаписи, вставка нового фрагмента); амплитудные преобразования (эквалайзер «амплитуда-время»); частотные

преобразования (частотный эквалайзер); анализ спектра сигнала. В режиме частотных преобразований (частотный эквалайзер) графически задается амплитудно-частотная характеристика фильтра (АЧХ). Кроме этого, вводятся максимум и минимум АЧХ. Блок быстрого преобразования Фурье (БПФ): 128, 512, 1024, 2048, 4096, 8192, 16384; «временное окно»: «прямоугольное», Хэмминга, Хеннинга, Бартлетта, Блэкмана.

Из анализа сонограммы рис. 8 следует, что частотно-временное разрешение анализируемого сигнала на основе преобразования Фурье достаточно низкое и не позволяет решать задачи первичного инженерно-криптографического анализа засекреченных сигналов. Разрешение Фурье-сонограммы открытого речевого сигнала (рис. 7) также следует считать неудовлетворительным. Несмотря на то, что недостатки и связанные с ними ограничения при Фурье-анализе нестационарных сигналов рассмотрены еще в 2006 году [11], практически все современные программные средства анализа при получении спектральных характеристик речи используют БПФ.

2.2. Анализ с использованием многоуровневого вейвлет-преобразования

Разработанные программные средства многоуровневого вейвлет-анализа нестационарных сигналов «WaveView-MWA» находят широкое применение при обработке акустических биомедицинских сигналов и создании защищенных систем телемедицины [12-18].

На рис. 9 и 10 представлены вейвлет-сонограммы открытого и засекреченного речевого сигнала, полученные с использованием «WaveView-MWA».

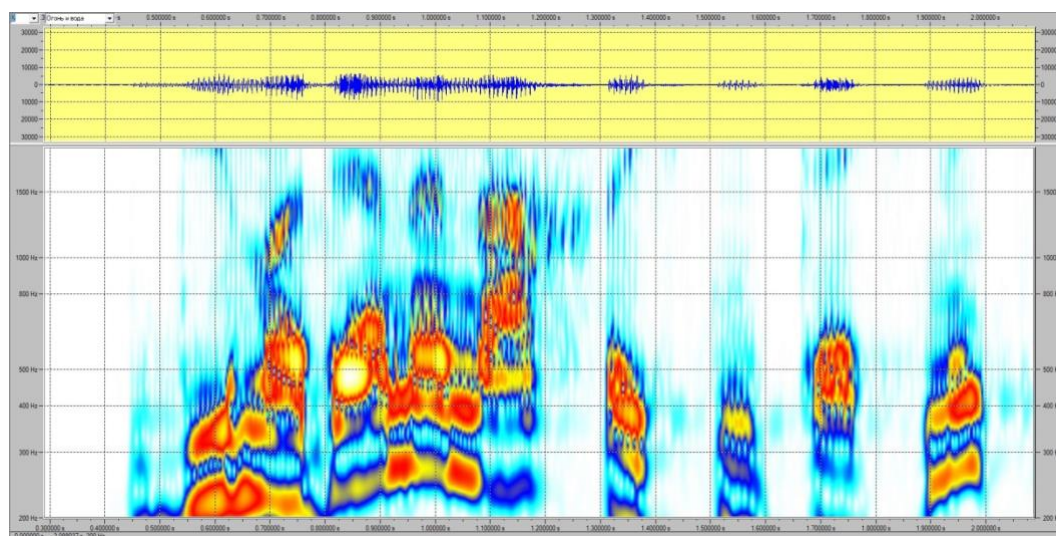


Рис. 9. Вейвлет-сонограмма открытого речевого сигнала

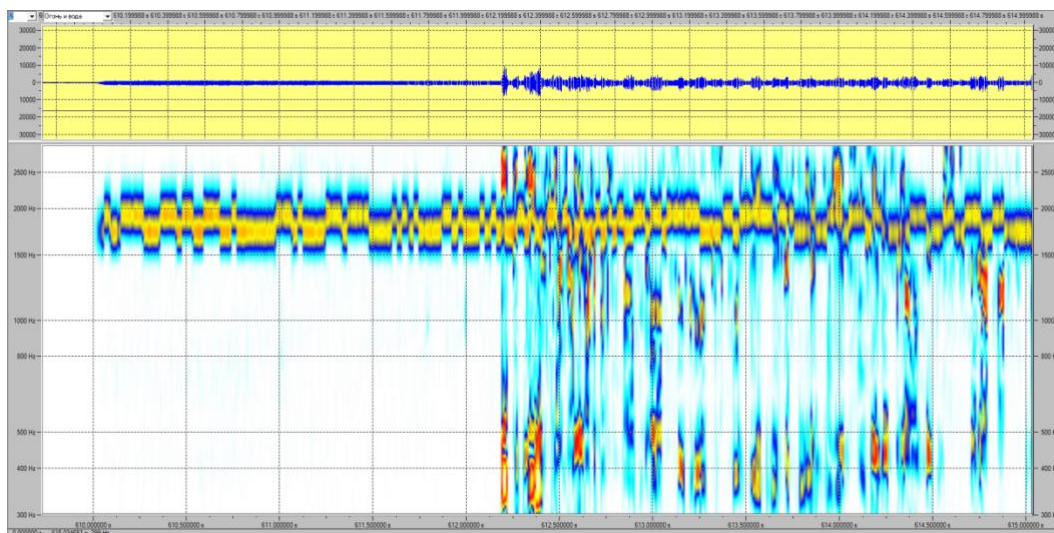


Рис. 10. Вейвлет-сонограмма засекреченного речевого сигнала

Частотно-временное разрешение анализируемого засекреченного сигнала (рис. 10) на основе многоуровневого вейвлет-анализа позволяет определять параметры линейной передачи: вид преобразования (частотные, временные, частотно-временные); длительность временного сегмента; значения частот сигнала синхронизации и т.д. Вейвлет-сонограмма открытого речевого сигнала (рис. 9) обеспечивает получение формантной структуры гласных, а также характеристик согласных звуков. Достигнутое высокое частотно-временное разрешение позволяет выделять биомаркеры уровня эмоциональной напряженности диктора.

Выводы

Программные средства «WaveView-MWA» с использованием технологии цифровой обработки нестационарных сигналов нового поколения –многоуровневого вейвлет-анализа позволяют решать задачи первичного инженерно-криптографического анализа засекреченных передач телефонных шифраторов. Полученные вейвлет-сонограммы на примере демонстрационной записи телефонного шифратора **Cryptophon 1100** могут служить основой для наглядной визуализации засекреченных сигналов при освоении студентами курса «Специальные технические средства и криптографические методы защиты нетекстовой информации».

«WaveView-MWA» в составе разработок МГТУ им. Н.Э. Баумана «АКУСТОКАРД», «АКУСТОМЕД-С», «ЭКСПЕРТ МВА», «СТРЕСС МВА» успешно демонстрировались на мероприятиях:

1. XVII Международная выставка по электронике, компонентам, оборудованию и технологиям «ChirEXPO-2019». 16-18 октября, Экспоцентр, Москва.
2. XXIII Международная выставка «INTERPOLITEX-2019»: Безопасность, определяющая будущее. 22-25 октября, ВДНХ, Москва.
3. Международный военно-технический форум «Армия-2020». 23-29 августа, Кубинка, Московская область

Литература

1. Бутырский Л.С., Ларин Д.А. Борис Хагелин - отец коммерческой криптографии. BIS Journal, №3(6), 2012.

2. K. Riedhammer, M. Ring, E. Nöth and D. Kolb. A software kit for automatic voice descrambling. 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 2012, pp. 6764-6768. Doi: 10.1109/ICC.2012.6364883.
3. Горшков Ю.Г. Обработка речевых и акустических биомедицинских сигналов на основе вейвлетов / Научное издание. М.: Радиотехника. 2017. 240 с.
4. Н.Н. Kohad, V.R. Ingle, M.A. Gaikwad. An Overview of Speech Encryption Techniques. International Journal of Engineering Research and Development. e-ISSN: 2278-067X, p-ISSN: 2278-800X, Vol 3, Issue 4, August 2012, pp. 29-32.
5. Горшков Ю.Г. Анализ и засекречивание речевого сигнала: Учебное пособие. М.: Издательство МГТУ им. Н.Э. Баумана. 2007. 36 с.
6. Корниенко В.Т., Шостак А.А. Аналоговые скремблеры речевых сигналов. Руководство к лабораторно-практическим занятиям. «Безопасность жизнедеятельности», ч. 2 «Информационная безопасность». Таганрог: Издательство ТТИ ЮФУ, 2011. 48 с.
7. Голиков А.М. Исследование методов аналогового скремблирования: Учебно-методическое пособие по лабораторной работе [Электронный ресурс] / А.М. Голиков. Томск: ТУСУР, 2019. 25 с.
8. <https://www.cryptomuseum.com/crypto/datotek/dv505/>
9. <https://www.cryptomuseum.com/crypto/bbc/cryptophon/>
10. <https://www.cryptomuseum.com/crypto/hagelin/crm008/>
11. Горшков Ю.Г. Новые решения речевых технологий безопасности // Специальная техника. 2006. № 4. С. 41-47.
12. Горшков Ю.Г. Методы и средства многоуровневого вейвлет-анализа и засекречивания речи // Спецтехника и связь № 2, 2015. С. 42-50.
13. Горшков Ю.Г. Тестирование средств засекречивания речи // Вопросы кибербезопасности № 2 (10), 2015. С. 26-30.
14. Горшков Ю.Г., Кузин А.Ю., Цирлов В.Л. Засекречивание речевой информации на основе вейвлетов // Вестник МГТУ им. Н.Э. Баумана. Серия: Приборостроение S-2, 2011, С. 138-145.
15. Горшков Ю.Г., Каиндин А.М., Веряев А.С., Зорин Е.Л., Марков А.С., Цирлов В.Л. Система телемедицины с предварительным шифрованием биометрической информации // Вопросы кибербезопасности. № 5 (13), 2015. С. 63-69.
16. Горшков Ю.Г., Калинин А.Л., Каиндин А.М., Марков А.С., Цирлов В.Л. Защищенная система телемедицины дистанционного выявления ранних стадий заболеваний сердца. Патент на полезную модель RUS 127605. 18.12.2012; Заявка № 2012154801; опубл. 10.05.2013. Бюл. № 13.
17. Горшков Ю.Г. Засекречивание речи на каналах связи стандарта GSM // Вопросы кибербезопасности. 2013. №1(1). С.55-60.
18. Горшков Ю.Г., Марков А.С., Цирлов В.Л. Новые технологии анализа и засекречивания речевых сигналов // В сборнике: Безопасные информационные технологии (БИТ-2016) Сборник трудов Седьмой Всероссийской научно-технической конференции. Под редакцией В.А. Матвеева. 2016. С. 135-138.

Analysis of classified signals of telephone scramblers

Y.G. Gorshkov⁶³

Abstract. *The characteristics of foreign telephone scramblers for commercial use are considered. The structure of classified signals of linear transmissions is given. A comparison is made of the time-frequency characteristics of the sonograms of classified signals obtained using the Fourier transform and the multilevel wavelet transform. The possibilities of the software «Sound Edit» and «WaveView-MWA» in solving problems of analysis of complex non-stationary signals are presented. For the first time, examples of constructing wavelet sonograms of classified signals with a high frequency-time resolution are given.*

Keywords: *telephone scrambler, secret signal, multilevel wavelet analysis, sonogram.*

⁶³ Yuri Gorshkov, Ph.D., Bauman MSTU, Moscow, y.gorshkov@npo-echelon.ru

Постквантовый криптографический протокол выработки общего ключа, основанный на изогениях суперсингулярных эллиптических кривых

Гребнев С.В.⁶⁴, Ключарёв П.Г.⁶⁵, Коренева А.М.⁶⁶, Кошелев Д.И.⁶⁷,
Тараскин О.Г.⁶⁸, Тулебаев А.И.⁶⁹

Аннотация. В докладе описывается проект постквантового протокола выработки общего ключа «Форзиция», разработанного в рамках деятельности рабочей подгруппы по изогениям суперсингулярных эллиптических кривых Рабочей группы 2.5 «Постквантовые криптографические механизмы» технического комитета «Криптографическая защита информации» (ТК26). Приводятся необходимые математические определения, описание предлагаемого протокола и его параметров, упоминаются основные атаки на протокол. Протокол основан на изогениях суперсингулярных эллиптических кривых и использует схему SIDH. Он предоставляет три уровня квантовой стойкости – 80, 128 и 256 битов.

Ключевые слова: постквантовый криптографический протокол, изогении, выработка общего ключа.

Введение

Практические квантовые компьютеры, в случае их появления, сделают нестойкими традиционные протоколы выработки общего ключа типа Диффи-Хеллмана, основанные на вычислительной сложности задачи дискретного логарифмирования, поскольку, как известно, эта задача решается с помощью квантового алгоритма Шора за полиномиальное время. В связи с этим необходимы новые протоколы выработки общего ключа, для взлома которых неизвестно эффективных квантовых алгоритмов. Данная работа посвящена предлагаемому в рамках процесса стандартизации постквантовых криптографических алгоритмов в Российской Федерации протоколу выработки общего ключа «Форзиция», построенному на основе механизма изогений суперсингулярных эллиптических кривых.

Предлагаемый протокол использует схему SIDH, предоставляет три уровня квантовой стойкости – 80, 128 и 256 битов. Он использует стартовую эллиптическую кривую специального вида E_{19} , представление эллиптических кривых в форме Монтгомери. Кроме того, в нем не используется компрессия открытых ключей (в целях увеличения быстродействия).

Изогении и криптография

Изогения [1,2] – это рациональное отображение между двумя эллиптическими кривыми, являющееся гомоморфизмом. Если существует такого рода отображение между двумя эллиптическими кривыми, то они называются *изогенными*. *Графом изогений* называется граф, множеством вершин которого является множество классов изоморфизма эллиптических кривых. Две различных вершины этого графа соединены ребром тогда и только тогда, когда представители соответствующих классов изоморфизма изогенны. Если ограничиться только изогениями степени l , то получим

⁶⁴ Гребнев Сергей Владимирович, QApp, Москва, grebnev_sv@tc26.ru

⁶⁵ Ключарёв Петр Георгиевич, к.т.н., МГТУ им. Н.Э. Баумана, Москва, pk.iu8@yandex.ru

⁶⁶ Коренева Алиса Михайловна, к.ф.-м.н., Код безопасности, Москва, A.Koreneva@securitycode.ru

⁶⁷ Кошелев Дмитрий Игоревич, к.т.н., ИнфоТеКС, Москва, dishport@ya.ru

⁶⁸ Тараскин Олег Геннадьевич, Waves Enterprise, Москва, tog.postquant@gmail.com

⁶⁹ Тулебаев Азат Ирикович, Код безопасности, Москва, azatkabcs@yandex.ru

граф l -изогений. Для построения l -изогений используются так называемые формулы Велю [3].

При рассмотрении суперсингулярных эллиптических кривых над полем $GF(p^2)$ оказывается, что граф l -изогений обладает рядом свойств, позволяющих строить криптографические схемы, в основе стойкости которых лежит задача поиска пути между двумя вершинами в этом графе. Это свойство использовалось в ряде работ, в том числе в работе [4] и в работе [5], где впервые удалось предложить стойкий и практически эффективный протокол выработки общего ключа SIDH. Указанный протокол лег в основу предлагаемого нами протокола «Форзизия».

Описание протокола

Фиксируем открытые параметры протокола:

- простое число p вида $p = l_A^{e_A} l_B^{e_B} \cdot f - 1$, где l_A, l_B – маленькие простые (например, 2 и 3), $(l_A, f) = (l_B, f) = 1$;
- стартовая кривая – суперсингулярная эллиптическая кривая $E_0(GF(p^2))$, мощность группы точек которой равна $(l_A^{e_A} l_B^{e_B} \cdot f)^2$. $E[l_A^{e_A}]$ содержит $l_A^{e_A-1}(l_A + 1)$ циклических подгрупп порядка $l_A^{e_A}$, каждая из которых определяет собственную изогению (т.е. ядром которой она является), аналогичное замечание верно и для $E[l_B^{e_B}]$.
- базисы $\{P_A, Q_A\}$ и $\{P_B, Q_B\}$, которые порождают, соответственно, $E_0[l_A^{e_A}]$ и $E_0[l_B^{e_B}]$, т.е. $\langle P_A, Q_A \rangle = E_0[l_A^{e_A}]$ и $\langle P_B, Q_B \rangle = E_0[l_B^{e_B}]$.

Протокол состоит в следующем:

Абонент A выбирает случайный элемент $n_A \in_R \mathbb{Z} / l_A^{e_A} \mathbb{Z}$ и строит изогению $\varphi_A: E_0 \rightarrow E_A$ с ядром $K_A := \langle P_A + [n_A]Q_A \rangle$. Абонент A также вычисляет образ $\{\varphi_A(P_B), \varphi_A(Q_B)\}$ и посылает эти точки абоненту B вместе с эллиптической кривой E_A (т.е. ее описанием).

Аналогично, абонент B выбирает случайный элемент $n_B \in_R \mathbb{Z} / l_B^{e_B} \mathbb{Z}$ и строит изогению $\varphi_B: E_0 \rightarrow E_B$ с ядром $K_B := \langle P_B + [n_B]Q_B \rangle$. Абонент B также вычисляет образ $\{\varphi_B(P_A), \varphi_B(Q_A)\}$ и посылает эти точки абоненту A вместе с эллиптической кривой E_B (т.е. ее описанием).

Получив от абонента B набор $E_B, \varphi_B(P_A), \varphi_B(Q_A)$, абонент A строит изогению $\varphi'_A: E_B \rightarrow E_{AB}$ с ядром $\langle \varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$; абонент B выполняет аналогичные действия.

В качестве общего секретного ключа используется j -инвариант эллиптической кривой:

$$E_{AB} = \varphi'_B(\varphi_A(E_0)) = \varphi'_A(\varphi_B(E_0)) = E_0 / \langle P_A + [n_A]Q_A, P_B + [n_B]Q_B \rangle.$$

Оценки стойкости и выбор параметров

Формальный анализ протокола в модели Канетти-Кравчика проведен в [5]. Анализ практической стойкости протокола включает в себя рассмотрение как ряда классических атак, в том числе метода тотального перебора, метода встречи посередине, параллельного метода поиска коллизий (метода Винера–ван Ооршота [6]), так и ряда

квантовых атак, в том числе квантового алгоритма поиска зацеплений (claw-finding) [7] и квантового алгоритма Гровера. Исходя из результатов работы [8] было принято, что в реалистичной модели квантового вычислителя (с ограниченным объемом квантовой памяти, не превосходящим 2^{64} ячеек), среди квантовых атак, наиболее эффективной является атака, основанная на алгоритме Гровера.

В качестве стартовой эллиптической кривой протокола мы предлагаем использовать кривую E_{19} :

$$E_{19} : y^2 = x^3 - 2^3 \cdot 19x + 2 \cdot 19^2$$

с j -инвариантом $-2^{15}3^3$. Ее выбор обоснован в [9]. В частности, E_{19} не обладает эндоморфизмами степени 2 и 3, то есть петлями в графах 2- и 3-изогений. Также у нее отсутствуют кратные дуги в графах 2- и 3-изогений, в отличие от эллиптических кривых, использованных в SIKE [10].

Простое число p выбирается в виде $p = 2^{e_2} 3^{e_3} f - 1$, так что множители 2, 3 сбалансированы: $e_2 \approx e_3 \cdot \log_2 3$, а множитель f – малое простое число. При этом требуется, чтобы $\left(\frac{-19}{p}\right) = -1$. Опираясь на результаты анализа, предлагаются наборы параметров, приведенные в таблице 1.

Таблица 1.

Число	Формула	Наборы параметров	
		Классическая стойкость	Квантовая стойкость
p_{317}	$2^{132} \cdot 3^{85} \cdot 11 - 1$	82	131
p_{508}	$2^{208} \cdot 3^{129} \cdot 5 - 1$	135	203
p_{1023}	$2^{372} \cdot 3^{239} \cdot 7 - 1$	262	372

Заключение

Таким образом, на настоящий момент получены следующие результаты:

- Предложен постквантовый протокол выработки общего ключа двумя абонентами, основанный на протоколе SIDH;
- Выбраны параметры протокола, в том числе, стартовая кривая, характеристики поля и т.д.
- Разработан прототип программной реализации на языке Python с использованием библиотеки SAGE.

Разработанный протокол может найти широкое применение в задачах информационной безопасности.

Литература

1. Silverman J.H. The Arithmetic of Elliptic Curves. – Springer, 2009.
2. Washington L.C. Elliptic curves, number theory and cryptography. – CRC, 2008.
3. Velú J. Isogénies entre courbes elliptiques, C.R. Acad. Sc. Paris. 1971. Serie A., 273, P. 238–241.
4. Rostovtsev A., Stolbunov A. Public-Key Cryptosystem Based on Isogenies //IACR Cryptol. ePrint Arch. – 2006. URL: <https://ia.cr/2006/145>
5. De Feo L., Jao D., Plût J. Towards quantum resistant cryptosystems from supersingular elliptic curve isogenies. // Journal of Math. Cryptology, 2014. Vol. 8(3). P. 209–247.
6. Van Oorschot P. C., Wiener M. J. Parallel collision search with cryptanalytic applications //Journal of Cryptology. – 1999. – Т. 12. – №. 1. – P. 1-28.

7. Tani S. Claw finding algorithms using quantum walk //Theoretical Computer Science. – 2009. – Т. 410. – №. 50. – С. 5285-5297.
8. Jaques S., Schanck J.M. Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE // Cryptology ePrint Archive: Report 2019/103. – 2019. URL: <https://eprint.iacr.org/2019/103>.
9. Кошелев Д. Стартовая суперсингулярная эллиптическая кривая для криптографии на изогениях. 2020. Режим доступа: https://www.researchgate.net/publication/343386142_Startovaa_supersingularnaa_ellipticeskaa_krivaa_dla_kriptografii_na_izogeniah
10. Jao D. et al. Supersingular Isogeny Key Encapsulation. – 2017. URL: <https://sike.org>

A post-quantum key exchange cryptographic protocol based on isogenies of supersingular elliptic curves

Grebnev S.V.⁷⁰, Klyucharev P.G.⁷¹, Koreneva A.M.⁷², Koshelev D.I.⁷³,
Taraskin O.G.⁷⁴, Tulebaev A.I.⁷⁵

Abstract. The report describes the draft post-quantum cryptographic protocol "Forsythia" for generating a common key, developed within the framework of the working subgroup on isogeny of supersingular elliptic curves of Working Group 2.5 "Post-quantum cryptographic mechanisms" of the Technical Committee "Cryptography and Security Mechanisms" (TC26). The necessary mathematical definitions, a description of the proposed protocol and its parameters are given, and the main attacks on the protocol are mentioned. The protocol is based on isogenies of supersingular elliptic curves and uses the SIDH scheme. It provides three levels of quantum security – 80, 128, and 256 bits.

Keywords: post-quantum cryptography, key exchange, isogeny.

⁷⁰ Sergey Grebnev, QApp, Moscow, grebnev_sv@tc26.ru

⁷¹ Petr Klyucharev, Ph.D., Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

⁷² Alisa Koreneva, Ph.D., Security Code, Moscow, A.Koreneva@securitycode.ru

⁷³ Dmitrii Koshelev, Ph.D., Infotecs, Moscow, dishport@ya.ru

⁷⁴ Oleg Taraskin, Waves Enterprise, Moscow, tog.postquant@gmail.com

⁷⁵ Azat Tulebaev, Security Code, Moscow, azatkabcs@yandex.ru

Усовершенствование метода обработки граничных точек в задачах анализа изображений

Дамдинова Т.Ц.⁷⁶

Аннотация. В настоящее время создание цифровых видео и изображений происходит с очень высокой скоростью. Вычислительная мощность современных компьютеров, разработка новых способов автоматизации процесса анализа данных и скорость извлечения полезной информации из этих цифровых данных очень важны. Обзор литературы последних лет показывает, что методы и средства получения и обработки цифровых данных продолжают развиваться. В статье рассматривается задача обработки изображений при анализе видеоданных. Предложен способ формирования граничных точек с заданной погрешностью для выделения объектов с разным уровнем детализации, что влияет на скорость анализа данных.

Ключевые слова: защита информации, обработка цифровых изображений, выделение линий, распознавание образов.

Введение

Для организации мер технической защиты от несанкционированного доступа к информации одним из ключевых источников информации являются данные видеопотока, которые могут использоваться для выявления фактов нарушения безопасности. Успешное предотвращение несанкционированного доступа зависит от своевременного анализа данных, уровня автоматизации обработки видеоданных в режиме реального времени. Данной теме посвящено много научных работ последних лет, направленных на улучшение качества получения, анализа и распознавания видеoinформации. Выявление данных зависит от скорости обработки и представления данных, которые в основном опираются на данные о форме интересующих объектов.

Обработка изображений в области информационной безопасности.

К мерам технической безопасности относятся установка видеокамер. Обработка данных, получаемых с камер слежения, для поиска и распознавания объектов остается актуальной темой, которой посвящено много работ последнего периода [1-3]. Автоматизация данной задачи позволяет своевременно извлечь интересующие информацию о подозрительных объектах, их действиях и аномальном поведении.

Кроме обычных видеокамер используются данные камер беспилотных летательных аппаратов, 3D сканеров, рентгеновские сканеры, более безопасные для здоровья человека камеры контроля безопасности терагерцевого диапазона, тепловизоры и т.д. [4-7]. Во всех этих видеосистемах наряду с режимом ручного поиска и обнаружения опасных объектов используется автоматизированная обработка данных в режиме реального времени. Наиболее эффективными методами автоматизации обнаружения и распознавания является использование искусственного интеллекта с нейронной сетью [8,9].

Распознавание объектов при автоматизации анализа видеоданных базируются на анализе контуров, имеется большое количество методов выделения граничных точек объектов [10-13]. При этом необходимо учитывать влияние помех при формировании изображения [14] и на этапе предварительной обработки необходимо удалять возникшие аппаратные шумы и абберрации [8,14,15]. Благодаря современному развитию вычислительной мощности компьютеров, разработанные методы показывают высокую

⁷⁶Дамдинова Татьяна Цыбиковна, к.т.н., доцент, Восточно-Сибирский государственный университет технологий и управления, г.Улан-Удэ, dtatyanac@mail.ru

точность и надежность, полученные данные могут использоваться при создании интеллектуальных систем.

Для качественного выполнения задачи обнаружения объектов одним из ключевых факторов является определение таких характеристик объекта как форма, текстура, описание контура и другие геометрические характеристики объекта [16-19]. Особенно важно автоматизировать процесс получения точного контура. Для этого можно варьировать значение допустимой погрешности для извлечения границ при получении данных по объекту. Изменение значения погрешности контура на разных этапах позволит ускорять процесс поиска и анализа изображения. При обнаружении подозрительного объекта значение погрешности уменьшается для более детального и точного извлечения информации.

Выводы

С развитием информационных технологий методы и способы обработки цифровой информации находят широкое применение в области информационной безопасности. Наиболее информативной частью объекта является его форма. Для определения формы объекта необходима информация о контуре объекта. Точки контура объекта можно формировать с допустимой погрешностью. Изменяя значение погрешности, можно получать информацию об объекте разного уровня детализации.

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. Козлов В.А., Потапов А.С. Анализ методов выделения движущихся объектов на видеопоследовательностях с шумами // Научно-технический вестник информационных технологий, механики и оптики, №. 3 (73), 2011, с. 39-43.
3. Макаров М.А., Берестнева О.Г., Андреев С.Ю. Решение задачи описания и классификации контуров движущихся объектов на видео. // Известия Томского политехнического университета. Информационные технологии. 2014. Т. 325. №5... С. 77–83
4. Taiyang Hu, Zelong Xiao, Jianzhong Xu, Li Wu. Methods of Personnel Screening for Concealed Contraband Detection by Millimeter-wave Radiometric Imaging. *Procedia Engineering* 7 (2010) 28–37
5. Meng-Han Hu, Guang-Tao Zhai, Duo Li, Ye-Zhao Fan, Xiao-Hui Chen, Xiao-Kang Yang. Synergetic use of thermal and visible imaging techniques for contactless and unobtrusive breathing measurement // *J. of Biomedical Optics*, 22(3), 036006 (2017)
6. V. Engert A. Merla J. A. Grant D. Cardone A. Tusche and T. Singer. Exploring the use of thermal infrared imaging in human stress research. // *PLoS ONE* vol. 9 no. 3 pp. e90782 (2014).
7. MinWan, John J.Healy, John T.Sheridan. Terahertz phase imaging and biomedical applications. // *Optics & Laser Technology*, ISSN: 0030-3992, Vol: 122, Page: 105859
8. Z.Tong, J.Zhou. Face alignment using two-stage cascaded pose regression and mirror error correction. // *Pattern Recognition*, Volume 115, July 2021, 107866.
9. Д.В. Машанов. Реализация быстрого способа идентификации человека на основе детектора Кэнни с использованием нейронной сети. // *Электронные средства и системы управления. XIV Международная научно-практическая конференция*, 28–30 ноября 2018 г. с.83-86.
10. Гонсалес Р., Вудс Р., Цифровая обработка изображений. — М.: Техносфера, 2005, 2006. — 1072 с.
11. Сакович И.О., Белов Ю.С. Обзор основных методов контурного анализа для выделения контуров движущихся объектов. *Инженерный журнал: наука и инновации*, 2014, вып. 12.
12. Новиков А.И., Саблина В.А., Горячев Е.О. Применение контурного анализа для совмещения изображений. *Известия ТулГУ. Технические науки*. 2013. Вып. 9. Ч.1. – с.260-269
13. Цапко И.В., Власов А.В. Выделение объектов на изображениях методом поиска границ регионов // *Автоматизация. Современные технологии*. – 2015. № 9. С. 33-38

14. Дамдинова Т.Ц. Способы формирования цифровых изображений и анализ их погрешностей. // Вопросы кибербезопасности.- 2014. - №5. - с.43-46. - ISSN 2311-3456
15. P.Smith, V.Kurlin, Skeletonisation algorithms with theoretical guarantees for unorganised point clouds with high levels of noise. // Pattern Recognition. Volume 115, July 2021, 107902
16. Дамдинова Т.Ц., Бубеев ИТ., Мотошкин ПВ. Метод моделирования кривой первого порядка гладкости. // Программные системы и вычислительные методы. - 2019.- вып.17. с.12-17
17. Damdinova Tatyana, Bazaron Seseg, Abatnin Alexander. Image Processing in Information Security // CEUR Workshop Proceedings, 2020, Vol-2603. pp. 16-19.
18. Дамдинова Т.Ц., Базарон С.А., Абатнин А.А. Обработка изображений в информационной безопасности. / В сборнике Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019. с.121-123
19. S A Bazaron, T Ts Damdinova and E B Bochektueva. Determination of the geometric characteristics of fatigue cracks by digital image processing method. //IOP Conf. Series: Materials Science and Engineering 684 (2019) 012022.

Annotation

Nowadays, digital video and image creation are obtained with very high speed. The computing power of modern computers, the development of new methods to automate the data analysis process and the speed of extracting useful information from this digital data are very important. A review of the literature of recent years shows that the methods and means of obtaining and processing digital data continue to develop. The article deals with the problem of image processing for analyzing video data. A method for the formation of boundary points with a given tolerance to select objects with different levels of detail, which affects the speed of data analysis is proposed.

Keywords: *information security, digital image processing, edge detection, pattern recognition.*

⁷⁷ Damdinova Tatiana, Ph.D., Associate Professor, East-Siberia State University of Technology and Management, Ulan-Ude, dtatyanac@mail.ru

Клеточные автоматы и запреты булевых функций Жуков А.Е.⁷⁸

Аннотация. В работе показано, что обратимость одномерного клеточного автомата (КЛА) связана со свойствами конструкции, называемой нелинейный фильтр с входной памятью (НФВП). При этом НФВП не зависит от числа ячеек памяти КЛА, а зависит только от его локальной функции связи. Полученные результаты позволяют снизить сложность решения массовых задач переборного типа, связанных с вопросами обратимости КЛА. Все полученные результаты можно перенести на КЛА с небинарным заполнением ячеек и на КЛА размерности большей 1.

Ключевые слова: обратимость клеточного автомата, нелинейный фильтр с входной памятью, автомат с запретами, автомат без запретов, автомат с потерей информации, автомат без потери информации, граф запретов.

Введение

Клеточные автоматы (КЛА) как вычислительные структуры известны уже более 70 лет [1]. На первый взгляд тема «клеточные автоматы» вроде бы не относится к направлению «информационная безопасность», но в последнее время клеточные автоматы (в особенности обратимые) активно применяются в качестве криптографических примитивов [2]. Вообще вопросы обратимости КЛА исследованы достаточно подробно, но, как это не парадоксально, исследования в основном касались КЛА на бесконечных решетках. В криптографии же, как и в большинстве приложений, используются КЛА на решетках конечного размера. Вопросы обратимости для таких КЛА в принципе всегда разрешимы, и основная задача состоит в нахождении приемлемых критериев для проверки обратимости, алгоритмов для реализации обратного преобразования и оценки сложности этих алгоритмов. И здесь результатов существенно меньше.

В настоящей работе устанавливается связь обратимости однородных одномерных бинарных клеточных автоматов с автоматами без потери информации и запретами булевых функций. Эта связь позволяет решать вопрос обратимости КЛА с большей эффективностью. Полученные результаты легко переносятся на КЛА с небинарным множеством состояний ячеек памяти, а также на КЛА с решеткой размерности больше 1.

Конкретный тип автоматов, рассматриваемых в данной работе

Объектом изучения в настоящей работе является однородный одномерный бинарный клеточный автомат.

Однородный одномерный (1D) бинарный клеточный автомат (КЛА) длины L с локальной функцией связи f определяется следующим образом:

Пусть имеется линейно упорядоченный (1D) массив из L двоичных ячеек памяти (клеток). Время для клеточного автомата изменяется дискретными шагами (тактами). Пусть $m_i(t)$ – булева величина, являющаяся заполнением i -й ячейки памяти в момент времени t . Внутренним состоянием (или **конфигурацией**) КЛА в момент времени t

⁷⁸ Жуков Алексей Евгеньевич, кандидат физико-математических наук, директор ассоциации «РусКрипто», доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, aez_iu8@rambler.ru

называется заполнение всего массива ячеек: $(m_1(t), m_2(t), \dots, m_L(t))$. Число различных конфигураций 1D бинарного КЛА длины L равно 2^L .

Изменение заполнений ячеек происходит синхронно и одновременно при увеличении номера такта в соответствии с правилами перехода, определяющими новое заполнение каждой ячейки памяти как функцию от текущих заполнений соседних ячеек, т.е. ячеек, входящих в ее окрестность.

В рассматриваемом ниже примере окрестностью i -й ячейки будем называть ячейки с номерами $i - 1, i, i + 1$.

Тогда заполнение i -й ячейки в момент времени t определяется формулой

$$m_i(t) = f(m_{i-1}(t-1), m_i(t-1), m_{i+1}(t-1)).$$

Функция $f(z_1, z_2, z_3)$ называется **локальной функцией связи**.

Задача нахождения прообраза заданной конфигурации 1D КЛА

Пусть $(x_1, x_2, \dots, x_L)$ – конфигурация 1D КЛА в момент времени t , а $(y_1, y_2, \dots, y_L)$ – конфигурация КЛА в следующий момент времени (рис. 1).

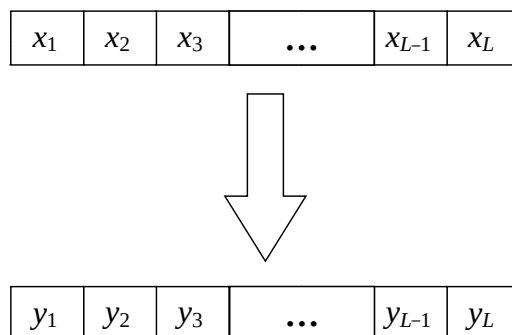


Рис. 1

Поскольку решетка нашего клеточного автомата имеет конечные размеры, возникает так называемая «проблема краевых клеток» – как задавать значения аргументов локальной функции связи для ячеек, у которых отсутствует часть соседей. Для этого вводятся граничные условия:

- Чаще всего в соответствии со свойством однородности для разрешения проблемы краевых клеток противоположные края решетки клеточного автомата отождествляются – это так называемая **периодическая граница** (PB – periodic boundary).
- Другой тип граничных условий – **нулевая граница** (NB – null boundary): значения для отсутствующих соседей полагаются равными нулю.
- Еще один тип граничных условий – **отражающая граница** (RB – reflective boundary).

Таким образом, для вычисления следующей конфигурации КЛА помимо текущего заполнения L ячеек $(x_1, x_2, \dots, x_L)$ требуется знать значения в виртуальных ячейках (в нашем случае это x_0 и x_{L+1} – см. рис. 2).

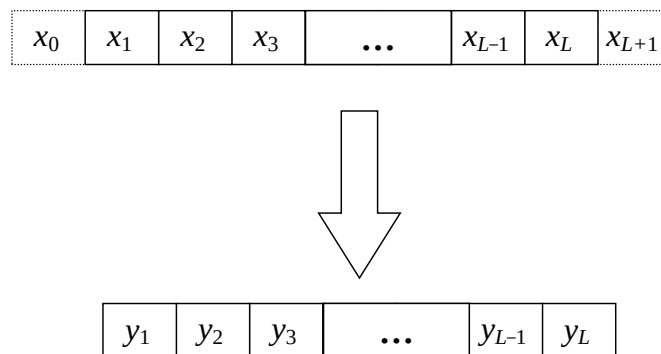


Рис. 2

Набор $(x_0, x_1, x_2, \dots, x_L, x_{L+1})$ назовем **виртуальным прообразом** состояния $(y_1, y_2, \dots, y_L)$.

На рис. 3 приведена схема вычисления следующей конфигурации 1D КЛА:

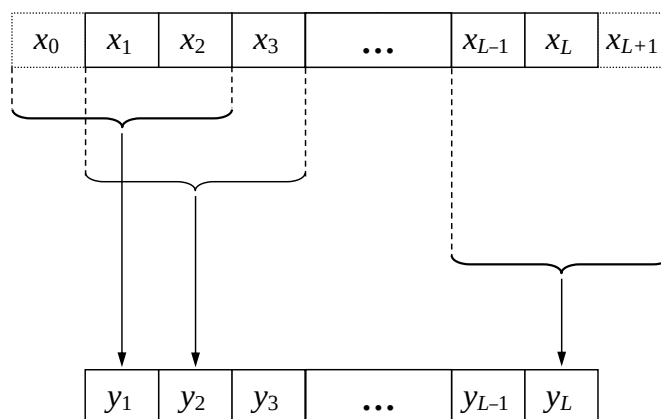


Рис. 3

Следующую конфигурацию КЛА можно вычислить с помощью конструкции (рис. 4), называемой **нелинейным фильтром с входной памятью (НФВП)** [3] или **кодирующим устройством с конечной памятью и без обратной связи** [4], [5].

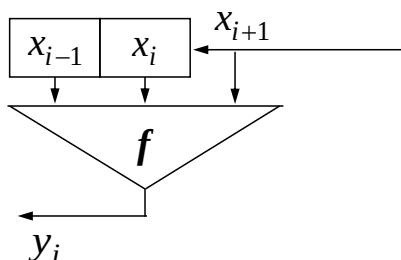


Рис. 4

Задавая (x_0, x_1) в качестве начального состояния (начального заполнения регистра) и подавая на вход последовательность $x_2, x_3, \dots, x_L, x_{L+1}$, на выходе мы получим последовательность $y_1, y_2, \dots, y_L$, т.е. конфигурацию нашего КЛА в следующий момент времени (см. рис. 5).

Тогда нахождение прообраза для конфигурации КЛА $(y_1, y_2, \dots, y_L)$ эквивалентно нахождению прообраза для выходной последовательности НФВП $y_1, y_2, \dots, y_L$, т.е. нахождению такого начального состояния (x_0, x_1) и входной последовательности

$x_2, x_3, \dots, x_L, x_{L+1}$, чтобы на выходе НФВП мы получили последовательность $y_1, y_2, \dots, y_L$. Последовательность $x_0, x_1, x_2, x_3, \dots, x_L, x_{L+1}$, образованную начальным заполнением регистра НФВП и входной последовательностью, назовем **виртуальным прообразом** последовательности $y_1, y_2, \dots, y_L$.

При этом наличие граничных условий налагает ограничения на значения x_0 и x_{L+1} (значения в виртуальных ячейках). В случае нулевой границы (NB) это $x_0 = x_{L+1} = 0$.

Задачи нахождения прообраза выходной последовательности конечного автомата достаточно хорошо изучены в таких разделах теории конечных автоматов, как «Конечные автоматы без потери информации (БПИ)» и «Запреты конечных автоматов».

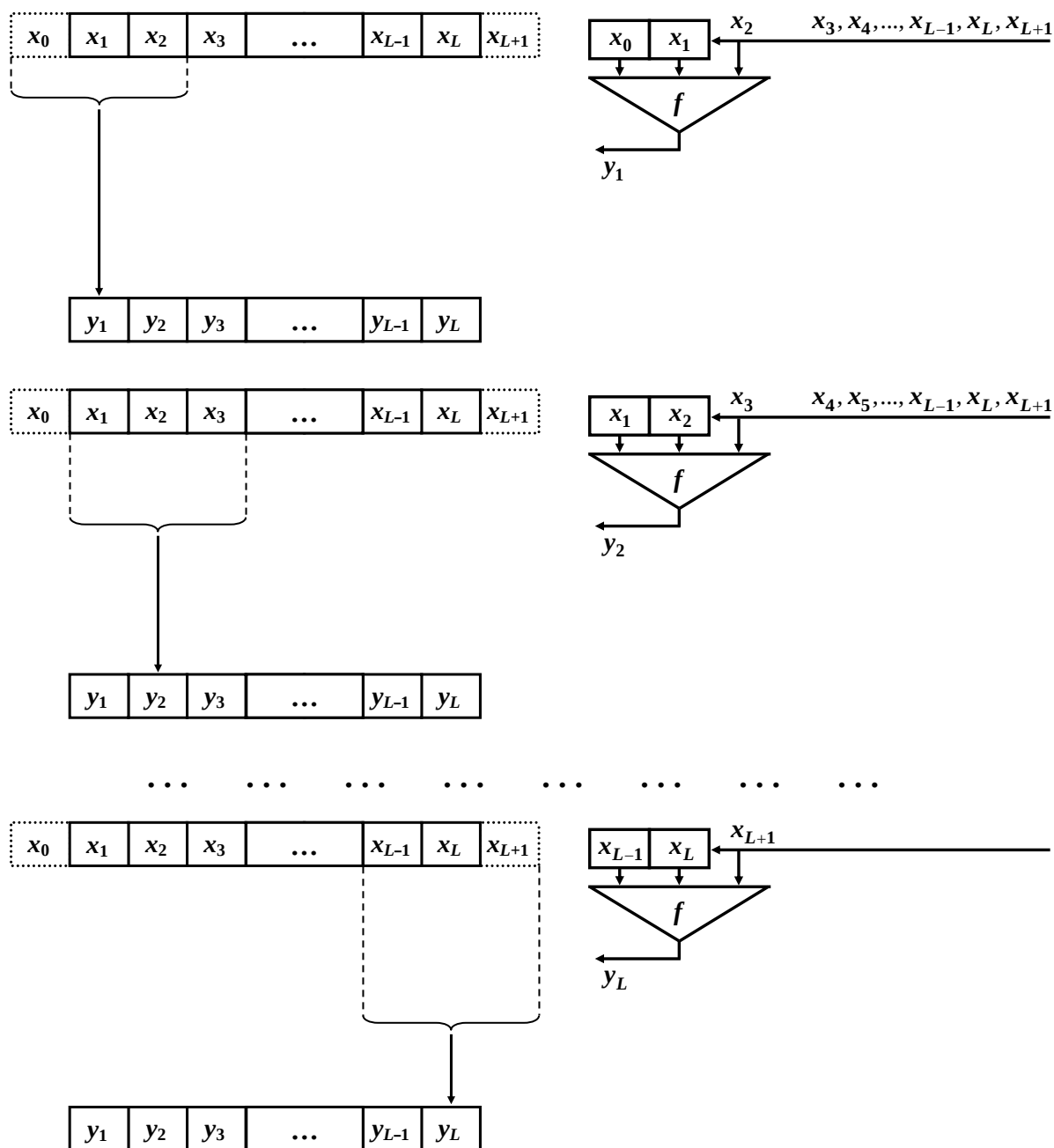


Рис. 5

Автоматы без запретов и автоматы без потери информации

Для дальнейшего изложения нам понадобятся понятия автомата с запретами, автомата без запретов, автомата с потерей информации и автомата без потери информации. Приведем основные определения и результаты, связанные с этими понятиями. Читатель, для которого эти понятия известны, может пропустить настоящий раздел.

Рассмотрим конечный автомат $A = \{X, Q, Y, f, g\}$, где X и Y – входной и, соответственно, выходной алфавиты, Q – множество внутренних состояний автомата, f и g – функции выхода и, соответственно, перехода в следующее состояние.

Автомат A называется автоматом *без запретов* (БЗ), если для любой последовательности $y^{(T)} = y_1, y_2, \dots, y_T, y_t \in Y$ найдутся такое внутреннее состояние q_0 и последовательность $x^{(T)} = x_1, x_2, \dots, x_T, x_t \in X$, что автомат A , находясь в начальном состоянии q_0 и получив на вход последовательность $x^{(T)}$, даст на выходе последовательность $y^{(T)}$. Если же для некоторой последовательности $y^{(T)}$ такие q_0 и $x^{(T)}$ не существуют, то автомат A называется автоматом *с запретами*, соответствующая последовательность $y^{(T)}$ называется *запретом* автомата A , а T – длиной этого запрета.

Незаменимым инструментом для исследований запретов является так называемый *граф запретов*. Формального описания графа запретов в опубликованной литературе, насколько это известно автору, не существует, в то же время эта конструкция (возможно под другими названиями) на протяжении нескольких последних десятилетий использовалась в анализе свойств конечных автоматов. В этой связи приведем в достаточной для понимания подробности эту конструкцию, которая, по сути, является «графом преемников по выходу» (схожая, но в некотором смысле «избыточная» конструкция приведена в [6]).

Граф запретов G автомата A определяется следующим образом.

Вершинами графа являются $V \subseteq Q$ – подмножества множества внутренних состояний автомата, включая, возможно, вершину $V = \emptyset$.

Построение графа начинается с вершины V_0 – начальной вершины графа запретов. Ее образует множество возможных начальных состояний автомата. При отсутствии каких-либо ограничений V_0 совпадает с множеством Q всех внутренних состояний автомата.

Далее алгоритм построения графа запретов таков. Выбирается необработанная вершина $V = \{q_{i_1}, \dots, q_{i_k}\}$. Выбирается символ выходного алфавита: $u \in Y$. Для каждого состояния $q \in V$ определяются его преемники по выходу – это те состояния, в которые можно за один такт перейти из состояния q с выходом u . Объединение преемников по выходу u для всех состояний $q \in V$ образует подмножество V' . Заметим, что множество V' может совпадать с V или быть пустым множеством: $V' = \emptyset$. Если вершина, соответствующая подмножеству V' , была получена ранее, то в графе добавляется дуга, помеченная символом u , которая ведет из V в V' . Если вершины, соответствующей подмножеству V' , в графе нет, то такая вершина добавляется в граф вместе с дугой, помеченной символом u , которая ведет из V в V' . После чего процедура повторяется для следующего символа выходного алфавита.

Для вершины $V = \emptyset$ все дуги с пометками $u \in Y$ ведут в нее же, т.е. являются петлями.

После обработки всех вершин (а эта процедура конечна, поскольку число вершин не превосходит числа всех подмножеств конечного множества Q) получаем связный ориентированный граф G с одной выделенной вершиной V_0 , называемой начальной. Вершинами графа G являются подмножества (как правило – не все) множества внутренних состояний автомата. Из каждой вершины выходит $|Y|$ дуг, помеченных символами $u \in Y$. Дуга, помеченная символом $u \in Y$, соединяет вершину $V =$

$\{q_{i_1}, \dots, q_{i_k}\}$ с вершиной, образованной y -преемниками всех состояний, входящих в V . По построению любая вершина построенного графа достижима из начальной вершины V_0 . Тогда, если из начальной вершины V_0 в вершину $V = \{q_{i_1}, \dots, q_{i_k}\}$ ведет путь длины T , пометки которого образуют последовательность $\mathbf{y}^{(T)} = y_1, y_2, \dots, y_T$, то $V = \{q_{i_1}, \dots, q_{i_k}\}$ – это множество возможных состояний, в которые может перейти наш автомат, начавший работу в одном из состояний из множества V_0 и выработавший при этом выходную последовательность $\mathbf{y}^{(T)}$. Если конечная вершина, соответствующая пути $\mathbf{y}^{(T)}$, является пустой ($V_\emptyset = \emptyset$), это означает, что выходная последовательность $\mathbf{y}^{(T)}$ не может быть выработана нашим автоматом с множеством начальных состояний из V_0 . Если при этом $V_0 = Q$, то последовательность $\mathbf{y}^{(T)}$ является запретом нашего автомата.

Таким образом, запретами (или запретными комбинациями) автомата A являются все последовательности знаков выходного алфавита, соответствующие путям, ведущим из начальной вершины $V_0 = Q$ в вершину $V_\emptyset$.

В свою очередь, если для любого $T > 0$, любой последовательности $\mathbf{y}^{(T)} = y_1, y_2, \dots, y_T$, $y_t \in Y$, в графе запретов G существует путь длины T , помеченный знаками последовательности $\mathbf{y}^{(T)}$, начинающийся в V_0 и заканчивающийся в вершине $V \neq \emptyset$, автомат A является автоматом без запретов. Иными словами, отсутствие запретов у автомата A означает, что граф запретов G не содержит вершину $V_\emptyset = \emptyset$.

Сложность построения графа запретов можно оценить как $O(2^{|Q|})$, Q – множество внутренних состояний автомата.

В работе [5] вводится понятие запрета булевой функции: если НФВП с функцией выхода f является автоматом без запретов, то функция f называется **функцией без запретов**, в противном случае f называется **функцией с запретами**, а последовательность, являющаяся запретной для НФВП, называется **запретом функции** f .

В работах [5], [7] было показано, что для НФВП, рассматриваемого как конечный автомат, отсутствие запретов эквивалентно свойству отсутствия потери информации. Конечный автомат A называется **автоматом без потери информации** – БПИ (*information lossless*), если знание начального состояния, выходной последовательности и конечного состояния достаточно для однозначного определения входной последовательности [8]. Конечный автомат, который не является автоматом без потери информации, называется **автоматом с потерей информации** – ПИ (*lossy*).

Для проверки, является ли данный автомат автоматом без потери информации, имеется эффективный алгоритм, сложность которого оценивается как $O(|Q|^2)$ [9].

Обратимость одномерных клеточных автоматов конечного размера

Возвращаясь к одномерным клеточным автоматам, рассмотрим 1D КЛА длины L с произвольной окрестностью. В общем случае окрестностью i -й ячейки 1D КЛА будем называть ячейки с номерами $i + j$, где $-r_1 \leq j \leq r_2$. Назовем **размером окрестности** величину $R = r_1 + r_2$.

Тогда заполнение i -й ячейки в момент времени t определяется формулой

$$m_i(t) = f(m_{i-r_1}(t-1), \dots, m_{i-1}(t-1), m_i(t-1), m_{i+1}(t-1), \dots, m_{i+r_2}(t-1)),$$

где функция $f(z_{-r_1}, \dots, z_{-1}, z_0, z_1, \dots, z_{r_2})$ – локальная функция связи.

Мы будем исследовать КЛА с нулевой границей (NB): $m_i(t) = 0$ для всех $i < 1$ или $i > L$ и всех t .

Клеточный автомат называется **обратимым**, если для каждой конфигурации КЛА существует только одна предшествующая конфигурация. В силу конечности числа конфигураций у рассматриваемых КЛА, для доказательства обратимости достаточно

показать, что для каждой конфигурации существует хотя бы одна предшествующая конфигурация.

Обратимость 1D КЛА длины L с локальной функцией связи f может быть проверена непосредственным вычислением конфигурации, в которую переходит автомат, находящийся в конфигурации $(x_1, x_2, \dots, x_L)$. Прodelав эти вычисления для всех 2^L конфигураций КЛА, мы, по сути, получаем список всех дуг графа автономного автомата, соответствующего нашему КЛА, по которому легко определить обратимость КЛА: обратимость эквивалентна тому, что в граф представляет собой объединение непересекающихся циклов без подходов. Сложность такого алгоритма оценивается как $O(L \cdot 2^L)$, требуемая память – как $O(2^L)$.

В то же время, если использовать подход, описанный в начале данной работы, нахождение прообраза для состояние КЛА $(y_1, y_2, \dots, y_L)$ эквивалентно нахождению прообраза выходной последовательности $y_1, y_2, \dots, y_L$ для НФВП, приведенного на рис. 6, т.е. нахождению такого начального состояния $(x_{1-r_1}, \dots, x_0, x_1, x_2, \dots, x_{r_2})$ и входной последовательности $x_{r_2+1}, x_{r_2+2}, \dots, x_{r_2+L}$, чтобы на выходе НФВП получилась последовательность $y_1, y_2, \dots, y_L$. При этом нулевая граница (NB) накладывает дополнительные условия: $x_{1-r_1} = \dots = x_0 = x_{L+1} = \dots = x_{L+r_2} = 0$.

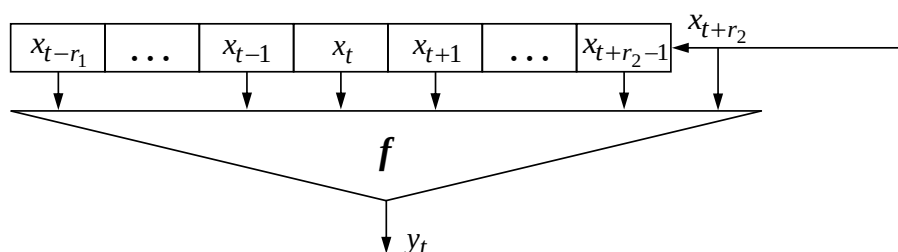


Рис. 6

Обратимость 1D КЛА длины L с локальной функцией связи f эквивалентна тому, что НФВП с регистром длины R (R – размер окрестности КЛА) и функцией выхода f порождает все возможные выходные последовательности длины L .

Для проверки этого свойства построим *ограниченный граф запретов* $\tilde{G}$. Строится он по тем же правилам, что и обычный граф запретов G , но в качестве V_0 – начальной вершины графа запретов – берется множество состояний НФВП, удовлетворяющих граничным условиям $x_{1-r_1} = \dots = x_0 = 0$. Обратимость 1D КЛА длины L эквивалентна тому, что в ограниченном графе запретов любой путь длины L , начинающийся в вершине V_0 , должен заканчиваться в вершине, содержащей хотя бы одно состояние НФВП, удовлетворяющее граничным условиям $x_{L+1} = \dots = x_{L+r_2} = 0$.

Заметим, что граф $\tilde{G}$, как и граф G , зависит только от f – локальной функции связи; сложность его построения зависит от числа внутренних состояний НФВП, равного 2^R , где R – размер окрестности 1D КЛА, и не зависит от L – длины 1D КЛА. Таким образом, исследование 1D КЛА с локальной функцией связи f , можно проводить независимо от размера КЛА.

Для этого исследуется ограниченный граф запретов $\tilde{G}$.

- Если каждая вершина, принадлежащая графу $\tilde{G}$, содержит хотя бы одно состояние НФВП, удовлетворяющее граничным условиям $x_{L+1} = \dots = x_{L+r_2} = 0$, то все 1D КЛА с локальной функцией связи f являются обратимыми, не зависимо от длины КЛА.
- Если граф $\tilde{G}$ содержит вершину V , не содержащую ни одного состояния НФВП, удовлетворяющего граничным условиям $x_{L+1} = \dots = x_{L+r_2} = 0$ (V может

совпадать с V_0), и имеется путь длины L из V_0 в V , то 1D КЛА длины L с локальной функцией связи f необратим.

Заметим, что если ограниченный граф запретов $\tilde{G}$ содержит вершину $V_\emptyset = \emptyset$ и l_0 – длина кратчайшего пути из V_0 в $V_\emptyset$, то все 1D КЛА длины $L \geq l_0$ с локальной функцией связи f не являются обратимыми. Для $L < l_0$ потребуется провести исследование, аналогичное описанному выше.

Заметим также, что если НФВП с функцией выхода f является автоматом с запретом, его граф запретов G содержит вершину $V_\emptyset = \emptyset$. Из построения ограниченного графа запретов $\tilde{G}$ следует, что граф $\tilde{G}$ также содержит вершину $V_\emptyset$, причем длина кратчайшего пути из V_0 в $V_\emptyset$ в графе $\tilde{G}$ не превосходит длину кратчайшего пути из V_0 в $V_\emptyset$ в графе G . Однако в силу того, что для НФВП, рассматриваемого как конечный автомат, наличие запретов эквивалентно наличию потери информации, проверить факт наличия запрета легче с помощью эффективного алгоритмы проверки автомата на наличие потери информации. Сложность этой проверки можно оценить как $O(2^{2R})$.

Заметим в заключение, что все приведенные выше рассуждения можно перенести на 1D КЛА с небинарным заполнением клеток.

Применение к двумерным клеточным автоматам

Рассмотренный выше подход можно применить для исследования двумерных клеточных автоматов (2D КЛА).

Рассмотрим 2D КЛА размера $k \times L$, заполнение каждой ячейки которого является булевой величиной (бинарный 2D КЛА) – рис. 7.

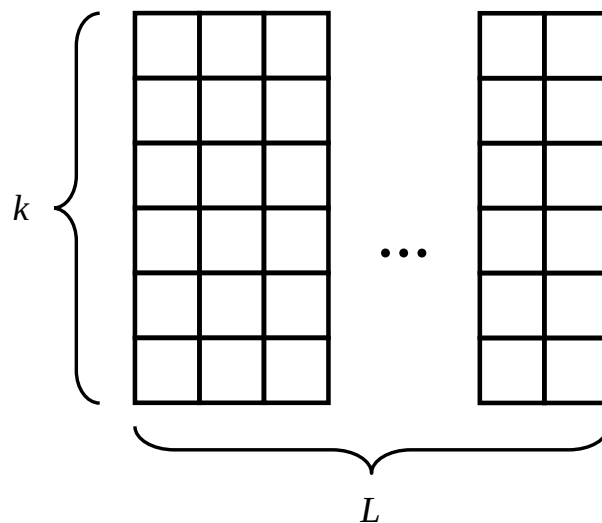


Рис. 7

В качестве окрестности ячейки выберем окрестность фон Неймана радиуса $r = 1$ (см. рис. 8):

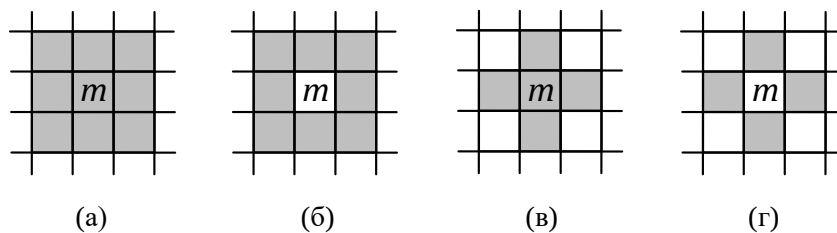


Рис. 8 – Некоторые типы окрестности радиуса $r = 1$ для ячейки m двумерного КЛА:
а) полная окрестность (окрестность Мура)

- б) квазиполная окрестность Мура
- в) окрестность фон Неймана
- г) неполная окрестность фон Неймана

Клетки, лежащие в одном столбце, можно считать одной ячейкой, содержащее которой принимает 2^k значений и является элементом $\mathbb{Z}_2^k$ или $\mathbb{Z}_{2^k}$ (рис. 9). Тогда 2D КЛА размера $k \times L$ можно рассматривать как 1D КЛА размера L над алфавитом мощности 2^k (рис. 10).

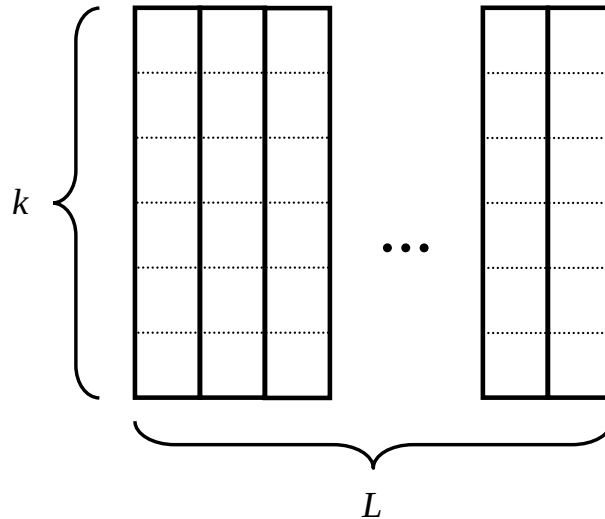


Рис. 9

Рис. 10

Задача: по окрестности и локальной функции связи f для 2D КЛА построить окрестность и локальную функцию связи f_1 для соответствующего 1D КЛА.

Выводы

В работе показано, что 1D КЛА с локальной функцией связи f можно сопоставить НФВП с регистром длины R (где R – размер окрестности КЛА) и функцией выхода, совпадающей с локальной функцией связи 1D КЛА. Определение обратимости 1D КЛА связано с нахождением прообраза (а, по сути, с обратимостью) НФВП. При этом от L (размера 1D КЛА) НФВП не зависит. Полученные результаты позволяют снизить сложность решения массовых задач переборного типа, связанных с вопросами обратимости КЛА. Все полученные результаты можно перенести на КЛА с небинарным заполнением ячеек и на КЛА размерности большей 1.

Литература

- [1] Жуков А.Е. Клеточные автоматы в криптографии. Часть 1 // Вопросы кибербезопасности. 2017. № 3 (21). С. 70-76. DOI: 10.21581/2311-3456-2017-3-70-76.
- [2] Жуков А.Е. Клеточные автоматы в криптографии. Часть 2 // Вопросы кибербезопасности. 2017. № 4 (22). С. 47-66. DOI: 10.21581/2311-3456-2017-4-47-66
- [3] Lai X., Massey J.L. Some connections between scramblers and invertible automata. In Proc. 1988 Beijing Int. Workshop on Info. Theory, Beijing, China, July 4-7, 1988, p. DI-5.1 – DI-5.5.
- [4] Preparata F.P. Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties // IEEE Trans. Electron. Comput., 1966, v. 15, № 6, p. 898-909.
- [5] Сумароков С.Н. Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики, сер. дискретн. матем., 1994, т. 1, в. 1, с. 33-55.
- [6] Бабаш А.В. Запреты автоматов и двоичных функций // Труды по дискретной математике. – Том 9, с. 7-20. – М.: Гелиос АРБ, 2006
- [7] Olson R.R. On the invertibility of finite state machines. Ph.D. diss., Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana, USA, 1970.
- [8] Huffman D.A. Canonical forms for information loss less finite state logical machines // IRE Trans. Circuit Theory, 1959, v. 6, spec. suppl., p. 41-59.
- [9] Zvi Kohavi, Niraj K. Jha. Switching and Finite Automata Theory. – Cambridge University Press, Cambridge, UK, 2010

Cellular automata and prohibitions of Boolean functions

Zhukov A. E.⁷⁹

Abstract. *The paper shows that the reversibility of a one-dimensional cellular automaton (CA) is related to the properties of a construction called «binary filter with input memory» (BFIM). In our case, the BFIM does not depend on the number of memory cells of the CA, but depends only on its local transition function. The results obtained make it possible to reduce the complexity of solving mass enumeration problems related to the CA reversibility. All the results obtained can be transferred to CA with non-binary cell filling and to CA of dimension greater than 1.*

Keywords: *reversible cellular automaton, binary filter with input memory, an automaton with prohibitions, an automaton without prohibitions, information lossless automaton, information lossy automaton, a graph of automaton prohibitions.*

References

- [1] Zhukov A.E. Kletochnye avtomaty v kriptografii. Chast' 1. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017, No 3 (21). P. 70-76. DOI: 10.21581/2311-3456-2017-3-70-76.
- [2] Zhukov A.E. Kletochnye avtomaty v kriptografii. Chast' 2. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017, No 4 (22), P. 47-66. DOI: 10.21681/2311-3456-2017-4-47-66
- [3] Lai X., Massey J.L. Some connections between scramblers and invertible automata. In Proc. 1988 Beijing Int. Workshop on Info. Theory, Beijing, China, July 4-7, 1988, p. DI-5.1 – DI-5.5.
- [4] Preparata F.P. Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties // IEEE Trans. Electron. Comput., 1966, v. 15, № 6, p. 898-909.
- [5] Sumarokov S.N. Zaprety dvoichnyh funkciy i obratimost dlja odnogo klassa kodirujuschih ustrojstv. Obozrenije prikladnoj i promyshlennoj matematiki [Review of Applied and Industrial Mathematics], ser. discr. math. 1994, v.1, No1, P. 33-55.
- [6] Babash A.V. Zaprety avtomatov i dvoichnyh funkciy. Trudy po diskretnoj matematike [Proceedings on discrete mathematics]. 2006, v.9, P. 7-20.
- [7] Olson R.R. On the invertibility of finite state machines. Ph.D. diss., Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana, USA, 1970.
- [8] Huffman D.A. Canonical forms for information loss less finite state logical machines // IRE Trans. Circuit Theory, 1959, v. 6, spec. suppl., p. 41-59.
- [9] Zvi Kohavi, Niraj K. Jha. Switching and Finite Automata Theory. – Cambridge University Press, Cambridge, UK, 2010

⁷⁹ Zhukov Alexey Evgenjevich, Ph.D. (Math.), Associate Professor, Director at Association «RusCrypto», BMSTU, Moscow, aez_iu8@rambler.ru

Исследование булевых функций с аффинными аннигиляторами

Зеленецкий А.С.⁸⁰

Аннотация. Булева функция f называется аннигилятором булевой функции g , если выполнено тождество $fg \equiv 0$. Аннигиляторы находят свое применение в алгебраическом криптоанализе, а также в некоторых задачах анализа конечных автоматов. В обоих случаях, как правило, требуется найти аннигиляторы низкой алгебраической степени для заданной булевой функции. Данная работа посвящена булевым функциям с аффинными аннигиляторами. Представлена оценка количества таких функций, а также получена связь спектра булевой функции с наличием у нее аффинного аннигилятора. Помимо этого, предложен способ анализа булевых уравнений с помощью функций, имеющих аффинные аннигиляторы.

Ключевые слова: булева функция, аффинная функция, аннигилятор, бент-функция, преобразование Уолша-Адамара.

Введение

Рассмотрим произвольную систему булевых полиномиальных уравнений от нескольких переменных. Как правило, решить такую систему уравнений на практике при высоких алгебраических степенях исходных уравнений невозможно в связи с большой вычислительной сложностью. Однако существуют методы сведения исходной системы уравнений к более простой, которые в некоторых случаях могут помочь найти решение. Один из таких методов был представлен в работе [1], посвященной криптоанализу фильтрующего генератора псевдослучайной последовательности. Для упрощения уравнения $f(x) = b$, где f является булевой функцией, x вектором неизвестных, а $b \in \{0,1\}$, предлагается использовать булеву функцию g , удовлетворяющую следующим свойствам:

- 1) Функция g имеет низкую алгебраическую степень;
- 2) Булева функция h , равная побитовому произведению функций f и g , также имеет низкую алгебраическую степень.

При наличии подходящей функции g можно свести исходной уравнение к уравнению $h(x) = bg(x)$. Полученное уравнение имеет, очевидно, более низкую степень. В работе [2] было показано, что для успешного применения данного метода достаточно найти аннигилятор низкой степени либо для функции f , либо для функции $f + 1$. Под аннигилятором булевой функции f понимается такая булева функция g , что $fg \equiv 0$.

Для осуществления предложенного метода упрощения булевых уравнений на практике необходим алгоритм поиска аннигиляторов низкой степени для произвольной булевой функции. Таким алгоритмам посвящены работы [3, 4, 5]. Величина $AI(f) =$

$\min_{\substack{g \neq 0 \\ fg \equiv 0 \vee (f+1)g \equiv 0}} \deg g$ называется порядком алгебраической иммунности функции f . Чем

меньше данная величина, тем эффективнее рассмотренный метод анализа для уравнения $f(x) = b$. В работах [6,7,8,9] исследуется связь порядка алгебраической иммунности булевой функции с такими ее характеристиками как, например, вес и нелинейность r – го порядка. В [10] представлены сведения об основных достижениях в изучении порядка алгебраической иммунности булевой функции.

⁸⁰ Зеленецкий Алексей Сергеевич, МГТУ им. Н.Э.Баумана, Москва

Данная работа посвящена исследованию булевых функций, имеющих аффинные аннигиляторы. Получена оценка их количества, а также представлена связь спектра булевой функции с наличием у нее аффинного аннигилятора. Также предложен метод анализа булевых уравнений с использованием булевых функций, имеющих аффинные аннигиляторы.

Оценка количества булевых функций с аффинными аннигиляторами

Обозначим множество булевых функций от n переменных, имеющих аффинные аннигиляторы, как AA_n . Нами были получены несколько неравенств, в которых ограничивается мощность данного множества.

$$|AA_n| \geq 2|AA_{n-1}|(2^{2^{n-2}} - 1) + 2^{2^{n-1}}. \quad (1)$$

Неравенство (1) служит оценкой снизу для количества булевых функций с аффинными аннигиляторами.

$$|AA_n| \leq 2^{2^{n-1}+n+1}. \quad (2)$$

Данное неравенство является оценкой сверху для мощности множества AA_n . Неравенства (1) и (2) используются нами для получения следующей оценки.

$$|AA_n| \geq c 2^{2^{n-1}+n+1}, \quad (3)$$

здесь $c \in (0, 0.5]$ и $n \geq 5$.

Все вышеперечисленное позволяет нам заключить, что при $n \rightarrow \infty$ функции $|AA_n|$ и $g(n) = 2^{2^{n-1}+n+1}$ являются функциями одного порядка.

Связь спектра булевой функции с наличием у нее аффинного аннигилятора

Рассмотрим уравнение $f(x) = 1$, где $f \in AA_n$. Согласно работе [2], для решения данного уравнения мы можем перейти к решению уравнения первой степени $a(x) = 0$, где $a(x)$ является аффинной функцией, аннигилирующей f . Теперь рассмотрим некоторую функцию $h \notin AA_n$, находящуюся на небольшом расстоянии от функции f . Так как h находится на небольшом расстоянии от f , с высокой вероятностью $h(x) = 1$ на тех же x , где $f(x) = 1$. Поэтому для решения уравнения $h(x) = 1$, мы также предлагаем его замену на уравнение $a(x) = 0$. Предложенный метод похож на метод замены булевой функции ее линейным статаналогом, однако может быть более успешным в виду того, что мощность множества AA_n значительно превосходит количество аффинных функций. Критерием успеха представленного метода является отношение $\frac{d(f, AA_n)}{\|f\|}$.

Нами была выведена формула расстояния между произвольной булевой функцией f и множеством AA_n . Данная формула связывает упомянутое расстояние со спектром булевой функции, а также с ее весом.

$$d(f, AA_n) = \frac{\|f\|}{2} - \max_{u \neq 0} \frac{|W_f(u)|}{4}, \quad (4)$$

здесь $W_f(u)$ значение преобразования Уолша-Адамара булевой функции f на векторе u . Из формулы (4) легко следует, что булева функция f имеет аффинный аннигилятор тогда и только тогда, когда найдется такой вектор $u \neq 0$, что $|W_f(u)| = 2 \|f\|$. Более того,

формула (4) дает возможность установить ограничения на значения коэффициентов Уолша-Адамара для заданной булевой функции f . Очевидно, что для любого $u \neq 0$ выполнено неравенство $|W_f(u)| \leq 2\|f\|$.

Также нами было установлено, что значение отношения $\frac{d(f, AA_n)}{\|f\|}$ для бент-функций принимает максимально возможное значение при $n \rightarrow \infty$. А именно, было доказано, что для любой бент-функции f

$$\lim_{n \rightarrow \infty} \frac{d(f, AA_n)}{\|f\|} = 0.5 . \quad (5)$$

Выводы

В данной работе были исследованы булевы функции, имеющие аффинные аннигиляторы. Удалось оценить количество таких функций. Был предложен метод анализа булевых уравнений, основанный на замене функции из уравнения на ближайшую к ней функцию с аффинным аннигилятором. Для реализации предложенного метода была получена взаимосвязь между спектром булевой функции и ее расстоянием до множества функций, имеющих аффинные аннигиляторы, а также был получен критерий принадлежности функции к данному множеству. Было доказано, что бент-функции максимально удалены от функций с аффинными аннигиляторами.

Литература

1. Courtois N., Meier W. Algebraic Attacks on Stream Cipher with Linear Feedback // Lecture Notes Computer Sci. (2003) 2656, p.345-359.
2. Meier W., Pasalic E., Carlet C. Algebraic Attacks and Decomposition of Boolean Functions // Lecture Notes Computer Sci.(2004) 3027, p.474-491.
3. Courtois N. Fast algebraic attacks on stream ciphers with linear feedback // Lecture Notes Computer Sci.(2003) 2729, p.177-194.
4. Баев В.В. О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций // Дискрет. матем., 2006, том 18, выауск 3, с.138-151.
5. Баев В.В. Усовершенствованный алгоритм поиска аннигиляторов низкой степени булевых функций // Дискрет.матем., 2007, том 19, выпуск 4, с.132-138.
6. Armknecht F. On the Existence of low-degree Equations for Algebraic Attacks // Cryptology ePrint Archive: Report 2004/185.
7. Dalai D.K., Gupta K.C., Maitra S. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions // Indocrypt 2004. Berlin/Heidelberg: Springer-Verlag, 2004, p. 92-106.
8. Carlet C. On the higher order nonlinearities of algebraic immune functions // CRYPTO 2006. Lect. Notes in Comp.Sci. Berlin/Heidelberg: Springer-Verlag, 2006, p. 584-601.
9. Mesnager S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescibed algebraic immunity // Cryptology ePrint archive, <http://eprint.iacr.org/2007/117>.
10. О.А. Логачев, А.А. Сальников, С.В. Смышляев, В.В. Яценко Булевы функции в теории кодирования и криптологии. М.:ЛЕНАНД, 2015.

Научный руководитель: Жуков Дмитрий Александрович, доцент, кандидат физико-математических наук, МГТУ им. Н.Э.Баумана.

Investigation of Boolean Functions with Affine Annihilators

Zelenetsky A.S.⁸¹

Annotation. *A Boolean function f is called an annihilator of a Boolean function g if the identity $fg=0$ holds. Annihilators find their application in algebraic cryptanalysis, as well as in some problems of analysis of finite automata. In both cases, as a rule, it is required to find annihilators of low algebraic degree for a given Boolean function. This work is devoted to Boolean functions with affine annihilators. An estimate of the number of such functions is presented, and a connection is obtained between the spectrum of a Boolean function and the presence of an affine annihilator in it. In addition, a method for analyzing Boolean equations using functions with affine annihilators is proposed.*

Keywords: *Boolean function, affine function, annihilator, bent function, Walsh-Hadamard transform.*

УДК 004.056

⁸¹ Zelenetsky Alexey Sergeevich, Bauman MSTU, Moscow

Методика фаззинг-тестирования кода с помощью AFL

Зимин Е.Е.⁸²

Аннотация. Приведено решение фаззинг-тестирования кода, написанного на базе языка программирования C, с помощью фаззера American Fuzzy Lop в операционной системе Ubuntu, дистрибутиве Linux. Результатом тестирования являются найденные уникальные уязвимости кода в рамках его защиты в области информационной безопасности.

Ключевые слова: фаззер, LibFuzzer, санитайзер.

Введение

Термин Fuzzing появился еще в 1988 году в работе "The Fuzz Generator", опубликованной Бартом Миллером, где предложил подсовывать программе заведомо некорректные и зачастую вообще случайные данные, отлавливая ситуации, когда та не сможет их обработать и вылетит. В то же время данный подход как стохастическое тестирование был известен задолго до него [1].

Программа, осуществляющая фаззинг, называется фаззером. Фаззер может использовать грубую силу для перебора всевозможных входных данных или использовать какие-то шаблоны, заточенные под определённые форматы данных. В основном их разрабатывают и используют исследователи в области безопасности для поиска уязвимостей в программных продуктах.

Одним из фаззеров является AFL (American Fuzzy Lop) за авторством известного эксперта в области безопасности Michal Zalewski. AFL внедряет в код специальные ассемблерные инструкции в точки ветвления для отслеживания поведения подопытной программы, позволяя определять, когда происходит переключение на новую ветвь исполнения, и какие входные данные повлияли на это. Для этих целей требуется собрать исходный код программы с помощью компиляторов-обёрток. После того как программа собрана, она может быть подвергнута тестированию [1-12].

Объект исследования – фаззинг-тестирование кода с помощью AFL.

Предмет исследования – методика данного фаззинг-тестирования.

Целью данной работы является составление методики фаззинг-тестирования кода с помощью AFL.

Входные данные

Код, который будет подвергнут фаззингу, — это простенькая программа на языке C, содержащая все нижеупомянутые распространенные типы уязвимостей:

Целочисленное переполнение (integer overflow) — ситуация, при которой вычисленное в результате операции значение не может быть помещено в n-битный целочисленный тип данных;

- a. Integer underflow;
- б. Out of bound Read;
- в. Out of bound Write;
- г. Double Free;
- д. Use-After-Free возникает если указатель кучи продолжает использоваться уже после ее освобождения. Такая уязвимость может повлечь за собой выполнение производного кода;
- е. Утечка памяти (Memory leaks) — процесс неконтролируемого уменьшения объёма свободной оперативной или виртуальной памяти компьютера, связанный с ошибками в работающих программах, вовремя не

⁸² Зимин Евгений Евгеньевич, Финансовый Университет при Правительстве РФ, Москва, kengazheka@mail.ru

освобождающих ненужные участки памяти, или с ошибками системных служб контроля памяти;

жс. Stack exhaustion;

з. Heap exhaustion.

Все операции будут выполняться на Ubuntu, так что заранее требуется подготовить технику для работы на данной операционной системе.

Порядок действий фаззинг-тестирования

Устанавливаем AFL и компилируем:

```
$ git clone https://github.com/google/AFL.git
```

```
$ cd AFL/
```

```
$ make
```

1. Компилируем режим LLVM:

```
$ cd llvm_mode/
```

```
$ make
```

```
$ cd ..
```

```
$ sudo make install
```

2. Чтобы генерировать входные данные для AFL, просто создадим пример входного файла следующим образом, а дальше AFL сам обо всё позаботится:

```
$ echo "IMG" >1.txt
```

AFL автоматически генерирует новые тестовые случаи и обнаруживает большинство уязвимостей, упомянутых выше.

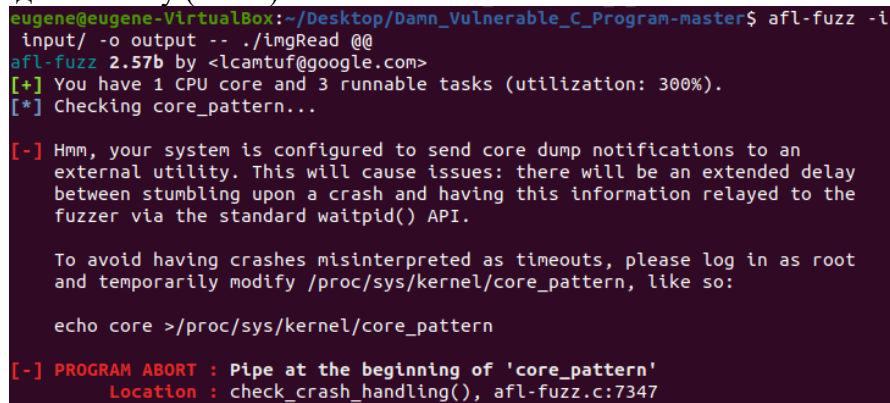
3. Сделаем компиляцию в файл imgRead:

```
$ afl-gcc -g -fsanitize=address imgRead.c -o imgRead
```

4. Запускаем фаззер:

```
$ afl-fuzz -i input -o output -m none -- ./imgRead @@
```

Выводит ошибку (Рис.1).



```
eugene@eugene-VirtualBox:~/Desktop/Damn_Vulnerable_C_Program-master$ afl-fuzz -i
input/ -o output -- ./imgRead @@
afl-fuzz 2.57b by <lcamtuf@google.com>
[+] You have 1 CPU core and 3 runnable tasks (utilization: 300%).
[*] Checking core_pattern...

[-] Hmm, your system is configured to send core dump notifications to an
external utility. This will cause issues: there will be an extended delay
between stumbling upon a crash and having this information relayed to the
fuzzer via the standard waitpid() API.

To avoid having crashes misinterpreted as timeouts, please log in as root
and temporarily modify /proc/sys/kernel/core_pattern, like so:

echo core >/proc/sys/kernel/core_pattern

[-] PROGRAM ABORT : Pipe at the beginning of 'core_pattern'
Location : check_crash_handling(), afl-fuzz.c:7347
```

Рис.1. Ошибка при попытке запуска фаззера

Решаем так:

```
$ cd --
```

```
$ echo "core-%e" | sudo tee /proc/sys/kernel/core_pattern &> /dev/null
```

Еще одна ошибка (Рис.2):

```
eugene@eugene-VirtualBox:~/Desktop/Damn_Vulnerable_C_Program-master$ afl-fuzz -i input/
-o output -- ./imgRed @@
afl-fuzz 2.57b by <lcantuf@google.com>
[+] You have 1 CPU core and 4 runnable tasks (utilization: 400%).
[*] Checking core_pattern...
[*] Setting up output directories...
[+] Output directory exists but deemed OK to reuse.
[*] Deleting old session data...
[+] Output dir cleanup successful.
[*] Scanning 'input/'...
[+] No auto-generated dictionary tokens to reuse.
[*] Creating hard links for all input files...
[*] Validating target binary...
[*] Attempting dry run with 'id:000000,orig:1.txt'...
[*] Spinning up the fork server...

[-] Whoops, the target binary crashed suddenly, before receiving any input
    from the fuzzer! Since it seems to be built with ASAN and you have a
    restrictive memory limit configured, this is expected; please read
    /usr/local/share/doc/afl/notes_for_asan.txt for help.

[-] PROGRAM ABORT : Fork server crashed with signal 6
    Location : init_forkserver(), afl-fuzz.c:2230
```

Рис.2. Ошибка при попытке запуска фаззера

Что касается ошибки, приведенной на рисунке 4, она решается добавлением “-m попе”, что уже, собственно, сделано в изначально предложенном варианте написания команды. Так же иногда программа проверяет расширение файла или имеет проблемы с теми именами, которые придумывает afl-fuzz, для это есть удобная опция -f, которая передаёт одно и тоже имя файла.

Начинается процесс фаззинга (Рис.3), который может занять достаточно длительное время.

american fuzzy lop 2.57b (imgRead)			
process timing		overall results	
run time :	0 days, 0 hrs, 0 min, 50 sec	cycles done :	108
last new path :	none yet (odd, check syntax!)	total paths :	1
last uniq crash :	0 days, 0 hrs, 0 min, 40 sec	uniq crashes :	7
last uniq hang :	none seen yet	uniq hangs :	0
cycle progress		map coverage	
now processing :	0 (0.00%)	map density :	0.01% / 0.01%
paths timed out :	0 (0.00%)	count coverage :	1.00 bits/tuple
stage progress		findings in depth	
now trying :	havoc	favored paths :	1 (100.00%)
stage execs :	120/256 (46.88%)	new edges on :	1 (100.00%)
total execs :	29.1k	total crashes :	1220 (7 unique)
exec speed :	599.9/sec	total tmouts :	872 (3 unique)
fuzzing strategy yields		path geometry	
bit flips :	0/32, 0/31, 0/29	levels :	1
byte flips :	0/4, 0/3, 0/1	pending :	0
arithmetics :	0/224, 0/25, 0/0	pend fav :	0
known ints :	0/25, 0/84, 0/44	own finds :	0
dictionary :	0/0, 0/0, 0/0	imported :	n/a
havoc :	7/28.4k, 0/0	stability :	100.00%
trim :	n/a, 0.00%		
[cpu:306%]			

Рис.3. Процесс фаззинга файла imgRead

В данном случае на фаззинг можно было бы выделить около часа, чтобы найти 8 уникальных случаев сбоя. Тем не менее, получаем результаты фаззинг-тестирования скомпилированного файла imgRead спустя 2 часа работы фаззера (Рис.4).

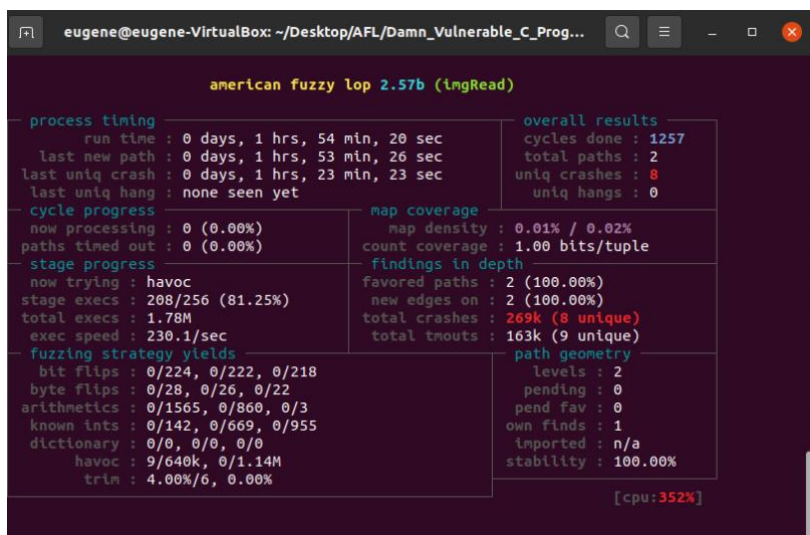


Рис.4. Процесс фаззинга файла imgRead

Пройдя 1257 циклов, программа обнаружила 8 уникальных случаев сбоев за 270 тысяч случаев сбоя.

5. Нажав сочетание клавиш Ctrl+C, останавливаем процесс фаззинга.
6. Можем перейти в папку output/crashes, чтобы посмотреть на перечень сбоев. Их тут как раз 8 штук (Рис.5).

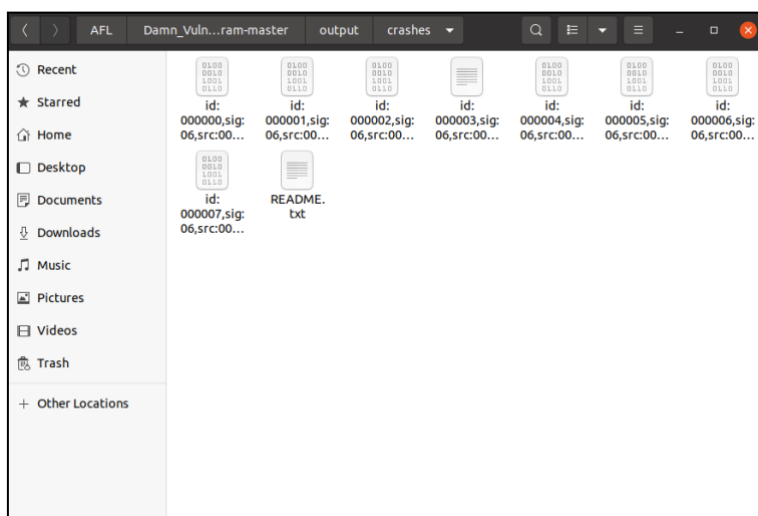


Рис.5. Перечень сбоев после фаззинга файла imgRead

Незамысловатым способом можно открыть данный перечень через консоль, как это представлено на рисунке 6:

```
eugene@eugene-VirtualBox:~/Desktop/AFL/Damn_Vulnerable_C_Program-master$ cd output/
eugene@eugene-VirtualBox:~/Desktop/AFL/Damn_Vulnerable_C_Program-master/output$ ls
crashes fuzz_bitmap fuzz_stats hangs plot_data queue
eugene@eugene-VirtualBox:~/Desktop/AFL/Damn_Vulnerable_C_Program-master/output$ cd crashes/
eugene@eugene-VirtualBox:~/Desktop/AFL/Damn_Vulnerable_C_Program-master/output/crashes$ ls
id:000000,sig:06,src:000000,op:havoc,rep:128
id:000001,sig:06,src:000000,op:havoc,rep:64
id:000002,sig:06,src:000000,op:havoc,rep:64
id:000003,sig:06,src:000000,op:havoc,rep:8
id:000004,sig:06,src:000000,op:havoc,rep:16
id:000005,sig:06,src:000000,op:havoc,rep:32
id:000006,sig:06,src:000000,op:havoc,rep:128
id:000007,sig:06,src:000000,op:havoc,rep:128
README.txt
```

Рис.6. Перечень сбоев после фаззинга файла imgRead в консоли

Расшифровка: id – индивидуальный номер, sig – сигнал, src – ресурс, ор – ядро, гер – репозиторий.

Таким образом, достаточно практичная методика установки AFL и проверки на простейшем уязвимом коде.

Выводы

Тема фаззинга на сегодняшний день уже вышла далеко за пределы просто одного из видов тестирования. По версии DevSecOps, все больше компаний внедряют этот тип тестирования в том или ином виде. В нашей стране фаззинг является обязательной процедурой при разработке безопасных программ [12].

Так, в ходе учебной практики был описан такой метод фаззинг-тестирования, как фаззинг кода с помощью AFL. Экспериментальным способом были выведены уязвимости определенного кода, что влияет на его защиту в рамках информационной безопасности.

Литература

1. Reber, G., Malmquist, K., Shcherbakov, A. 2014. Mapping the Application Security Terrain. *Voprosy kiberbezopasnosti (Cybersecurity Issues)*. 2014, N 1(2), P. 36-39.
2. Godefroid P. Automated whitebox fuzz testing / P. Godefroid, M. Levin // NDSS. - 2008. - 250 p.
3. Oehlert P. Violating Assumptions with Fuzzing / P. Oehlert // IEEE Security & Privacy. - 2005. - № 2. - P. 58-67.
4. Casella G., Fienberg S., Olkin I. The Bayesian Choice / G. Casella, S. Fienberg, I. Olkin. - Springer, 2007. - P. 285-310.
5. Russel S., Norvig P. Artificial Intelligence A Modern Approach / S. Russel, P. Norvig. - Prentice Hall. - 2009. - P. 566-599.
6. Zalewski M. The Tangled Web. A Guide to Securing Modern Web Applications / M. Zalewski. - No starch Press, 2012. - 477 p.
7. Тулупьев А. Байесовские сети, логико-вероятностный подход / А. Тулупьев, С. Николенко, А. Сироткин. - СПб.: Наука, 2006. - 728 с.
8. Böhme M., Pham V., Nguyen M., Roychoudhury A. Directed Greybox Fuzzing // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. P. 2329-2344.
9. Pak B. Hybrid Fuzz Testing: Discovering Software Bugs via Fuzzing and Symbolic Execution / PhD Thesis. Carnegie Mellon University, 2012. 80 p.
10. Addison A. Blending fuzzing and symbolic execution for malware analysis / Diss. for the Degree Bachelor of Science in Comp. Sc. - Georgia Institute of Technology, 2017. 24 p.
11. Shudrak M., Zolotarev V. The technique of dynamic binary analysis and its application in the information security sphere // In Proceedings of IEEE EuroCon - 2013, Zagreb, Croatia. 2013. P. 112-118.
12. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5 (13). С. 2-10.

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

The technique of fuzzing code using AFL

Zimin E.E.⁸³

Abstract. *There is the solution of fuzzing code written on the basis of the C programming language, using the fuzzer American Fuzzy Lop (AFL) in the Ubuntu operating system (distribution of Linux). The result of testing is the unique vulnerabilities found in the code as part of its protection in the field of information security.*

Keywords: *fuzzer, libFuzzer, sanitizer.*

⁸³ Zimin Eugene Eugenevich, Financial University under the government of the Russian Federation, Moscow, kengazheka@mail.ru

О возможном подходе к аутентификации пользователя по клавиатурному почерку на основе ПЭМИ клавиатуры

Казанцев И.С.⁸⁴

Аннотация. Проведен совокупный анализ современных исследований в области обнаружения сигналов побочных электромагнитных излучений от стандартной клавиатуры интерфейса USB и способов аутентификации по динамике нажатия клавиш. Выявлена зависимость между возникновением спектра сигнала в радиоэфире и частотой набора текста на клавиатуре. Данные исследования могут позволить усовершенствовать подходы к аутентификации пользователей и созданию приемного программно-аппаратного ключа.

Ключевые слова: побочные электромагнитные излучения, аутентификация, динамика нажатия клавиш.

Введение

В настоящее время инсайдерские угрозы являются актуальной проблемой [1]. Создание новых решений по защите конфиденциальной информации от несанкционированного доступа позволит снизить риски информационной безопасности на предприятии. Применяемые средства защиты можно «обмануть» путем кражи знания уникального ключа. Современные биометрические системы требуют дополнительных финансовых затрат, но в эпоху развития информационных технологий последние являются оправданными [2]. Недостаток в использовании аппаратного USB-ключа состоит в том, что при краже этого устройства [3] и знании PIN-кода, возможно овладение информацией и нарушение её целостности. Непрерывный контроль за законным оператором ключевой системы посредством приема информативного сигнала, создаваемого побочными электромагнитными излучениями (далее – ПЭМИ) клавиатуры при наборе текста, позволит исключить возможность работы злоумышленника. Таким образом, реализация устройства, в основе работы которого лежит алгоритм аутентификации пользователя по динамике нажатия клавиш и алгоритм записи сигналов ПЭМИ клавиатуры, позволит улучшить современные подходы к защите конфиденциальной информации. Алгоритм расчета качества оптимального приемника [4] совместно с анализом радиоэфира, в котором выделены частотные составляющие клавиатурного почерка [5, 6], позволят на некотором удалении от автоматизированного рабочего места оператора вести радиоконтроль, что является актуальным для [7].

Особенности сигнала ПЭМИ клавиатуры

Работы ученых [8-11] в области обнаружения, анализа и восстановления сигналов ПЭМИ позволяют сделать вывод об актуальности совершенствования методики распознавания информативных данных. О физической природе возникновения ПЭМИ подробно написано в [12]. Кобяков В.Ю. и Лучинин А.С. в своей работе [13] подробно рассмотрели особенности протокола USB и рассчитали теоретически реализуемый порог чувствительности приемника, равный 13,3 мкВ. При этом на вход приемника поступает сигнал $y(t)$, который определяется уравнением:

$$y(t) = s(t) + \varepsilon(t) + n(t), \quad (1)$$

где: $s(t)$ – полезный сигнал, представляющий собой последовательность перепадов фронтов в начале каждого импульса, $\varepsilon(t)$ – помеха, $n(t)$ – нормальный внутренний шум приемника [4].

Проведенные исследования [14] показывают возможность восстановления

⁸⁴ Казанцев Иван Сергеевич, аспирант, МГТУ им. Н.Э. Баумана, Москва, kazantsevivan1991@mail.ru

информации о каждой отдельно нажатой клавише. Сигнал, излученный от кабеля USB клавиатуры, измеряется при помощи осциллографа и в последующем является шаблоном в алгоритме восстановления. В [15] приведены схема проведения эксперимента и алгоритм по восстановлению сигнала от клавиатуры USB. В ходе проведения настоящего исследования в лаборатории, был использован анализатор сигналов Keysight N9020B MXA и измерительная гибридная антенна АИГ–12М. Иванов А.В. в своей работе [16] выделяет требования к измерению параметров ПЭМИ. Существующее решение [17] позволяет производить процесс корреляции времени, которое используется для автоматического обнаружения ПЭМИ клавиатуры. Анализ возможности аутентификации по клавиатурному почерку на основе ПЭМИ при использовании других типов подключения клавиатуры (Bluetooth, WiFi, PS/2) берет начало в исследованиях Vuagnoux M. и Pasini S. [18].

Современные подходы к аутентификации пользователя на основе клавиатурного почерка

Динамика нажатия клавиш делится на два основных класса: фиксированный текст и свободный текст [19]. Существующая методика аутентификации по фиксированному тексту, в основе которой лежит формирование шаблона клавиатурного почерка (например, при входе в систему требуется ввод пароля), не позволяет в течение всего учетного времени работы за компьютером проводить анализ угроз нарушителей конфиденциальной информации. Вследствие этого, применение методики анализа клавиатурного почерка по свободному тексту имеет преимущество, которое заключается в непрерывном контроле за законным оператором информационной системы.

В анализе исследований [20] приводится пример редактирования текста разными способами. Было отмечено, что операторы используют различные комбинации клавиш при удалении текста: Backspace, Delete Keys, вставка и перемещение слов и символов также могут выполняться различными способами: Вставка (Insert), клавиша быстрого вызова или Правка (Edit) – Вставка (Paste), способ набора заглавных букв с зажатой клавишей Shift, либо включением Caps Lock, набор цифр на клавиатуре с помощью дополнительной клавиатуры, либо с применением символьных клавиш.

Рассмотренная возможность применения искусственной нейронной сети обратного распространения в структуре аутентификации пользователя [21] создает перспективы для совершенствования системы анализа динамики нажатия клавиш в области радиомониторинга. Нейронные сети позволяют давать оценку параметрам клавиатурного почерка при различных условиях, при этом не требуется наличие точных знаний о всех вносящих вклад переменных и их отношений в отличие от математических моделей. Нейронная сеть обратного распространения позволяет решать сложные задачи с относительно компактной сетевой структурой [22].

Выводы

Приведенные в данной работе исследования нацелены на оценку возможности обнаружения зависимости появления информационного сигнала от клавиатуры в радиозоне и реализацию проведения аутентификации оператора, на основании анализа временных характеристик динамики нажатия клавиш. В представленной работе проводится анализ возможности аутентификации оператора с использованием стандартной USB клавиатуры. Дальнейшие исследования в этой области планируется проводить с беспроводными клавиатурами, клавиатурой с интерфейсом PS/2, а также клавиатурой ноутбука.

Достоверность предлагаемого научного решения состоит в совокупном анализе индексируемых литературных источников по теме исследования и практической работой на базе испытательной лаборатории предприятия в направлении исследования

Литература

1. Шатунов А.В., Ченцов В.А. Подход к предотвращению инсайдерских утечек информации. Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019. С. 380-386.
2. Грижебовская А.Г., Михалев А.В. Биометрический метод идентификации человека по сосудистому рисунку пальца // Вопросы кибербезопасности. 2019. № 5 (33). С. 51-56.
3. Савинов А.В. Методы, модели и алгоритмы распознавания клавиатурного почерка в ключевых системах: дис. канд. техн. наук: 05.13.19. / Поволжский государственный технологический университет. – Санкт-Петербург, 2013. С. 17.
4. Соколов Р.И. Исследование алгоритмов обработки сигналов для обнаружения и восстановления информативных данных из побочного электромагнитного излучения USB клавиатур: дис. канд. техн. наук: 05.12.13. / Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. – Екатеринбург, 2016. С. 45-52.
5. Ложников П.С., Сулавко А.Е., Бурая Е.В., Писаренко В.Ю. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица // Вопросы кибербезопасности. 2017. № 3 (21). С. 24-34.
6. Крутохвостов Д.С., Хиценко В.Е. Парольная и непрерывная аутентификация по клавиатурному почерку средствами математической статистики // Вопросы кибербезопасности. 2017. № 5 (24). С. 91-99.
7. Чиликов А.А., Яковлев А.Н. Информационная безопасность и цифровая криминалистика: проблемы, решения и новые вызовы. Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019. С. 361-366.
8. Kubiak I., Boitan A., Halunga S. Assessing the Security of TEMPEST Fonts against Electromagnetic Eavesdropping by Using Different Specialized Receivers. Appl. Sci. 2020, 10, 2828. <https://doi.org/10.3390/app10082828>.
9. Kubiak I., Przybysz A. The Effectiveness of TMDS Coding in Counteracting the Non-Invasive Acquisition of Graphic Data. Electronics 2019, 8, 1063. <https://doi.org/10.3390/electronics8101063>.
10. Boitan A., Kubiak I., Halunga S., Przybysz A., Stanczak A. Method of Colors and Secure Fonts Used for Source Shaping of Valuable Emissions from Projector in Electromagnetic Eavesdropping Process. Symmetry 2020, 12, 1908. <https://doi.org/10.3390/sym12111908>.
11. Sun S., Zhang H., Cui X., Dong L., Khan M.S., Fang X. Multibyte Electromagnetic Analysis Based on Particle Swarm Optimization Algorithm. Appl. Sci. 2021, 11, 839. <https://doi.org/10.3390/app11020839>.
12. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. Учебник для вузов, М.: Горячая линия – Телеком, 2019, 444 с.
13. Кобяков В.Ю., Лучинин А.С. Обнаружение ПЭМИ проводников и коннекторов при передаче по интерфейсу USB // Вестник УрФО. Безопасность в информационной сфере. 2014 № 4(14). С. 4-8.
14. Dong-ju S., Ho Seong L., Jong-Gwan Y., Kyuhong S. Measurement and Analysis of the Compromising Electromagnetic Emanations from USB Keyboard. In 2016 Asia-Pacific International Symposium on Electromagnetic Compatibility, APEMC 2016. Institute of Electrical and Electronics Engineers Inc., 2016, pp. 518-520.
15. Hyo-Joon C., Ho Seong L., Dongjoo S., Jong-Gwan Y., Kyuhong S. Reconstruction of Leaked Signal from USB Keyboards. 2016 URSI Asia-Pacific Radio Science Conference, 2016, pp. 1281-1283.
16. Иванов А.В. Оценка защищенности информации от утечек по каналам побочных электромагнитных излучений и наводок: учебное пособие / А.В. Иванов. – Новосибирск: Изд-во НГТУ, 2018. – 64 с.
17. Boitan A., Bartusica R., Halunga S., Popescu M., Ionuta I. Compromising Electromagnetic Emanations of Wired USB Keyboards. ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2018, pp. 39-44.
18. Vuagnoux M., Pasini S. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. SSYM'09: Proceedings of the 18th conference on USENIX security symposium, 2009,

pp. 1-16.

19. Alsultan A., Warwick K. Keystroke Dynamics Authentication: A Survey of free-text methods, International Journal of Computer Science Issues, 2013, pp. 1-10.

20. Alsultan A., Warwick K., Wei H. Non-Conventional Keystroke Dynamics for User Authentication. Pattern Recognition Letters, 2017, pp. 53-59.

21. Казанцев И.С. Защита информации в системах критически важных объектов, созданная на основе анализа клавиатурного почерка с использованием нейронной сети обратного распространения. Тезисы докладов 74-ой Международной молодежной научной конференции «Нефть и газ - 2020» – М.: РГУ нефти и газа им И.М. Губкина, 2020, С. 346-347.

22. Chandrasekar V. User authentication based on Hausdroff distance in keystroke dynamics using memetic algorithms. International Journal of Pure and applied Mathematics, Vol-118, 2018, pp. 117-125.

Научный руководитель: Басараб Михаил Алексеевич, доктор физико-математических наук, доцент, заведующий кафедрой «Информационная безопасность» МГТУ им. Н.Э. Баумана, basarab@bmstu.ru.

On a possible approach to user authentication using keyboard handwriting based on TEMPEST keyboard

Kazantsev I.S.⁸⁵

Abstract. *A combined analysis of modern research in the field of compromising electromagnetic radiation emanations from the standard USB interface keyboard and keystroke speaker authentication methods is presented. A relationship was identified between the occurrence of the signal spectrum in the radio broadcast and the frequency of typing on the keyboard. These studies were conducted with the aim of improving approaches to user authentication, creating a receiving software and hardware key, and will also be of interest in the field of computer forensics.*

Keywords: *compromising electromagnetic emanations, authentication, keystroke dynamics.*

⁸⁵ Kazantsev Ivan Sergeevich, post-graduate student, Bauman Moscow State Technical University, Moscow, kazantsevivan1991@mail.ru

О криптографических алгоритмах, основанных на обобщенных клеточных автоматах, и перспективах их применения

Ключарёв П.Г.⁸⁶

Аннотация. Работа посвящена криптографическим алгоритмам, основанным на обобщенных клеточных автоматах, разработанным автором за последние годы. Кратко описываются обобщенные клеточные автоматы, кратко говорится о разработанных на их основе алгоритмах блочного шифрования, поточного шифрования и криптографических хэш-функциях, приводятся данные по производительности этих алгоритмов при реализации на ПЛИС, рассматриваются некоторые перспективы их применения. Оказывается, что алгоритмы из построенных семейств обладают как высокой производительностью при аппаратной реализации, так и низкими требованиями к аппаратным ресурсам. Все это делает их применение весьма перспективным.

Ключевые слова: обобщенные клеточные автоматы, криптоалгоритм, блочный шифр, хэш-функция.

Введение

За последние несколько лет автором была разработана теоретическая база для построения высокопроизводительных криптографических алгоритмов, основанных на обобщенных клеточных автоматах. На основе разработанных теоретических положений автором были построены семейства алгоритмов поточного шифрования (GRACE-S) [1], алгоритмов блочного шифрования (GRACE-B) [2] и два семейства криптографических хэш-функций (GRACE-H [3] и GRACE-H2 [4]).

Обобщенные клеточные автоматы

Алгоритмы, о которых идет речь в настоящей работе, построены на основе обобщенных клеточных автоматов. Обобщенный клеточный автомат представляет собой ориентированный граф, каждой вершине v_i которого соответствует булева переменная m_i (будем называть ее ячейкой) и булева функция $f_i(x_1, \dots, x_{d_i})$, называемая локальной функцией связи этой вершины (заметим, что здесь и далее мы употребляем термин «граф», допуская наличие петель и кратных ребер). При этом для вершины v_i , входящие в неё ребра пронумерованы числами $1 \dots d_i$, соответствующими номеру аргумента локальной функции связи. Обобщенный клеточный 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 $(m_1(t), m_2(t), \dots, m_N(t))$, где N – число вершин.

В рассматриваемых алгоритмах применяются только неориентированные регулярные графы (т.е. можно считать, что неориентированное ребро $\{u, v\}$ соответствует паре ориентированных ребер (u, v) и (v, u)), а все локальные функции связи одинаковы. Впервые использовать подобные автоматы в криптографии (для построения генераторов

⁸⁶ Ключарёв Петр Георгиевич, к.т.н., МГТУ им. Н.Э. Баумана, г. Москва, pk.iu8@yandex.ru

псевдослучайных последовательностей) было предложено Б.М. Сухининым (см., например, работу [5], где они назывались неоднородными клеточными автоматами).

Особенности алгоритмов, основанных на обобщенных клеточных автоматах

Семейства криптографических алгоритмов GRACE отличаются тем, что графами лежащих в их основе обобщенных клеточных автоматов, являются графы Рамануджана. Одним из примеров семейства таких графов, подходящих для использования в обобщенных клеточных автоматах, являются графы изогений суперсингулярных эллиптических кривых [6], называемые также графами Пайзера (т.к. Пайзер доказал, что изоморфные им графы являются графами Рамануджана [7]). Множеством вершин такого графа является множество классов изоморфизма суперсингулярных эллиптических кривых над конечным полем определенного порядка, а ребрами – изогении между представителями этих классов (напомним здесь, что изогенией между эллиптическими кривыми называется морфизм, сохраняющий точку в бесконечности [8]). Графы изогений суперсингулярных эллиптических кривых интересны также тем, что они используются в постквантовых протоколах обмена ключами [9].

Другим примером графов Рамануджана, подходящих для использования в обобщенных клеточных автоматах, являются графы $Y^{p,q}$ Любоцкого-Филипса-Сарнака [10]. Смысл использования графов Рамануджана в обобщенных клеточных автоматах в том, что такие графы, имея логарифмический относительно числа вершин диаметр, позволяют добиться отличных показателей лавинного эффекта. Кроме того, по целому ряду свойств такие графы близки к случайным регулярным графам (а случайный регулярный граф с большой вероятностью является графом Рамануджана).

Локальные функции связи обобщенных клеточных автоматов выбираются специальным образом, исходя из ряда теоретических соображений. Функция нумерации ребер η также выбирается исходя из ряда теоретических соображений. Соображения эти изложены в ряде статей автора и позволяют обеспечить высокий уровень криптографической стойкости.

Основой алгоритмов блочного шифрования GRACE-B и хэш-функций GRACE-H и GRACE-H2 являются псевдослучайные функции-кандидаты, представляющие собой, по существу, преобразование, выполняемое обобщенным клеточным автоматом за определенное число шагов – аргумент функции подается на определенное подмножество ячеек в начальный момент времени, а после окончания работы значение функции снимается с определенных ячеек. Например, в блочных шифрах GRACE-B такая функция используется как раундовая функция в схеме Фейстеля, служа одновременно и для смешивания с ключом (на ячейки обобщенного клеточного автомата, перед началом его работы, подается подблок, раундовый ключ и некоторая константа).

Производительность и перспективы применения криптографических алгоритмов, основанных на обобщенных клеточных автоматах

Все обсуждаемые криптографические алгоритмы предназначены, прежде всего, для аппаратной реализации. Были проведены эксперименты (результаты некоторых из которых опубликованы в ряде работ автора) по реализации их на ПЛИС. При реализации на ПЛИС Altera Stratix V, алгоритмы семейства GRACE-S показали производительность, превышающую 1100 Гбит/с, что более чем в 50 раз выше, чем производительность, например, алгоритма Trivium. Алгоритмы блочного шифрования GRACE-B показали на ПЛИС производительность до 53 Гбит/с, что приблизительно в 2.5 раза превышает производительность лучших аппаратных реализаций алгоритма AES. Производительность при реализации на ПЛИС криптографических хэш-функций GRACE-H достигла 198 Гбит/с, а GRACE-H2 – превысила 130 Гбит/с.

Подобные скорости работы позволяют использовать построенные алгоритмы в аппаратных средствах, обеспечивающих шифрование информации, передаваемой в

современных компьютерных сетях. Так, алгоритмы поточного шифрования из семейства GRACE-S могут найти применение в аппаратных средствах криптографической защиты информации, предназначенных для применения в компьютерных сетях недавно принятых стандартов IEEE 802.3bs–2017 и IEEE 802.3ck–2020, функционирующих на скоростях 400 и 800 Гбит/с, соответственно.

Другая область применения таких алгоритмов – это сети вычислительных устройств с ограниченными вычислительными ресурсами (такие, как Internet of Things). Как показали эксперименты, алгоритмы семейства GRACE могут быть эффективно реализованы аппаратно для устройств с ограниченными аппаратными вычислительными ресурсами.

Кроме того, криптографические алгоритмы из семейств GRACE могут найти широкое применение в различных распределенных вычислительных системах (например, изучаемых в работах [11, 12]), а также в системах спутниковой связи.

Заключение

Семейства GRACE алгоритмов поточного шифрования, алгоритмов блочного шифрования и криптографических хэш-функций, основанных на обобщенных клеточных автоматах, при аппаратной реализации позволяют достичь высоких скоростей обработки информации, а также обеспечить низкие требования к вычислительным ресурсам, что делает весьма перспективным их использование как в высокоскоростных компьютерных сетях, так и в сетях устройств с ограниченными вычислительными ресурсами.

Литература

1. Ключарёв П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей. // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2011 - №10. Режим доступа: <http://technomag.edu.ru/doc/241308.html>
2. Ключарёв П. Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. - 2012. - № 12. С. 361-374. Режим доступа: <http://technomag.edu.ru/doc/517543.html>
3. Ключарёв П. Г. Криптографические хэш-функции, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. - 2013. - № 1. С.161-172. Режим доступа: <http://technomag.edu.ru/doc/534640.html>
4. Ключарёв П. Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности, 2017, №1 (19), С.45-50.
5. Сухинин Б.М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2010, №9.
6. Charles D. X., Lauter K. E., Goren E. Z. Cryptographic hash functions from expander graphs //Journal of CRYPTOLOGY. – 2009. – Т. 22. – №. 1. – С. 93-113.
7. Pizer A.K. Ramanujan graphs and Hecke operators // Bull. Amer. Math. Soc. 1990. V.23.
8. Silverman J. H. The arithmetic of elliptic curves. – Springer Science & Business Media, 2009.
9. De Feo L., Jao D., Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies //Journal of Mathematical Cryptology. – 2014. – Т. 8. – №. 3. – С. 209-247.
10. Sarnak P. Some Applications of Modular Forms. Cambridge University Press, 1990.
11. 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.
12. Быков А.Ю., Панфилов Ф.А., Ховрина А.В. Алгоритм выбора классов защищенности для объектов распределенной информационной системы и размещения данных по объектам на основе приведения оптимизационной задачи к задаче теории игр с непротивоположными интересами // Наука и образование. Научное издание МГТУ им. Н.Э. Баумана. - 2016. - № 1. С. 90-107.

Cryptographic algorithms based on generalized cellular automata and their possible applications

Klyucharev P.G.⁸⁷

Abstract. *The paper is devoted to cryptographic algorithms based on generalized cellular automata, developed by the author in recent years. Generalized cellular automata are briefly described, the block ciphers, stream ciphers and cryptographic hash functions based on generalized cellular automata are briefly discussed, data on the performance of these algorithms implemented on FPGAs are provided, and a number of their possible applications are considered. It is concluded that the algorithms from the constructed families have both high performance in hardware implementation and low requirements for hardware resources. These properties make these algorithms very promising.*

Keywords: *generalized cellular automata, stream cipher, block cipher, hash function.*

⁸⁷ Peter Klyucharev, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

Модель стеганографического канала, основанного на использовании текстового стеганографического контейнера

Козачок А.В.⁸⁸, Копылов С.А.⁸⁹, Гайнов А.Е.⁹⁰, Кондратьев Б.В.⁹¹

Аннотация. В статье представлена модель стеганографического канала, основанная на текстовом стеганографическом контейнере, сформированном посредством стеганографического внедрения информации за счет изменения величин интервалов между словами. Разработанная модель позволяет описать процесс передачи информации, скрытой в напечатанном текстовом документе, по стеганографическому каналу устойчивому к преобразованию формата электронного текстового документа в изображение, содержащее текст. В ходе разработки модели проведен анализ особенностей представления электронных текстовых документов, определены требования и ограничения, предъявляемые к текстовому стеганографическому контейнеру. Представлено описание текстового стеганографического контейнера, а также основных параметров его характеризующих. Определены направления дальнейших исследований.

Ключевые слова: стеганография, маркирование текстовых документов, стеганографический контейнер, математическое моделирование.

Введение

Разработка и совершенствование средств защиты информации от угрозы несанкционированного копирования, распространения и утечки в последние десятилетия остается одним из наиболее актуальных направлением исследований. По данным аналитического центра InfoWatch за девять месяцев 2020 года зарегистрировано 1773 случая утечки конфиденциальной информации⁹². Одним из типов данных, подвергшихся компрометации выступают текстовые документы, подготовленные к печати. Помимо утечки физических копий текстовых документов за пределы контролируемого периметра, отмечается утечка электронных версий напечатанных на бумаге текстовых документов, которая реализуется посредством сканирования или фотографирования напечатанного на бумаге документа с последующей отправкой полученного изображения⁹³.

В современных средствах защиты текстовой информации описанному каналу утечки не уделяется должного внимания. Для решения указанной задачи разработан подход к маркированию текстовых электронных документов, основанный на стеганографическом подходе к внедрению за счет изменения величин интервалов между словами. Маркирование текстовых документов реализуется посредством внедрения в электронный текстовый документ, выводимый на печать, информации позволяющей однозначно идентифицировать исполнителя и степень конфиденциальности исходного документа. Для оценки возможности использования разработанного подхода в процессе защиты от утечки посредством перцептивно невидимого внедрения идентификационной информации в текстовый документ, выводимый на печать необходимо рассмотреть особенности формирования и использования текстовых стеганографических контейнеров для стеганографических систем [1-6].

⁸⁸Козачок Александр Васильевич, д.т.н., Академия ФСО России, Орёл, a.kozachok@academ.msk.rsnet.ru

⁸⁹Копылов Сергей Александрович, Академия ФСО России, Орёл, gremlin.kop@mail.ru

⁹⁰Гайнов Артур Евгеньевич, Министерство обороны Российской Федерации, Москва, gae@mil.ru

⁹¹Кондратьев Борис Владимирович, Министерство обороны Российской Федерации, Москва, gae@mil.ru

⁹² www.infowatch.ru/analytics/reports/30708

⁹³ www.infowatch.ru/analytics/digest/15511

1. Особенности текстовых стеганографических контейнеров

Под стеганографическим контейнером (стегано-контейнером, стего-контейнером) понимается контейнер, содержащий встраиваемую информацию. Стеганографический контейнер формируется из исходного файла-контейнера (контейнера) посредством стеганографического внедрения информации и представляет собой видоизмененный контейнер, полностью соответствующий типу данных оригинала.

Файл-контейнер (контейнер) представляет собой данные, используемые для сокрытия в них сообщений (информации) [7]. В зависимости от типа данных контейнеры могут быть разделены на: текстовый, графический, аудио, видео или звуковой [8]. Встраиваемая информация, в свою очередь, может быть представлена последовательностью бит, текстовым документом либо файлами мультимедиа (изображение, видео или аудио данные) [9].

В зависимости от размера контейнеры делятся на потоковый и фиксированный [10]. Потоковый контейнер представляет собой непрерывно следующую последовательность бит (информации). Отличительной особенностью потоковых контейнеров является возможность встраивания одновременно нескольких исходных последовательностей. В отличие от потокового контейнера, размеры и характеристики фиксированного контейнера заранее известны. К фиксированным контейнерам относятся электронные текстовые документы, изображения, аудио и видео данные, ввиду того, что размер и параметры файлов представляют собой постоянную величину.

Исходя из того, что в разработанном подходе к маркированию в качестве контейнера выступают текстовые документы, представленные в электронном виде, вне зависимости от используемого типа данных, стеганографический контейнер может быть охарактеризован как текстовый, фиксированный. Для разработки модели стеганографического канала, основанного на использовании текстового стеганографического контейнера устойчивого к преобразованию формата необходимо рассмотреть основные параметры электронных текстовых документов.

В ГОСТ Р 7.0.8–2013 под электронным документом понимается документ, информация которого представлена в электронной форме⁹⁴. При этом в ГОСТ 2.105–2019 приводится следующее определение текстового документа: текстовый документ – документ, содержащий в основном сплошной текст или текст, разбитый на графы⁹⁵. Исходя из представленных определений и отсутствия в нормативной документации определения электронного текстового документа, под последним будем понимать документ, содержащий сплошной текст, текст, разбитый на графы, а также другую текстовую информацию, представленную в электронной форме.

Электронные текстовые документы могут быть разделены на документы, предназначенные для распечатки на бумаге и документы, которые будут использоваться только в электронном виде (подготавливаемые для визуального восприятия) [11]. Ввиду того, что в разработанном подходе к маркированию осуществляется внедрение информации в текстовые документы, выводимые на печать, параметры электронных текстовых документов, подготовленных для визуального восприятия, в процессе маркирования не рассматриваются.

Параметры электронных текстовых документов, подготовленных к печати, характеризуются особенностями устройств вывода информации на печать и могут быть представлены [12, 13]:

- размером печатного листа A ;
- полями (размерами) текстового пространства M ;
- величинами типографических элементов F .

⁹⁴ ГОСТ Р 7.0.8–2013. Делопроизводство и архивное дело. Термины и определения.

⁹⁵ ГОСТ Р 2.105–2019: ЕСКД. Общие требования к текстовым документам

В качестве размера печатного листа выступают значения следующих элементов: формат бумаги и ориентация листа. В качестве используемого формата могут применяться следующие форматы: описанные в ISO 216⁹⁶ – A3 (297x420 мм), A4 (210x297 мм), A5 (148x210 мм), а также – в североамериканском стандарте – Letter (216x280 мм). Ориентация текстового документа допускается: вертикальна (книжная) или горизонтальная (альбомная).

Под полями (размерами) m текстового пространства понимают величины полей текстового документа (верхнее, нижнее, левое и правое), границ текста (ширина текста, высота текста), колонтитулов и отступов от колонтитулов. Типографическими элементами текста являются следующие характеристики: используемая гарнитура G и кегль шрифта γ , величины интервалов и отступов.

В соответствии с ГОСТ Р 7.0.97-2016 текстовые электронные документы должны оформляться согласно следующих требований⁹⁷:

- используемый формат бумаги: A4 (210x297 мм) или A5 (148x210 мм);
- поля каждого листа документа должен иметь размеры не менее: 20 мм – левое, 10 мм – правое, 20 мм – верхнее, 20 мм – нижнее;
- необходимо использование свободно распространяемых бесплатных шрифтов с размером кегля 12, 13, 14 пт;
- абзацный отступ – 1,25 см;
- межстрочный интервал – 1-1,5 межстрочных интервала;
- интервал между буквами в словах – обычный.

На основе рассмотренных особенностей создания электронных текстовых документов и требований, предъявляемых к оформлению разработана модель стеганографического канала, основанного на использовании текстового стеганографического контейнера, устойчивого к преобразованию формата.

2. Модель стеганографического канала, основанного на использовании текстового стеганографического контейнера, устойчивого к преобразованию формата

В общем виде стеганографическая система (стего-система) может быть рассмотрена как система связи (передачи данных) и представлена как стеганографический канал (канал системы связи) (рис. 1) [14].

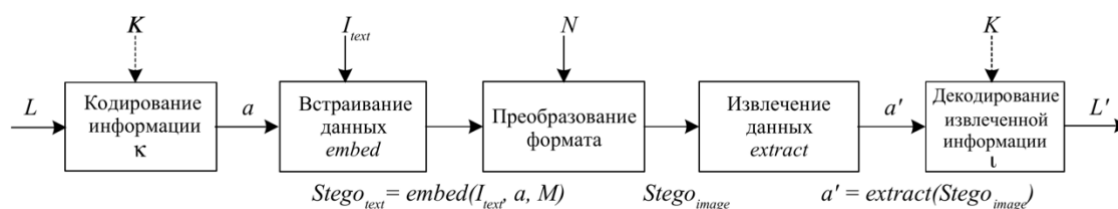


Рис.1. Модель стеганографического канала

На рисунке 1 представлена обобщенная модель стеганографического канала (стего-системы), использующей в качестве контейнера текстовые документы. Процесс передачи скрываемой информации в представленном стеганографическом канале состоит из следующих этапов [6]:

- 1) кодирование встраиваемой информации;

⁹⁶ ISO 216:2007 Writing paper and certain classes of printed matter – Trimmed sizes – A and B series, and indication of machine direction.

⁹⁷ ГОСТ Р 7.0.97–2016: Организационно-распорядительная документация. Требования к оформлению документов.

- 2) формирование стеганографического контейнера (встраивание данных в контейнер);
- 3) преобразование формата стеганографического контейнера;
- 4) обнаружение и извлечение данных из преобразованного стеганографического контейнера;
- 5) декодирование извлеченной информации.

Введем следующие обозначения: W – множество возможных встраиваемых комбинаций ($a, a' \in W$), K – множество ключей ($K \in K$), I – множество текстовых контейнеров ($I_{text} \in I$), L – множество встраиваемых сообщений ($L, L' \in L$), N – множество воздействий оказываемых на стеганографический контейнер в процессе преобразования формата.

Математическая модель представленной стеганографической системы может быть описана следующим образом:

- 1) процесс кодирования встраиваемой информации описывается как:

$$a = \kappa(K, L), \quad (1)$$

где κ – функция, осуществляющая кодирование встраиваемой информации L .

В процессе формирования РВЗ для повышения защищенности встроенных данных используется секретный ключ K . Под секретным ключом понимается используемый подход к внедрению за счет изменения интервалов между словами. В качестве секретного ключа K выступают сам алгоритм встраивания и величины изменения интервалов между словами.

В процессе кодирования встраиваемой информации на функцию κ накладывается требование по инвариантности встроенных данных к внесению искажений и применению различных преобразований $\kappa(K, L) = \kappa(K, L')$, где $L' = L + \varepsilon$. К возможным искажениям и преобразованиям ($\varepsilon \in N$) данных могут быть отнесены: геометрические искажения контейнера, преднамеренные атаки и другие воздействия (в том числе легитимные), которые способны исказить исходное представление контейнера. Для повышения робастности встроенных данных на этапе кодирования встраиваемой информации могут применяться методы помехоустойчивого кодирования.

- 2) процесс формирования стеганографического контейнера $Stego_{text}$ (встраивание данных в контейнер) описывается функцией $embed$:

$$Stego_{text} = embed(I_{text}, a, M), \quad (2)$$

где M – маска встраивания, учитывающая характеристики зрительной системы человека, предназначена для уменьшения заметности встроенных данных.

Встроенные в текстовый документ данные должны обеспечивать инвариантность к преобразованию формата, обусловленного применением операции "печать–сканирование" ("печать–фотографирование"), а также к заранее определенным или ко всем существующим воздействиям, которым может быть подвержен стеганографический контейнер.

Под процессом преобразования формата текстового стеганографического контейнера $Stego_{image} = tr(Stego_{text}, N)$ (tr – процесс преобразования формата) понимается изменение формата представления исходного текстового документа в изображение, содержащее текст. К преобразованию tr относятся операции "печать–сканирование" ("печать–фотографирование") электронного текстового документа, а также сопутствующие легитимные воздействия, которые могут быть осуществлены в процессе указанного преобразования.

- 4) процесс извлечения данных из преобразованного стеганографического контейнера описывается:

$$a' = extract(Stego_{image}), \quad (3)$$

где $\text{Stego}_{\text{image}}$ – цифровое изображение (стеганографический контейнер), содержащее встроенные данные.

В случае обеспечения требования по инвариантности встроенных данных к преобразованию формата, а также сопутствующих легитимных воздействий на стего-контейнер, результат извлечения из электронного текстового документа $a = \text{extract}(\text{Stego}_{\text{text}})$ и результат извлечения из изображения, содержащего текст $a' = \text{extract}(\text{Stego}_{\text{image}})$, должны быть одинаковыми: $a' = a$, при условии $\text{Stego}_{\text{image}} \neq \text{Stego}_{\text{text}}$.

5) процесс декодирования извлеченной информации описывается следующим образом:

$$L' = \iota(a', K). \quad (4)$$

В случае соблюдения требования по инвариантности скрываемых данных к возможным преобразованиям в процессе кодирования встраиваемой информации $\kappa(K, L) = \kappa(K, L')$ результат извлечения встроенных данных примет вид:

$$L' = \iota(a', K) = \iota(a, K) = L. \quad (4)$$

В качестве встраиваемой информации L может выступать информация, определяющая метку конфиденциальности исходного текстового документа, а также идентификационная информация, характеризующая пользователя и данные, содержащиеся в тексте документа:

- идентификатор исполнителя (владельца) документа;
- дата создания (модификации) документа;
- идентификатор ЭВМ, на которой обрабатывался документ;
- контрольная сумма (для контроля целостности данных).

Выводы

Представленная модель стеганографического канала, основанного на использовании текстового стеганографического контейнера, устойчивого к преобразованию формата, позволяет описать основные характеристики разработанной стеганографической системы, а также оценить влияние параметров встраивания и процесса внедрения и извлечения информации на конечное значение робастности встроенных данных к осуществлению преобразования формата текстовых документов посредством операции "печать–сканирование" или "печать–фотографирование". Для экспериментальной оценки и моделирования разработанного подхода к маркированию необходимо разработать и реализовать алгоритм маркирования электронных текстовых документов за счет изменения величин интервалом между словами. Решение поставленной задачи является направлением дальнейших исследований.

Литература

1. Макаренко С.И. Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии//Вопросы кибербезопасности. 2014. № 2 (3). С. 24-32.
2. Математические основы информационной безопасности/Басараб М.А., Булатов В.В., Булдакова Т.И., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г., Медведев Н.В., Троицкий И.И., Чичварин Н.В. и др.: Под ред. Матвеева В.А. -М.: НИИ РИЛ МГТУ им.Н.Э.Баумана, 2013. -244 с.
3. Мироненко А.Н., Величко М.Д. Метод применения (t, n)-пороговой схемы в стеганографии. В сборнике: Безопасные информационные технологии. Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 302-307.

4. Сивачев А.В., Прохожев Н.Н., Михайличенко О.В., Башмаков Д.А. Эффективность стеганоанализа на основе методов машинного обучения // Вопросы кибербезопасности. 2017. № 2 (20). С. 53-60.
5. Шниперов А.Н., Прокофьева А.В. Метод стеганоанализа статических изображений формата jpeg на основе искусственных иммунных систем // Вопросы кибербезопасности. 2020. № 2 (36). С. 22-31.
6. Evsutin O., Shelupanov A., Kokurina A., Shumskaya O., Kozachok A. Approach to increase in efficiency of information embedding into a phase spectrum of the discrete fourier transformation due to minimization of quantity of changeable frequency coefficients // CEUR Workshop Proceedings. conference proceedings. 2017. С. 54-58.
7. Стеганография, цифровые водяные знаки и стеганоанализ / А. В. Аграновский [и др.] // Москва : Вузовская книга. 2009. 220 с.
8. Anderson R., Pfitzmann B. Information Hiding Terminology // Information Hiding: Proceedings of First International Workshop, Cambridge, UK, May 30 June 1. 1996. Vol. 1. pp. 347-350.
9. Petitcolas F., Anderson R., Kuhn M. Information Hiding – A Survey // Proceedings of the IEEE, Special issue on protection of multimedia content. 1999. № 87 (7). pp. 1062–1078.
10. Грибунин В. Г., Оков И.Н., Туринцев И.В. Цифровая стеганография // Москва : СОЛОН-Пресс. 2017. 262 с.
11. Brogain S.O. Typographic measurement: A critique and a proposal // Journal of the Institute of Printing. 1983. Vol. 12, № 5. pp. 9–14.
12. Шрифты. Разработка и использование / Г. М. Барышников [и др.] // Москва : Издательство ЭКОМ. 1997. 288 с.
13. Rello L., Baeza-Yates R. Good fonts for dyslexia // Proceedings of the 15th international ACM SIGACCESS conference on computers and accessibility. 2013. pp. 1–8.
14. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и Практика // Киев : МК-Пресс. 2006. 288 с.

Steganographic channel model based on text steganographic container

Kozachok A.V.⁹⁸, Kopylov S.A.⁹⁹, Gaynov A.E.¹⁰⁰, Kondrat'ev B.V.¹⁰¹

Abstract. *The article presents a steganographic channel model based on a text steganographic container formed by steganographic information embedding through interword spacing values changing. The developed model makes it possible to describe the process of transmitting information hidden in a printed text document over a steganographic channel that is robust to format converting of an electronic text document into an image containing text. In the course of developing the model, the features analysis of electronic text documents presentation was carried out, the requirements and restrictions for the text steganographic container were determined. The description of the text steganographic container, as well as the main parameters characterizing it, is presented. The further research directions are determined.*

Keywords: *steganography, documents marking, steganographic container, mathematical modeling.*

⁹⁸Kozachok Alexander Vasilevich, Dr. Sc., Academy of Federal Guard Service, Oryol, a.kozachok@academ.msk.rnet.ru

⁹⁹Kopylov Sergey Alexandrovich, Academy of Federal Guard Service, Oryol, gremlin.kop@mail.ru

¹⁰⁰Gaynov Arthur Evgenevich, Ministry of Defence of the Russian Federation, Moscow, gae@mil.ru

¹⁰¹Kondrat'ev Boris Vladimirovich, Ministry of Defence of the Russian Federation, Moscow, gae@mil.ru

Многоуровневая модель политики безопасности управления доступом операционных систем семейства Windows

Козачок А.В.¹⁰², Кочетков Е.В.¹⁰³

Аннотация. Целью исследования является совершенствование механизма разграничения доступа в семействе операционных систем Windows для защиты от скрытых каналов утечки информации по памяти. Результатом исследования является набор структур многоуровневой модели, отражающий атрибуты, значимые для моделирования процесса доступа субъектов к объектам; моделирование ключевых механизмов разграничения доступа в операционной системе: управление пользователями, группами, субъектами, объектами, ролями, правами, дискреционное и мандатное управление доступом, мандатный контроль целостности – многоуровневое управление доступом субъектов к объектам; определение механизма контроля создания субъектов на основе исполняемых файлов для организации изолированной программной среды; определение инвариантов корректности переменных в процессе верификации и безопасного доступа субъектов к объектам.

Ключевые слова: информационная безопасность, несанкционированный доступ, модели безопасности, верификация, моделирование, темпоральная логика.

Введение

Основной технической мерой защиты от функционирования вредоносных программ являются средства антивирусной защиты. Эксперименты по оценке их эффективности показывают близкую к нулю вероятность пропуска цели. Однако даже при достаточно высокой вероятности обнаружения существует непустое множество вредоносных программ, оставшихся необнаруженными, что создает непосредственную угрозу деструктивного программного воздействия, что особенно актуально для объектов критической информационной инфраструктуры (КИИ).

Достижение принципиальной невозможности функционирования вредоносных программ вероятностными методами обнаружения, такими как сигнатурный или эвристический, невозможно. Вследствие высокого потенциального ущерба, вызванного нарушением штатного режима функционирования объекта КИИ, на таких объектах необходимым является применение формальных методов защиты от вредоносных программ.

В этом случае одним из решений является автоматическая формальная верификация модели политики безопасности управления доступом методом Model checking, который является математически обоснованным способом доказательства того, что модель соответствует заданной для нее спецификации [1, 2] с использованием инструментальных средств [3, 4].

Актуальность проблемы разработки формальных моделей политик безопасности управления доступом также связана с внедрением ФСТЭК России «Требований безопасности информации к операционным системам», в частности выполнение требований функциональной компоненты ADV_SPM.1 «Формальная модель политики безопасности» [5].

Для семейства операционных систем Linux решение подобной задачи рассмотрено в работах [6-8].

Определение структур модели

Состояние модели определяется набором значений каждого элемента из следующих переменных:

¹⁰² Козачок Александр Васильевич, д-р техн. наук, Академия ФСО России, Орёл, a.kozachok@academ.msk.rsn.ru

¹⁰³ Кочетков Евгений Викторович, Академия ФСО России, Орёл, mr.koch91@mail.ru

- множество доступов A ;
- множество объектов доступа O ;
- множество субъектов доступа S ;
- множество пользователей U ;
- множество групп пользователей G .

При определении структур модели с использованием TLA+ отсутствует строгая типизация (по умолчанию производится проверка только встроенных типов), однако, проверка инвариантов типов является неотъемлемой частью спецификации, поскольку верификация производится методом Model Checking.

Проведение верификации на множестве элементов близком к реальному приведет к существенному увеличению количества возможных состояний, что существенно замедлит процесс исследования. Ряд значений, заданных в модели, являются модельными для снижения ресурсоемкости процесса верификации, но не влияют на общность и адекватность модели в целом [9, 10].

Множества идентификаторов процессов, контейнеров, файлов и пользователей (значения модельные):

$$\begin{aligned} UserIDs &\triangleq 0..2 \\ GroupIDs &\triangleq 0..2 \\ SubjectIDs &\triangleq 0..1 \\ ObjectIDs &\triangleq 0..6 \end{aligned}$$

где $UserIDs$ – множество идентификаторов пользователей; $GroupIDs$ – множество идентификаторов групп; $SubjectIDs$ – множество идентификаторов субъектов; $ObjectIDs$ – множество идентификаторов объектов.

Структура субъекта определена следующим выражением:

$$\begin{aligned} Subject \triangleq [& \\ & sid: SubjectIDs, \\ & uid: UserIDs, \\ & cl: ConfLevs, \\ & il: IntLevs, \\ & confCats: SUBSET ConfCats, \\ & intCats: SUBSET IntCats \\ &] \end{aligned}$$

где sid – идентификатор субъекта; uid – идентификатор пользователя; cl – уровень конфиденциальности субъекта; il – уровень целостности субъекта; $confCats$ – множество доступных субъекту категорий конфиденциальности; $intCats$ – множество доступных субъекту категорий целостности.

Моделирование разграничения доступа

При попытке доступа субъекта к объекту производится проверка возможности совершения такого доступа на основе дискреционного и многоуровневого контроля доступа. Доступ разрешается только если проверка по обоим механизмам контроля доступа принимает истинное значение.

Возможность совершения доступа a субъектом s по отношению к объекту o в соответствии с дискреционными правилами разграничения доступа проверяется предикатом $DACMayDo$ (выражение 1).

Предикат $DACMayDo$ принимает истинное значение в любом из следующих случаев:

- пользователь u , создавший субъект s является администратором;
- пользователь u , создавший субъект s , является владельцем объекта o ;
- существует такое правило $r \in o.aclus$, в котором на первой позиции задан идентификатор пользователя, создавшего субъект s и доступ a входит во множество разрешений данного правила;

– существует такая группа $g \in \text{SelectUserGroups}(s.\text{uid})$, в которую входит пользователь, и такое правило $r \in o.\text{aclgs}$, в котором на первой позиции задан идентификатор группы, и доступ a входит во множество разрешений данного правила.

$$\begin{aligned} \text{DACMayDo}(s, o, a) \triangleq & \\ & \vee o.\text{owner} = s.\text{uid} \\ & \vee \text{IsUserAdmin}(s) \\ & \vee \exists r \in o.\text{aclgs}: \\ & \quad \wedge r[1] = s.\text{uid} \\ & \quad \wedge a \in r[2] \\ & \vee \exists g \in \text{SelectUserGroups}(s.\text{uid}): \\ & \quad \vee \exists r \in o.\text{aclgs}: \\ & \quad \quad \wedge r[1] = \text{SelectGroup}(g).\text{gid} \\ & \quad \quad \wedge a \in r[2] \end{aligned} \quad (1)$$

Инициализация начальных значений модели

Начальное состояние системы определено из минимально необходимого набора значений на основе экспертного подхода. Множество текущих действий чтения и записи A на этапе инициализации является пустым. Для ускорения процесса верификации вводятся начальные взаимосвязанные между собой элементы множеств переменных. Пример начальных для множества субъектов представлен в таблице 1.

Таблица 1.

Атрибуты элементов множества субъектов при инициализации

Атрибут	s_0	s_1
sid	0	1
uid	0	1
cl	0	1
$confCats$	{"C1", "C2"}	{"C1"}
il	1	1
$intCats$	{"I1", "I2"}	{"I1"}

На этапе инициализации в системе заданы два субъекта s_0 и s_1 . Субъект s_0 создан пользователем с идентификатором 0. Для него заданы уровень конфиденциальности cl равный 0 и целостности il равный 1. Субъект s_0 имеет доступ к объектам категорий "C1" и "C2" по конфиденциальности и к объектам категорий "I1" и "I2" по целостности. Характеристика начальных значений субъекта s_1 аналогична s_0 с учетом значений атрибутов.

Предикаты действий

Последовательное выполнение предикатов действий в процессе верификации имитирует реальное поведение моделируемой системы. Каждый предикат действия состоит из пред- и постусловий. Предусловиями являются предикаты, выполнение которых необходимо для того, чтобы система всегда переходила в одно из множества разрешенных состояний.

Предусловия можно разделить на три группы: взаимодействующие сущности соответствуют выполняемому действию, проверка возможности заданного действия по дискреционным правилам разграничения доступа, проверка возможности заданного действия по многоуровневым правилам разграничения доступа.

Моделирование изменения некоторым субъектом s объекта o производится оператором $WriteD$ и представлено следующим выражением:

$$\begin{aligned}
WriteD \triangleq & \\
& \forall \exists s \in S: \\
& \forall \exists o \in O: \\
& \quad \wedge o.type = "file" \\
& \quad \wedge DACMayDo(s, o, "write") \\
& \quad \wedge MACMayDo(s, o) \\
& \quad \wedge Write(s, o)
\end{aligned}$$

Предусловия предиката действия *WriteD* определяют, что изменение субъектом *s* в объект *o* может быть совершено только для объектов типа «файл». В остальных случаях действие не будет совершено. Далее проверяется возможность совершения доступа согласно дискреционному и многоуровневому разграничению доступа. Если оба предиката возвращают истинное значение, то выполняется оператор *Write(s, o)*.

Постусловия для предиката действия *WriteD* представлены следующим выражением:

$$\begin{aligned}
Write(s, o) \triangleq & \\
& \forall \exists s \in S: \\
& \quad \wedge A' = A \cup \{ \langle s.sid, o.oid, "write" \rangle \} \\
& \quad \wedge UNCHANGED \langle U, G, S \rangle
\end{aligned}$$

Выполнение постусловия *WriteD* добавляет во множество совершенных доступов *A* картеж, содержащий идентификатор субъекта, идентификатор объекта и имя операции. Переменные *U, G, S* остаются неизменными.

Инварианты модели

Модель является верифицированной, если для каждого из возможных состояний системы выполняются все инварианты – глобальные свойства безопасности. На каждом шаге верификации выполнение всех инвариантов подтверждает, что все переменные находятся в допустимых доменах значений, данное состояние не является запрещенным. Инвариант представляет собой логическое выражение, включающее в себя темпоральные операторы.

При выполнении верификации важно, чтобы все переменные находились в заданных для них доменах значений. Для достижения этого требования введен инвариант *TypeInv*, заданный следующим выражением:

$$\begin{aligned}
TypeInv \triangleq & \\
& \wedge S \subseteq Subjects \\
& \wedge O \subseteq Objects \\
& \wedge U \subseteq Users \\
& \wedge G \subseteq Groups
\end{aligned}$$

Инвариант *TypeInv* не проверяет вхождение переменных из множества *A* в заданный домен значений, так как элементы картежей из множества совершенных доступов имеют различные домены значений.

В соответствии с правилами реализации многоуровневого разграничения доступа для любого состояния системы должен выполняться инвариант *MACSafety*, представленный следующим выражением:

$$\begin{aligned}
MACSafety \triangleq & \\
& \wedge \forall o \in O: \\
& \quad \vee \wedge o.type \in Containers \\
& \quad \quad \wedge \forall ch \in SelectAllChilds(o): \\
& \quad \quad \quad \wedge \vee "ccnr" \in o.ext\_attr \\
& \quad \quad \quad \quad \vee \wedge ch.cl \leq o.cl \\
& \quad \quad \quad \quad \quad \wedge \vee o.confCats = \{\} \\
& \quad \quad \quad \quad \quad \quad \vee ch.confCats \subseteq o.confCats \\
& \quad \quad \quad \wedge \vee "icnr" \in o.ext\_attr \\
& \quad \quad \quad \quad \vee \wedge ch.cl \geq o.cl \\
& \quad \quad \quad \quad \quad \wedge \vee o.intCats = \{\} \\
& \quad \quad \quad \quad \quad \quad \vee ch.intCats \subseteq o.intCats \\
& \quad \vee \wedge o.type \notin Containers \\
& \wedge \forall s \in S: \\
& \quad \wedge s.cl \leq SelectUser(s.uid).cl \\
& \quad \wedge s.confCats \subseteq SelectUser(s.uid).confCats \\
& \quad \wedge s.il \leq SelectUser(s.uid).il \\
& \quad \wedge s.intCats \subseteq SelectUser(s.uid).intCats
\end{aligned}$$

В данном инварианте происходит проверка, что для каждого объекта, если он является контейнером, должен содержаться флаг "ccnr" или "icnr" в его расширенных атрибутах, или уровни конфиденциальности и целостности вложенных объектов должны быть ниже уровней самого объекта соответственно. При отсутствии флагов "ccnr" или "icnr" категории вложенных объектов контейнера должны быть подмножествами категорий самого контейнера. Выполнение этих правил касается также и субъектов, созданных пользователями.

Вывод

Предложенный подход к верификации моделей безопасности операционных систем семейства Windows с использованием темпоральной логики действий Лэмпорта TLA+ позволяет произвести полностью автоматическую верификацию модели, что исключает влияние человеческого фактора на результат верификации, но не исключает возможность совершения ошибки при формировании спецификации модели. Направлением дальнейших исследований является анализ модели политики безопасности управления доступом на наличие скрытых каналов утечки информации по времени, а также ее верификация.

Литература

1. Havelund, Klaus, and Doron Peled. “Runtime verification: From propositional to first-order temporal logic.” In International Conference on Runtime Verification, pp. 90-112. Springer, Cham, 2018. DOI: 10.1007/978-3-030-03769-7_7
2. Kozachok A., Bochkov M., Lai Minh T., Kochetkov E. First order logic for program code functional requirements description // Вопросы кибербезопасности. 2017. № 3 (21). С. 2-7. DOI: 10.21681/2311-3456-2017-3-2-7
3. Markus Alexander Kuppe, Leslie Lamport and Daniel Ricketts. The TLA+ toolbox. In F-IDE@FM 2019, pages 50–62, 2019. DOI: 10.4204/EPTCS.310.6
4. McMillan K. L. Eager Abstraction for Symbolic Model Checking // Computer Aided Verification / ed. by G. Chockler Hana and Weissenbacher. Cham : Springer International Publishing, 2018. P. 191-208. DOI: 10.1007/978-3-319-96145-3_11.
5. Девянин П.Н. О проблеме представления формальной модели политики безопасности операционных систем. Труды ИСП РАН, том 29, вып. 3, 2017. С. 7-16. DOI: 10.15514/ISPRAS-2017-29(3)-1
6. Devyanin, P.N., Khoroshilov, A.V., Kuliainin, V.V., Petrenko, A.K. and Shchepetkov, I.V., 2020. Integrating RBAC, MIC, and MLS inverified hierarchical security model for operating system. Programming and Computer Software, 46(7), pp.443-453. DOI: 10.1134/S0361768820070026
7. Efremov, D. and Shchepetkov, I., 2019, October. Runtime Verification of Linux Kernel Security Module. In International Symposium on Formal Methods (pp. 185-199). Springer, Cham. DOI: 10.1007/978-3-030-54997-8_12
8. Georget, L., Jaume, M., Tronel, F., Piolle, G., Tong, V.V.T.: Verifying the reliability of operating system-level information flow control systems in Linux. In: 2017 IEEE/ACM 5th International FME Workshop on Formal Methods in Software Engineering (FormaliSE), pp. 10–16 DOI: 10.1109/FormaliSE.2017.1
9. Kozachok, A.: TLA+ based access control model specification. In: Proceedings of the Institute for System Programming of the RAS, vol. 30, pp. 147–162, January 2018. DOI: 10.15514/ISPRAS-2018-30(5)-9
10. Havelund, Klaus, and Doron Peled. “Runtime verification: From propositional to first-order temporal logic.” In International Conference on Runtime Verification, pp. 90-112. Springer, Cham, 2018. DOI: 10.1007/978-3-030-03769-7_7

Multilevel mandatory access control Windows NT family model

Kozachok A.V.¹⁰⁴, Kochetkov E.V.¹⁰⁵

Abstract. *The aim of the research is to develop a more advanced access control mechanism to protect against hidden channels of information leakage by memory in the Windows NT operating systems. The result of the research is the set of structures of a multilevel model, reflecting the attributes that are significant for modeling the process of access of subjects to objects; model of key mechanisms of access control in the operating system: management of users, groups, subjects, objects, roles, rights, discretionary and mandatory access control, mandatory integrity control – multilevel control access subjects to objects; define a mechanism for controlling the creation of subjects based on executable files to organize a sandboxed software environment; determinate the invariants of correctness variables in the process of verification and safe access subjects to objects.*

Keywords: *information security, unauthorized access, access control model, model verification.*

¹⁰⁴ Alexander Kozachok, Dr. Sc., Academy of Federal Guard Service, Oryol, a.kozachok@academ.msk.rsnet.ru

¹⁰⁵ Evgenii Kochetkov, Academy of Federal Guard Service, Oryol, mr.koch91@mail.ru

Моделирование псевдослучайных последовательностей, сформированных алгоритмами шифрования и сжатия данных

Козачок А.В.¹⁰⁶, Спирин А.А.¹⁰⁷

Аннотация. Отчеты информационно-аналитических агентств свидетельствуют о высокой доле внутренних нарушителей, как источников утечек конфиденциальных данных в России. Одним из возможных каналов утечек данных может являться их передача в зашифрованном виде. Современные средства анализа данных не способны достоверно обнаружить передачу информации после ее обработки криптографическими алгоритмами. Кроме того, злоумышленник может внедрить в зашифрованные данные цифровые сигнатуры, характерные для сжатых данных, тем самым замаскировать их под легитимные типы файлов. В работе представлен подход к классификации зашифрованных и сжатых данных на основе разработанной модели псевдослучайных последовательностей и алгоритма их классификации. Точность предложенного способа составила 0,97.

Ключевые слова: статистический анализ данных, машинное обучение, классификация зашифрованных и сжатых данных, бинарная классификация последовательностей.

Введение

Согласно отчету экспертно-аналитического центра группы компаний Infowatch, возросла доля внутренних нарушителей как источников утечек конфиденциальных данных в России в 2020 году [1], более чем в 79% случаев утечка конфиденциальных данных произошла по вине внутреннего нарушителя.

Для защиты информации от утечек применяются программные средства обнаружения и предотвращения утечек конфиденциальных данных и различные системы глубокого анализа трафика.

Методы анализа трафика, в зависимости от используемых при его классификации признаков пространств, возможно разделить на несколько групп: расчет энтропии всех данных, или их части [2,3]; служебная информация протоколов передачи данных [4–7], статистические характеристики и распределение байт [8–11]. Однако существуют способы обхода указанных методов защиты, например, применение процедур шифрования, сжатия данных или инкапсуляции в другие протоколы [12,13]. В указанных работах применялись алгоритмы машинного обучения: дерево решений (ДР), метод опорных векторов (МОВ), случайный лес (СЛ), цепи Маркова (ЦМ), бустинг (БГ), сверточные нейронные сети (СНС), определение автокорреляции распределений (АК). Рассмотренные способы применяют для анализа данных заголовки контейнеров и файлов, которые содержат в себе «магические» байты – цифровые сигнатуры, однозначно идентифицирующие протокол передачи или контейнер сжатых данных. При этом программно-аппаратные средства защиты от утечек информации не имеют механизмов анализа зашифрованных или сжатых данных, в случае отсутствия информации об алгоритме сжатия [3]. Обзор рассмотренных методов представлен в таблице 1.

Таблица 1.

Анализ предметной области исследований			
Авторы	Признаки	Мат. аппарат	Точность

¹⁰⁶ Козачок Александр Васильевич, к.т.н., Академия ФСО России, Орел, a.kozachok@academ.msk.rsn.ru

¹⁰⁷ Спирин Андрей Андреевич, Академия ФСО России, Орел, spirin_aa@bk.ru

Mamun M.S.I. [2]	Энтропия	ДР	0,981
Tang Z. [3]		МОВ, СЛ	0,979
Shen M. [4]	Служебная информация	ЦМ	0,912
Chen Y. [5]		БГ	0,987
Obasi T.C. [6]		СНС, СЛ, ДР	0,96
Yao Z. [7]		Скрытые ЦМ	0,99
Choudhury P. [9]	Распределение байт	АК	0,99
Baldini G. [10]		МОВ	0,8
Shen M. [11]		СЛ	0,882

Модель ПСП

Для предотвращения использования цифровых сигнатур и классификации зашифрованных и сжатых последовательностей, обладающих равномерным распределением байт и называемых псевдослучайными (ПСП), на основе статистических признаков была разработана модель ПСП. В формальном виде модель определяется выражением:

$$V = \{F(B_{i \in [0, \dots, 255]}), B_{mean}, B_{sko}, B_{min}, B_{max}, F(S_{j \in [0, \dots, 511]})\}, \quad (1)$$

где: $B_{i \in [0, \dots, 255]}$ – распределение байт в анализируемой ПСП; $S_{j \in [0, \dots, 511]}$ – распределение частот встречаемости подпоследовательностей длины 9 бит в анализируемой ПСП; B_{mean} – среднее значение распределения байт; (B_{sko}) – среднеквадратическое отклонение распределения байт; B_{min}, B_{max} – минимальное и максимальные значения количества байт в ПСП.

Частота появления подпоследовательностей в ПСП рассчитывается согласно выражению 2:

$$F(S_j) = f_j = \frac{n_j}{M - N + 1}, \quad (2)$$

где: n_j – количество вхождений подпоследовательности j в ПСП, M – длина ПСП в битах, N – длина подпоследовательности в битах.

Для проверки адекватности модели были проведены эксперименты по классификации сформированного набора зашифрованных и сжатых данных размером 600КБ. Было сформировано 2000 файлов, содержащих художественный текст на русском языке, далее они были обработаны алгоритмами шифрования (AES, DES, RC4, Camellia, ГОСТ34.12 «Кузнечик») и сжатия (RAR, ZIP, 7Z, GZ, BZ2, XZ).

Практическое применение разработанной модели ПСП

Для классификации использовался разработанный алгоритм, учитывающий дискриминирующую способность признаков модели ПСП на основе построения случайного леса и дерева решений [14]. Полученные результаты оценки точности классификации ПСП разработанным алгоритмом в зависимости от количества используемых признаков представлены на рисунке 1.

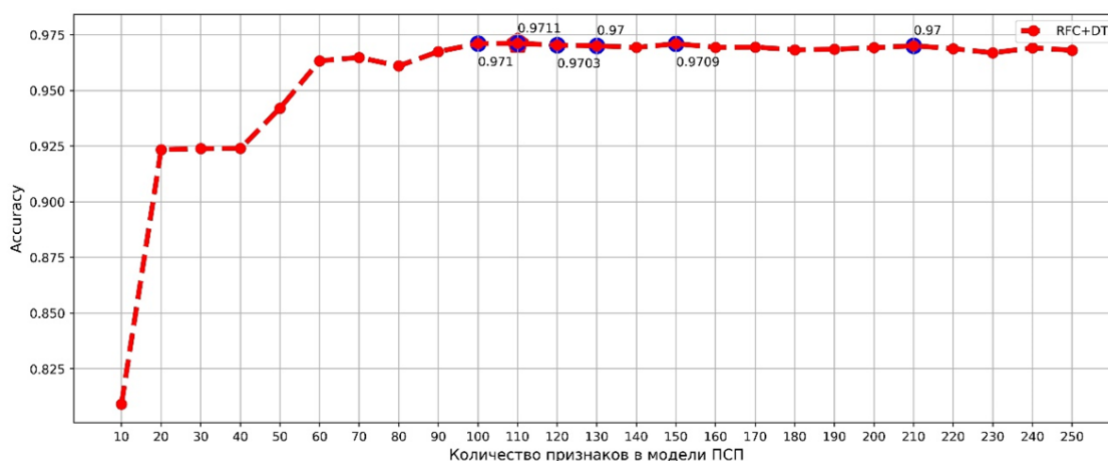


Рис. 1. Оценка точности классификации ПСП в зависимости от числа используемых признаков моделируемых ПСП

Наибольшей точности классификации ПСП удалось достигнуть при использовании 110 признаков модели, однако для дальнейшего использования было выбрано значение в 100 параметров, т.к. разница в точности составляет 0,0001, а время вычисления статистических признаков растет линейно в зависимости от их количества.

Предложенная модель ПСП на основе разработанного алгоритма классификации ПСП позволяет классифицировать зашифрованные и сжатые данные с точностью 0,97 за 0,5 секунды для последовательности длиной 600 кбайт. При проведении классификации не учитываются цифровые подписи, расширения файлов и другая служебная информация, учитываются только статистические признаки распределений байт и 9 битных подпоследовательностей.

Разработанное решение может быть внедрено в существующие средства обнаружения и предотвращения утечек информации и осуществлять статистический анализ данных, передаваемых за контролируемый периметр корпоративной сети передачи данных, блок-схема представлена на рисунке 2.

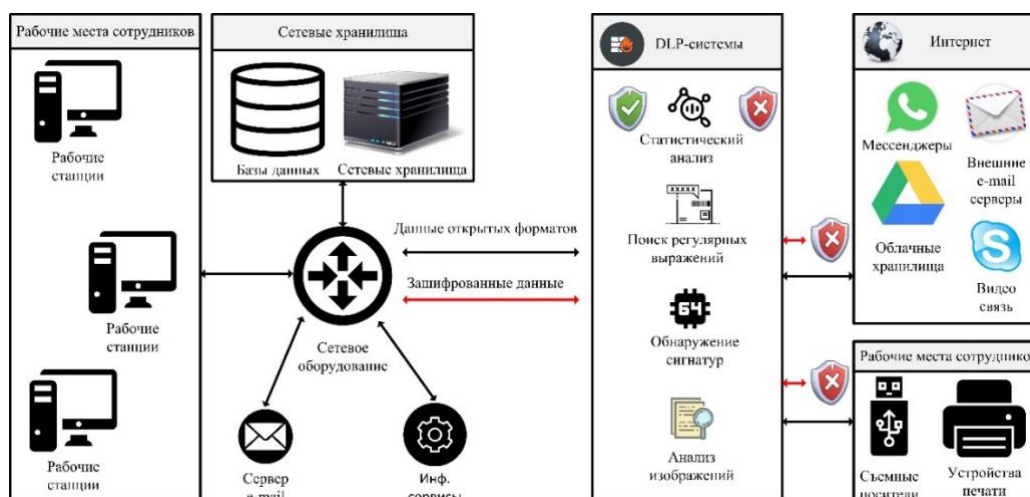


Рис. 2. Место внедрения разработанного подхода классификации ПСП в существующие средства обнаружения и предотвращения утечек информации

На рисунке 3 представлено место внедрения разработанной модели в сервер электронной почты свободно распространяемого программного обеспечения Exim.

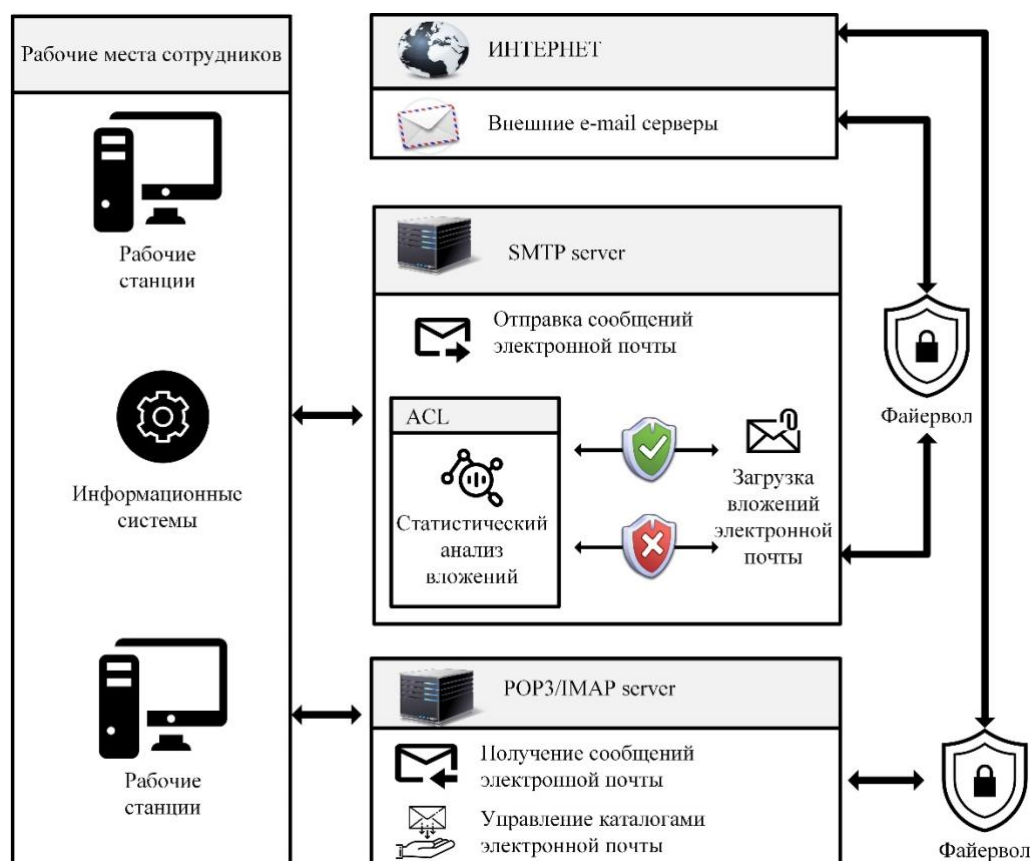


Рис. 3. Место внедрения разработанного подхода классификации ПСП в сервер электронной почты посредством применения списков контроля доступа сервера Exim

Выводы

Для повышения точности классификации ПСП, сформированных алгоритмами шифрования и сжатия данных, была разработана модель ПСП, использующая распределения байт и частоты встречаемости подпоследовательностей длины 9 бит в анализируемых ПСП. В ходе проведения экспериментов была подтверждена адекватность модели и возможность ее применения для классификации указанных в работе типов данных с точностью 0,971. Предложено место внедрения разработанной модели в средства обнаружения и предотвращения утечек информации и в сервер электронной почты Exim.

Литература

1. Отчет экспертно-аналитического центра группы компаний InfoWatch. URL: <https://www.infowatch.ru/analytics/reports/30708> (дата обращения 11.02.2021 г.)
2. Mamun M.S.I., Ghorbani A.A., Stakhanova N. (2016) An Entropy Based Encrypted Traffic Classifier. // In: Qing S., Okamoto E., Kim K., Liu D. (eds) Information and Communications Security. ICICS 2015. Lecture Notes in Computer Science, vol. 9543. Springer, Cham. DOI: 10.1007/978-3-319-29814-6_23.
3. Tang Z., Zeng X., Sheng Y. Entropy-based feature extraction algorithm for encrypted and non-encrypted compressed traffic classification. // International Journal of ICIC, 2019, vol. 15, no. 3, pp. 845–860. DOI: 10.24507/ijicic.15.03.845.
4. Shen M., Wei M., Zhu L. & Wang M. Classification of encrypted traffic with second-order markov chains and application attribute bigrams // IEEE Transactions on Information Forensics and Security, 2017, vol. 12, no. 8, pp. 1830-1843. DOI: 10.1109/TIFS.2017.2692682.
5. Chen Y., Zang T., Zhang Y., Zhou Y., & Wang Y. (2019, October). Rethinking Encrypted Traffic Classification: A Multi-Attribute Associated Fingerprint Approach. // 2019 IEEE 27th

International Conference on Network Protocols (ICNP), Chicago, IL, USA, 2019, pp. 1–11. DOI: 10.1109/ICNP.2019.8888043.

6. Obasi T.C. Encrypted Network Traffic Classification using Ensemble Learning Techniques // Doctoral dissertation, Carleton University, 2020. DOI: 10.22215/etd/2020-14171.

7. Yao Z., Ge J., Wu Y., Lin X., He R., & Ma Y. (2020). Encrypted traffic classification based on Gaussian mixture models and Hidden Markov Models. // Journal of Network and Computer Applications, 2020, vol. 166, p. 102711. DOI: 10.1016/j.jnca.2020.102711.

8. Wang F., Quach T.T., Wheeler J., Aimone J.B., James, C.D. Sparse coding for n-gram feature extraction and training for file fragment classification. // IEEE Transactions on Information Forensics and Security, 2018, vol. 13, no.10, pp. 2553–2562. DOI: 10.1109/TIFS.2018.2823697.

9. Choudhury P., Kumar K. P., Nandi S., Athithan G. An empirical approach towards characterization of encrypted and unencrypted VoIP traffic // Multimedia Tools and Applications, 2020, vol. 79, no. 1–2, pp. 603–631. DOI: <https://doi.org/10.1007/s11042-019-08088-w>.

10. Baldini G., Hernandez-Ramos J. L., Nowak S., Neisse R., Nowak M. Mitigation of Privacy Threats due to Encrypted Traffic Analysis through a Policy-Based Framework and MUD Profiles. // Symmetry, 2020, vol. 12, no.9, p. 1576. DOI: 10.3390/sym12091576.

11. Shen M., Liu Y., Zhu L., Xu K., Du X., Guizani N. Optimizing Feature Selection for Efficient Encrypted Traffic Classification: A Systematic Approach // IEEE Network, 2020, vol. 34, no. 4, pp. 20–27. DOI: 10.1109/MNET.011.1900366.

12. Huang X. et al. A novel mechanism for fast detection of transformed data leakage //IEEE Access, 2018, vol. 6, pp. 35926–35936. DOI: 10.1109/ACCESS.2018.2851228

13. Cheng L., Liu F., Yao D. D. Enterprise data breach: causes, challenges, prevention, and future directions //Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2017, vol. 7, no. 5. DOI: 10.1002/widm.1211.

14. Козачок А.В., Спирин А.А., Голембиовская О.М. Алгоритм классификации псевдослучайных последовательностей на основе построения случайного леса // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2020. – Т. 23. – № 3. –С. 55–60.

Simulation of pseudorandom sequences generated by data encryption and compression algorithms

Kozachok A.V.¹⁰⁸, Spirin A.A.¹⁰⁹

Abstract. Reports of information and analytical agencies indicate a high proportion of internal violators as sources of confidential data leaks in Russia. One of the possible channels of data leaks can be their transmission in encrypted form. Modern data analysis tools are not able to reliably detect the transfer of information after its processing by cryptographic algorithms. In addition, an attacker can embed digital signatures specific to compressed data in encrypted data, thereby disguising them as legitimate file types. The paper presents an approach to the classification of encrypted and compressed data based on the developed model of pseudorandom sequences and the algorithm for their classification. The accuracy of the proposed method was 0.97.

Keywords: statistical data analysis, machine learning, classification of encrypted and compressed data, binary sequence classification.

¹⁰⁸ Alexander Kozachok, Ph.D., Academy of Federal Guard Service, Orel, a.kozachok@academ.msk.rsnet.ru

¹⁰⁹ Andrey Spirin, Academy of Federal Guard Service, Orel, spirin_aa@bk.ru

Разработка низкоресурсного блочного стохастического преобразования на базе ARX конструкции для обеспечения универсальной защиты информации, пересылаемой по каналу связи

Козлов А.А.¹¹⁰

***Аннотация.** В работе исследуется проблема обеспечения безопасности передачи информации между ограниченными в вычислительных ресурсах мобильными устройствами на основе использования идеи стохастического кодирования С.А. Осмоловского. В подобных мобильных устройствах к алгоритмам безопасности предъявляются строгие требования по использованию энергетического и вычислительного ресурсов. Это является проблемой – классические алгоритмы обеспечения информационной безопасности в каналах связи не обладают свойством низкоресурсности. В качестве решения этой проблемы рассматривается построение кодера/декодера для каналов связи на основе низкоресурсного блочного стохастического преобразования. Разработан эффективный по требованиям к вычислительным ресурсам алгоритм блочного стохастического преобразования, исследованы его основные характеристики.*

***Ключевые слова:** стохастические методы защиты информации, стохастическое блочное преобразование, ARX, низкоресурсные алгоритмы.*

Введение

В области современных информационных решений все больше набирают популярность решения на основе низкоресурсных мобильных устройств (далее - НМУ)[1,2].

Информационный обмен между НМУ часто организован через одноранговые беспроводные Ad-hoc сети [3,4,5]. Основными требованиями при передаче данных в этих сетях являются:

- Обеспечение помехоустойчивости;
- Обеспечение целостности;
- Обеспечение конфиденциальности.

Сами НМУ характеризуются низкими вычислительными ресурсами и низким запасом источника питания [6,7].

Основным средством обеспечения конфиденциальности и целостности в НМУ является использование низкоресурсных алгоритмов [8,9]. Однако эти алгоритмы не позволяют решить задачу обеспечения помехозащищенности.

В данной работе предлагается в качестве решения для обеспечения всех требований к сетям работы НМУ использование стохастического метода защиты информации на основе стохастических кодов А.С. Осмоловского [10,11,12]. В качестве элемента стохастического кодера/декодера системы передачи в данной работе предложен низкоресурсный блочный алгоритм стохастического преобразования на базе ARX конструкции.

Проблема обеспечения универсальной защиты информации

Традиционно для решения задачи помехозащищенности используется помехоустойчивое кодирование [13]. Однако все эти коды разработаны для модели

¹¹⁰ Козлов Александр Александрович, ст. преподаватель каф. ИУ8 МГТУ им. Н.Э. Баумана, Москва
kozlov@bmstu.ru

передачи информации по двоичному симметричному каналу. Реальные каналы передачи информации чаще всего не являются таковыми.

Использование кодирования информации по предложенной С.А. Осмоловским схеме позволяет обеспечить равновероятность ошибок декодирования при передаче информации через реальный канал. На рис. 1 представлена схема работы стохастического кодера/декодера С.А. Осмоловского, где I – источник информации, K – кодер, R и R^{-1} – алгоритм прямого и обратного стохастического преобразования, $ДК$ – декодер, $Пр$ – приемник.

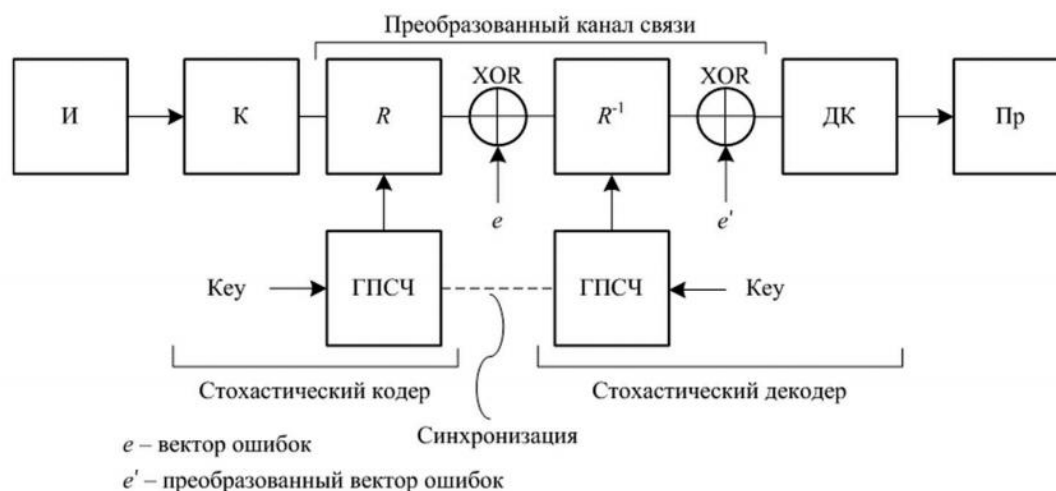


Рис 1. Схема работы стохастического кодера/декодера С.А. Осмоловского

В работе [14] было показано, что если в качестве алгоритма стохастического преобразования использовать алгоритм блочного многораундового стохастического преобразования, то кроме обеспечения помехоустойчивости такой декодер также сможет обеспечить конфиденциальность и целостность передаваемой информации.

Отметим, что одним из наиболее ресурсозатратных элементов в представленной схеме является именно стохастическое преобразование. Если преобразование R будет обладать свойством низкоресурсности, это позволит эффективно применять систему стохастического кодирования С.А. Осмоловского в НМУ.

Алгоритм блочного стохастического преобразования

Исходя из описанных требуемых свойств системы кодирования/декодирования информации в НМУ на основе стохастического кодера/декодера С.А. Осмоловского, были сформированы основные требования к блочному стохастическому алгоритму преобразования R , а именно:

- безопасность по отношению к угрозам нарушения свойства конфиденциальности;
- низкоресурсность.

Низкоресурсность в разработанном алгоритме обеспечивается за счет построения алгоритма R на основе ARX конструкции. Обеспечение безопасности по отношению к угрозам нарушения свойства конфиденциальности основано на результатах, полученных в работах [15] и [16]. В [15] было доказано, что наилучшая линейная аппроксимация единственного нелинейного элемента ARX конструкции выполняется с

вероятностью не более чем в $\frac{1}{4}$. В работе [16] были получены результаты для разностных свойств ARX преобразований.

Разработанный алгоритм блочного стохастического преобразования представлен на рис. 2, где L_i, R_i – входные полублоки раундового преобразования, $K_i = K_i^0 \parallel K_i^1$ – раундовый ключ, L_{i+1}, R_{i+1} – выходные полублоки раундового преобразования, $\boxplus$ – функция сложения по модулю 2^{16} . Основные параметры алгоритма R представлены в табл. 1.

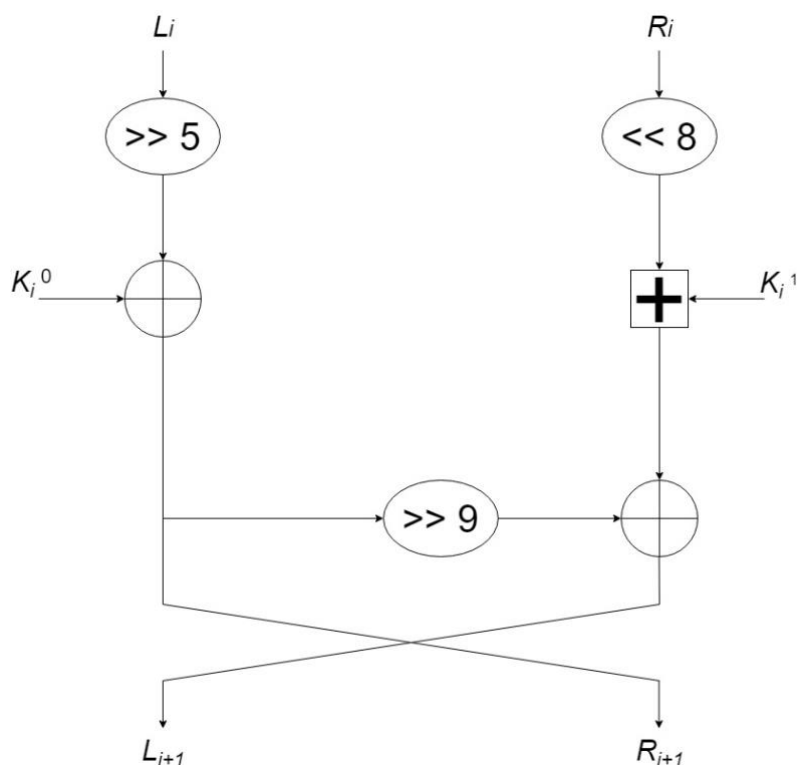


Рисунок 2. Раундовая функция алгоритма блочного стохастического преобразования

Таблица 1.

Основные параметры алгоритма R

Размер входного блока, бит	Размер входного полублока, бит	Размер ключа K , бит	Число раундов
32	16	32	20

Для оценки эффективности реализации алгоритмов на ИС в качестве меры используются: размер микросхемы, потребляемая энергия, и время, затраченное на исполнение программы.

Потребляемая энергия зависит от конкретной используемой элементной базы и поэтому не рассматривалась.

Для схемы предложенного алгоритма в качестве логической элементной базы используются три операции: сложение по модулю 2, сложение по модулю 2^n , и операция циклического сдвига. Сводная информация по требованиям к логической элементной базе и полученной производительности алгоритма R представлена в табл. 2.

Таблица 2.

Требования к элементной базе и полученная производительность алгоритма R

Число требуемых для реализации GE, шт	Производительность, Кбит/сек (100 КГц)
548	9.1
670	16.3
781	44.4

Выводы

В работе предложен подход к обеспечению универсальной защиты информации, пересылаемой по каналу связи между НМУ, на основе использования идеи стохастического кодирования С.А. Осмоловского. Был разработан низкоресурсный алгоритм блочного стохастического преобразования - ключевой элемент системы стохастического кодирования, а также представлены его основные характеристики. Полученные результаты позволяют использовать разработанный алгоритм в системах НМУ, где требуется эффективно использовать ограниченные вычислительные и энергетические ресурсы.

Литература

1. С. В. Рындина, С. В. Куликова, К. Д. Михайлова // Модели, системы, сети в экономике, технике, природе и обществе. – 2020. – No 2 (34). – С. 145–153. – DOI 10.21685/2227-8486-2020-2-11.
2. Курчеева Г.И., Денисов В.В. Угрозы для информационной безопасности в высокоорганизованных системах типа «Умный город»//Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, No3(2016).
3. Sarma S. E., Weis S. A., Engels D. W. Radio-frequency identification: Security risks and challenges. CryptoBytes 6, 1, pp. 2–9, 2003.
4. 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.
5. 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.
6. Жуков А.Е. Легковесная криптография. Часть 1. Вопросы кибербезопасности. 2015. №1(9). с 23-46.
7. Alexey Zhukov. Lightweight Cryptography: Modern Development Paradigms. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 7-7. DOI: 10.1145/2799979.2799981.
8. 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.
9. Manifavas C., Hatzivasilis G., Fysarakis K., Rantos K. Lightweight Cryptography for

Embedded Systems - A Comparative Analysis, SETOP'2013.

10. Осмоловский С.А. Стохастические методы передачи данных. – М.: Радио и связь, 1991.
11. Осмоловский С.А. Стохастические методы защиты информации. – М.: Радио и связь, 2003.
12. Осмоловский С. А. Стохастическая информатика: инновации в информационных системах. – М.: Горячая линия-Телеком, 2011.
13. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. Пер. с англ. – М.: Мир, 1976. 12. Блейхут Р. Б68 Теория и практика кодов, контролирующих ошибки / Блейхут Р. – М.: Книга. по Требованию, 2013. – 566 с
14. Иванов М.А. Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи. Вопросы кибербезопасности. 2019. №3(31). с 45-50. – DOI: 10.21681/2311-3456-2019-3-45-50
15. 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.
16. Козлов А.А. Криптографический анализ ARX шифров на основе усеченных разностей. Электронный журнал «Молодежный научно-технический вестник». // URL: <http://sntbul.bmstu.ru/doc/833658.html> (дата обращения: 12.03.2021)

Рецензент: Иванов Михаил Александрович, доктор технических наук, профессор, заведующий кафедрой компьютерных систем и технологий НИЯУ МИФИ, г. Москва, Россия, E-mail: MAIvanov@mephi.ru.

Development of a lightweight block stochastic algorithm based on ARX construction to provide universal protection of information transmitted via communication channel

Kozlov A.A.¹¹¹

Abstract. *The paper investigates the problem of ensuring the security of information transfer between mobile devices with limited computing resources on the basis of using the ideas of S.A. Osolovsky's stochastic coding. In such mobile devices, strict requirements for the use of energy and computing resources are imposed on security algorithms. But classical algorithms for ensuring information security in communication channels do not lightweight. As a solution to this problem, the construction of an encoder/decoder for communication channels based on a lightweight block stochastic algorithm is considered. Such efficient algorithm has been developed.*

Keywords: *stochastic information security methods, stochastic block algorithm, ARX, lightweight algorithm.*

¹¹¹ Kozlov Alexander Alexandrovich, Teacher of the Department of "Information Security", Bauman Moscow State Technical University, Moscow, kozlov@bmstu.ru

Использование нейросетевых методов и атомарных функций в задаче биометрической аутентификации по ЭКГ

Коннова Н.С.¹¹², Сафина А.Д.¹¹³

Аннотация. Наиболее распространённые методы биометрической аутентификации, где используются такие характеристики как голос, отпечатки пальца, лицо, сетчатка глаза, не устойчивы к фальсификации [1]. Однако потребность в более безопасных индивидуализированных функциях увеличивается с каждым годом. Одной из альтернатив является сигнал ЭКГ: он индивидуален, его амплитуды пика и других характеристик различны, и его трудно подделать [2]. Целью данной работы является разработка системы биометрической аутентификации по сердечному ритму с использованием свёрточной нейросети. Также будет рассмотрено использование атомарной функции активации в сравнении с часто используемой в данном типе нейросетей ReLU. Для оценивания получаемых результатов введены метрики, поставлен численный эксперимент с использованием разработанного программно-математического обеспечения, в рамках которого была реализована свёрточная НС. Для сравнения эффективности классификаторов приведены оценки Accuracy, Recall, Specificity, Precision, F₁-мера. Также были построены графики функции потерь и ROC-кривые.

Ключевые слова: Нейронная сеть (НС), Свёрточная НС (CNN), Функция Активации (ФА), Атомарная Функция (АФ).

Введение

До сих пор аутентификация на основе паролей является основным инструментом идентификации, однако это небезопасно по ряду причин. Основная причина – это недостаточно сложные пароли, несмотря на появление сервисов для хранения паролей. Поэтому сейчас все чаще используют биометрическую аутентификацию, где используются отличительные характеристики, которые могут использоваться для распознавания и проверки легитимности пользователей. ЭКГ сигнал имеет большой потенциал стать мощным инструментом аутентификации благодаря своим свойствам. Тем более что в последнее время вариабельность сердечного ритма была глубоко изучена и было доказано, что благодаря характеристикам анатомии человека, ЭКГ невозможно подделать. Также стоит отметить, что данную характеристику нельзя снять без специальных датчиков, что предотвращает утечку информации. Его дальнейшее использование в качестве биометрии, помимо диагностики в медицине, обусловлено факторами, описанными в работе [3].

В целом, в биометрических системах рассматривается два типа ошибок: ложное срабатывание (ошибка I рода), что приводит к отказу в доступе легитимному пользователю и пропуск событий (ошибка II рода), что приводит к доступу в систему нелегитимного пользователя. Эти ошибки являются обратозависимыми и регулируются порогом принятия решения классификатором в пользу удобства (уменьшение ошибок I рода), или в пользу безопасности (минимизация ошибок II рода).

Материалы и методы

¹¹² Коннова Н.С., к.т.н., доцент Московского государственного технического университета имени Н.Э. Баумана

¹¹³ Сафина А.Д., магистрант Московского государственного технического университета имени Н.Э. Баумана

Для проведения эксперимента использовалась международная база данных PhysioBank ATM измерений нормального сердечного ритма MIT-BIH nsrdb [4]. Эта база данных включает 18 долговременных записей ЭКГ субъектов. У субъектов, включённых в эту базу данных, не было значительных отклонений от нормы; в их число входят 5 мужчин в возрасте от 26 до 45 лет и 13 женщин в возрасте от 20 до 50 лет. Для случайно выбранного легитимного пользователя было собрано 18 сигналов по 10 секунд из общей записи, для остальных были выбраны по 2-3 отрезка, также по 10 секунд.

Предварительная обработка сигналов

Исходные данные требуют предварительной обработки, так как содержат шум и различные искажения. Фильтрация сигнала проводилась с помощью полосового фильтра Баттерворта (ПФБ) 0,5–45 Гц [5], который позволяет снизить частоту и убрать искажения сигнала, сохранив значимые компоненты.

После фильтрации необходимо выделить признаки сигнала ЭКГ, в основном это комплекс *QRS*, волны *P* и *T* [6]. Выделение признаков происходило по следующему алгоритму:

1. Обнаружить *R* волны в общем сигнале ЭКГ;
2. Разделить на циклы ЭКГ между соседними зубцами *R*;
3. Интерполировать циклы ЭКГ (так как шаблоны могут иметь разную длину и частоту, необходимо перед нормализацией провести интерполяцию каждого цикла; в данной работе интерполяция проводилась по алгоритму кубического сплайна [7]);
4. Нормализовать циклы ЭКГ с помощью алгоритма [7];
5. Далее необходимо выделить единый шаблон, для этого вычисляется среднее значение в каждой точке, т.е. для каждого $X_i \in [0 : 0,01 : 1]$ вычислить среднее значение $M(X_i) = \text{Medium}(C_j(X_i))$, где $X_i \in [0 : 0,01 : 1]$ и $j \in [0 : 1 : 10]$; вывести цикл ЭКГ $M = M(X_i)$, где $X_i \in [0 : 0,01 : 1]$.

Описание архитектуры нейронной сети

В глубоком обучении свёрточная нейронная сеть (CNN или ConvNet) представляет собой класс глубоких нейронных сетей, наиболее часто применяемых для анализа визуальных образов [8]. Суть свёртки заключается в создании другого набора значений, который называется ядром или фильтром. Сегодня в традиционной свёрточной нейронной сети присутствуют и другие слои, которые перемежаются со свёрточными слоями. Слой активации – слой, который представляет собой некую нелинейную функцию (обычно ReLU и ее модификации), часто логически объединяется со слоем свертки. Слой субдискретизации (pooling) – слой, представляющий собой нелинейное уплотнение карты признаков. Обычно используется функция максимума. Последним слоем сети является полносвязный слой. Каждый нейрон в этом слое – персептрон с нелинейной функцией активации

Схема свёрточной нейронной сети, используемой в данном исследовании, представлена на рис. 1.

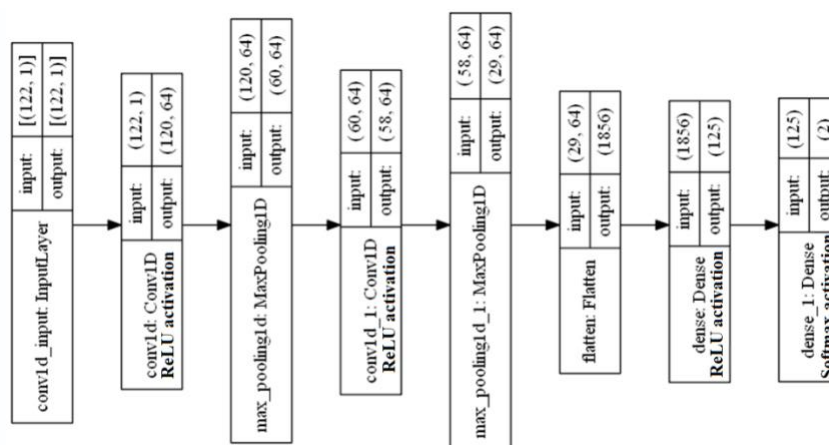


Рис. 1. Свёрточная нейронная сеть

Уникальные аппроксимативные свойства искусственных нейронных сетей во многом достигаются за счет функций активации, определяющих зависимость выходного сигнала от взвешенной суммы сигналов на входе нейрона. Таким образом, искусственный нейрон характеризуется своей функцией активации. Нелинейные функции активации позволяют НС решать нетривиальные задачи с небольшим количеством узлов. Рассмотрим использованные функции активации.

ReLU является выпрямленной функцией активации, ее идея заключается в том, что возбуждение биологических нейронов не может быть выражено отрицательным значением (1). Нейроны вводят нелинейность в нуле, которую можно использовать для принятия решений.

$$f(x) = \max \{0, x\} \quad (1)$$

Сигмоидальные функции, основанные на финитных бесконечно-гладких решениях функционально-дифференциальных уравнений с отклоняющимся аргументом, часто называются атомарными функциями (АФ), они были впервые введены в работах В. Л. Рвачева и В. А. Рвачева [9, 10]. Атомарные функции являются удобным аппаратом численного анализа, теории аппроксимации, цифровой обработки сигналов [11-13]. Несмотря на то, что АФ $up(x)$ не является целой функцией и имеет бесконечный спектр, разложение (2) обеспечивает удовлетворительное качество аппроксимации на интервале $[-1, 1]$.

$$up(x) = \sum_{k=-2^{n+1}}^{2^{n+1}-1} up\left(\frac{k}{2^n}\right) \text{sinc}[\pi(2^n x - k)], (-1 \leq x \leq 1) \quad (2)$$

Рассмотрим возможности АФ для представления функций активации. В качестве базовой выберем простейшую АФ $up(x)$. Определим

$$f(x) = \int_{-1}^x up(t) dt = \begin{cases} up(\frac{1}{2}x - \frac{1}{2}) & \text{при } x \leq 1 \\ 1 & \text{при } x \leq 1. \end{cases} \quad (3)$$

Тогда, в силу основного функционально-дифференциального уравнения для АФ $up(x)$, получаем простое выражение для производной:

$$f(x) = up(x) = f(2x + 1) - f(2x - 1) \quad (4).$$

Исходя из описанных выше свойств, можно предположить, что с использованием этих функций можно ожидать результат нейросетевой классификации как минимум не хуже, чем с применением выпрямленной функцией активации ReLU. Для проверки данной гипотезы был проведен численный эксперимент, описанный далее.

Описание численного эксперимента

После предварительной предобработки сигнала ЭКГ и этапа выделения признаков, для каждого сигнала был получен вектор из 122 коэффициентов,

представляющий шаблон сигнала. На рисунке 5 представлен вид нескольких шаблонов из общей выборки, наложенных для наглядности вариабельности данных.

Параметры нейронной сети подбирались эмпирически. CNN состоит из двух сверточных слоев, между которыми слои pooling и два полносвязных слоя по 125 нейронов с ФА ReLU, либо атомарной ФА; на выходном слое – два нейрона с softmax ФА. При обучении коэффициент кроссвалидации был равен нулю, так как в задачах биометрии необходимо достигнуть переобучения НС для лучшего распознавания легитимного пользователя.

В модели НС для распознавания сигналов ЭКГ используется бинарная классификация: класс «1» – легитимный пользователь и класс «0» – нелегитимный. Для оценки эффективности бинарного классификатора вычисляются следующие метрики оценки: доля правильных ответов (accuracy); точность (precision); полнота (recall); чувствительность (sensitivity); специфичность (specificity), F-мера (F-measure) [14] и ROC-кривая [15].

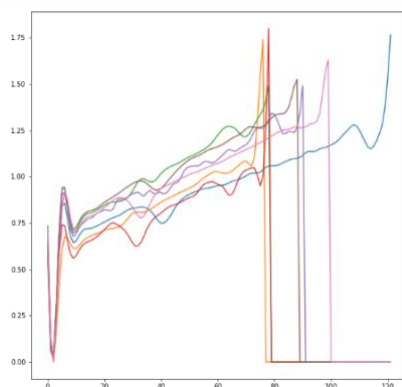


Рис. 5. Шаблоны сигналов ЭКГ

Результаты эксперимента

В табл. 1 показаны метрики эффективности сравниваемых ФА при обучении НС.

Таблица 1.

Сравнение эффективности ФА					
Метрики	НС	ReLU		АФ	
	Обуч. н.	Тест	Обуч. н.	Тест	
	Accuracy	0.9753	1.0000	0.9877	1.0000
	Recall	0.9753	1.0000	0.9877	1.0000
	Precision	0.9753	1.0000	0.9877	1.0000
	ROC-AUC	0.9476	1.0000	0.9877	1.0000

FN (ошибка I рода)	0.0322	0.0000	0.0163	0.0000
FP (ошибка II рода)	0.0322	0.0000	0.0163	0.0000
loss	0.2948	0.2353	0.0957	0.0190
Specificity	0.9545	1.0000	0.9772	1.0000
F-мера	0.9505	1.0000	0.9681	1.0000

Далее на рис. 6 приведены ROC-кривые для оценки качества бинарной классификации, графики точности распознавания (Ассигасу), графики функций потерь и график изменения количества ошибок II рода (FP) при обучении.

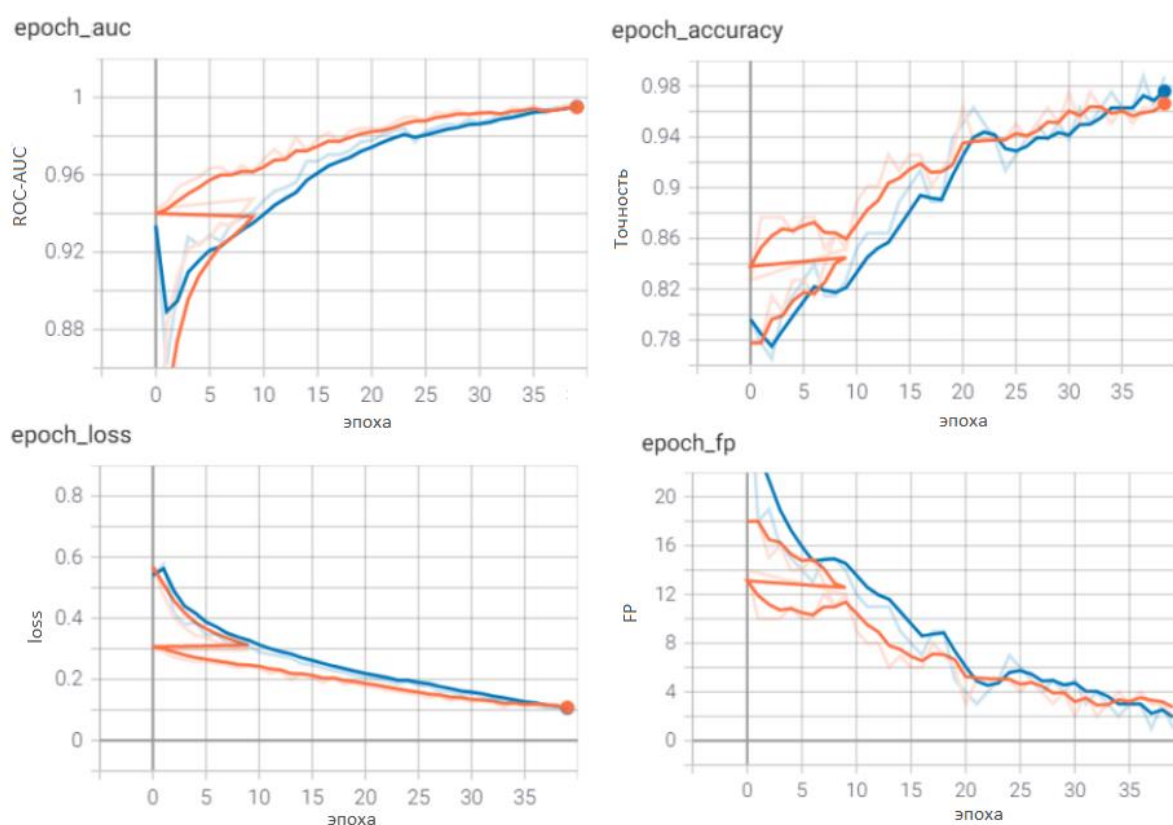


Рис. 6. Графики ROC-кривых, Точности (Ассигасу), Функций потерь и Ошибок II рода (Оранжевый - ReLU, Синий - АФ)

Для тестирования были выбраны образцы, не участвующие в обучении модели нейросети. Всего для тестирования было использовано 20 образцов, 10 из которых принадлежат легитимному пользователю.

При использовании ФА ReLU вероятность принадлежности образцов легитимного пользователя классу «1» в среднем составляет 0,9979, а образцов других пользователей классу «0» – ~1,0000. Это говорит как о том, что модель хорошо обучена и ошибки II рода минимизированы, так и о том, что вероятность ложных срабатываний небольшая.

При использовании Атомарной ФА вероятность принадлежности образцов легитимного пользователя классу «1» в среднем составляет 0,9667, а образцов других пользователей классу «0» – 0,9758. Т.е. немного хуже, чем при использовании ReLU.

Выводы

В данной работе описываются результаты применения свёрточной нейросети в совокупности с применением атомарной функции активации в задаче биометрической аутентификации.

При сравнении двух ФА замечаем: для часто используемой в подобных архитектурах НС ReLU и атомарной ФА, при обучении лучше всего показала себя атомарная (1% пропуска событий при обучении, F-мера 0.9681). Однако при тестировании ReLU показала себя лучше, что показывает ее соответствие для задачи аутентификации.

Как мы видим, свёрточные нейронные сети показывают высокие результаты при обучении и тестировании в задачах биометрической аутентификации, что свидетельствует о том, что они могут быть эффективно использованы для реализации данных систем ИБ, в том числе, для проверки прав доступа пользователя по сердечному ритму.

Литература

1. Sidek K, Sufi F, Khalil I, Al-Shammary D (2010) «An efficient method of biometric matching using»
2. Wang Y, Agrafioti F, Hatzinakos D, Plataniotis KN (2008) «Analysis of human electrocardiogram for biometric recognition». EURASIP J Adv Signal Process 2008: 19.
3. Da Silva, Hugo Plácido, et al. «Finger ECG signal for user authentication: Usability and performance» Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on. IEEE, 2013.
4. Архив сайта Physionet PhysioBank ATM [Электронный ресурс] // URL: <https://physionet.org/cgi-bin/atm/ATM> (дата обращения: 30.03.2021)
5. Butterworth S (1930) On the Theory of Filter Amplifiers. Wireless Engineer 7: 536–541.
6. Meixue Yang, Bin Liu, Miaomiao Zhao, Fan Li, Guoqing Wang, Fengfeng Zhou. «Normalizing Electrocardiograms of Both Healthy Persons and Cardiovascular Disease Patients for Biometric Authentication» //Plos one – 2013 – Vol. 8, No. 8 p. 1-7.
7. Felipe Gustavo Silva Teodoro, Sarajane M. Peres, and Clodoaldo A. M. Lima, «Feature Selection for Biometric Recognition Based on Electrocardiogram Signals», International Joint Conference on Neural Networks (IJCNN), 2017
8. Валуева, М.В.; Нагорнов, Н.Н.; Ляхов, П.А.; Валуев, Г.В.; Червяков, Н. (2020). «Применение системы счисления остатков для снижения затрат на оборудование для реализации свёрточной нейронной сети». Математика и компьютеры в моделировании. Elsevier BV. 177: 232–243.
9. Рвачев В.Л., Рвачев В.А. Об одной финитной функции // Докл. АН УССР. Сер. А. 1971. № 8. С. 705-707.
10. Рвачев В.Л., Рвачев В.А. Неклассические методы теории приближений в краевых задачах. - Киев: Наукова думка, 1979.

11. Басараб М.А., Зелкин Е.Г., Кравченко В.Ф., Яковлев В.П. [Цифровая обработка сигналов на основе теоремы Уиттекера–Котельникова–Шеннона](#). - М.: Радиотехника, 2004.
12. Кравченко В.Ф., Рвачев В.Л. [Алгебра логики, атомарные функции и вейвлеты в физических приложениях](#). - М.: Физматлит, 2006.
13. Коннова Н.С. Цифровая обработка сигналов доплеровского датчика объемной скорости кровотока в условиях переходных процессов в микроциркуляторном русле // Наука и образование: электронное научно-техническое издание. – 2012, №12. DOI: 10.7463/1212.0506267.
14. Применение нейросетей и алгоритмов машинного обучения с целью диагностики сердечно-сосудистых заболеваний на основе сигналов СКГ / Коннова Н. С., Хаперская В. Ю. // Биомедицинская радиоэлектроника. - 2020. - Т. 23, № 1. - С. 5-20
15. Kohavi R «A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection». — 14th International Joint Conference on Artificial Intelligence, Palais de Congres Montreal, Quebec, Canada. — 1995. — С. 1137-1145

The use of neural network methods and atomic functions in the problem of biometric authentication by ECG

Konnova N.S.¹¹⁴, Safina A.D.¹¹⁵

Annotation. The most common methods of biometric authentication, where such characteristics as voice, fingerprints, face, retina are used, are not resistant to falsification [1]. However, the need for safer, customized features is increasing every year. One of the alternatives is the ECG signal: it is individual, its peak amplitudes and other characteristics are different, and it is difficult to fake it [2]. The aim of this work is to develop a biometric heart rate authentication system using a convolutional neural network. The use of the atomic activation function will also be considered in comparison with the ReLU, which is often used in this type of neural network. To evaluate the results obtained, metrics were introduced, a numerical experiment was set up using the developed software, within which a convolutional neural network was implemented. To compare the efficiency of the classifiers, the estimates of Accuracy, Recall, Specificity, Precision, F1 are given - a measure. Loss function plots and ROC curves were also plotted.

Keywords: Neural Network (NN), Convolutional NN (CNN), Activation Function (FA), Atomic Function (AF)

¹¹⁴ Konnova N.S., Ph.D., Associate Professor, Bauman Moscow State Technical University

¹¹⁵ Safina A.D., undergraduate student, Bauman Moscow State Technical University

Анализ информационной безопасности объектов критической информационной инфраструктуры на базе информационно-энергетического подхода

Корнеев Н.В.¹¹⁶, Сафин И.Р.¹¹⁷

Аннотация. В работе определены задачи цифровой трансформаций имеющейся инфраструктуры для игроков топливно-энергетического рынка. Предложены компоненты экосистемы для крупных игроков топливно-энергетического рынка с учетом цифровой трансформаций имеющейся инфраструктуры. Проведен анализ информационной безопасности автоматизированных систем управления технологическим процессом (АСУ ТП) и систем диспетчерского контроля и сбора данных (SCADA) на базе информационно-энергетического подхода. Сформулировано новое понятие вектора атаки на инфраструктуру (в частности, критическую информационную инфраструктуру) на базе информационно-энергетического подхода, и показана его актуальность в области информационной безопасности АСУ ТП и SCADA.

Ключевые слова: комплексная безопасность, АСУ ТП, SCADA, цифровой след, цифровая трансформация, индустрия 5.0, кибератака.

Введение

Бурное развитие информационных технологий открывает новые перспективы в развитии систем обработки информации. Принципиально изменяется структура систем обработки информации, основой которых теперь являются распределенные информационно-вычислительные сети, подключенные к глобальным сетям передачи данных, конвергентные, гиперконвергентные, нейроморфные и квантовые вычислительные системы. В тоже время ужесточаются требования регуляторов, особенно в части комплексной безопасности объектов: физической, экономической, пожарной, информационной, психологической, безопасности интеллектуальной собственности, техногенной, безопасности от терроризма, экологической безопасности.

Для топливно-энергетического комплекса (ТЭК) – это в первую очередь Доктрина энергетической безопасности Российской Федерации (Указ Президента РФ от 13.05.2019 г. №216), новая редакция Доктрины информационной безопасности (Указ Президента РФ от 5.12.2016 г. №646), Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон от 21 июля 2011 г. №256-ФЗ «О безопасности объектов топливно-энергетического комплекса», Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации». В этих документах приоритетное место уделено вопросам обеспечения безопасности критических объектов топливно-энергетического комплекса, в том числе посредством постоянного осуществления мониторинга угроз функционирования объекта.

С учетом Национальной стратегии развития искусственного интеллекта на период до 2030 года (Указ Президента РФ от 10.10.2019 г. №490) вопросы обеспечения

¹¹⁶ Корнеев Николай Владимирович, доктор технических наук, доцент, РГУ нефти и газа (НИУ) имени И.М. Губкина, Финансовый университет при Правительстве Российской Федерации, ФГБУ "Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России" (федеральный центр науки и высоких технологий), Москва, niccuser@mail.ru

¹¹⁷ Сафин Ильнур Ришатович, инженер группы внедрения Департамента программных разработок АО "НПО "Эшелон", Москва, i.safin@npo-echelon.ru

безопасности критических объектов топливно-энергетического комплекса должны решаться с использованием интеллектуального анализа данных, где центральную роль занимает цифровизация бизнес-процессов топливно-энергетического комплекса.

Задачи цифровой трансформаций имеющейся инфраструктуры для игроков топливно-энергетического рынка

В этой связи всем игрокам топливно-энергетического рынка приходится решать задачи цифровой трансформации имеющейся инфраструктуры.

Опыт показывает, что подобный подход непременно приводит к созданию собственных искусственных экосистем, способных решать целый комплекс задач, в том числе задачи безопасности объектов топливно-энергетического комплекса. В качестве примера такой системы может выступать экосистема Сбербанка, где интеграция сервисов с учетом финансово-экономических целей цифровой трансформации достигается за счет эффективного использования цифровых технологий. Крупным игрокам топливно-энергетического рынка, аналогичным образом придется решать свои задачи цифровой трансформаций имеющейся инфраструктуры.

Компоненты экосистемы для крупных игроков топливно-энергетического рынка

В качестве компонентов экосистемы для крупных игроков топливно-энергетического рынка с учетом цифровой трансформаций имеющейся инфраструктуры можно выделить задачи формирования:

- цифровых средств труда, например цифровых месторождений, цифровая сейсморазведка, беспилотные летательные аппараты и др;
- цифровых орудий труда, например цифровые нефтеперерабатывающие заводы;
- умных работников, использующих экосистему с целью эффективного выполнения своих должностных обязанностей.

Состав компонентов указанными не ограничивается, ввиду динамического развития объекта и окружающей его среды [1].

Анализ информационной безопасности автоматизированных систем управления технологическим процессом (АСУ ТП) и систем диспетчерского контроля и сбора данных (SCADA) на базе информационно-энергетического подхода

Современные или крупные автоматизированные системы управления технологическим процессом (АСУ ТП) невозможны без систем диспетчерского контроля и сбора данных (SCADA). Примерами АСУ ТП могут послужить такие объекты критической информационной инфраструктур (КИИ) как системы и сети управления транспорта, системы и сети управления электроснабжения, системы и сети управления теплоснабжения, системы и сети управления топливно-энергетического комплекса (ТЭК), системы и сети управления атомных электростанций и т.д. Все эти современные системы и сети с одной стороны базируются на принципах автоматического управления [1] и используют цифровые данные в АСУ ТП и SCADA, а с другой стороны представляют собой систему обработки информации [2], которая уязвима для соответствующих дестабилизирующих факторов [2] по стандарту ISO/IEC 27002, в том числе кибератака, вредоносное ПО, например «Triton» [3], «Irongate» [4] и модулей для

фреймворков, таких как «Autosploit» [5], «ICSSPLOIT», «Metasploit», «Core Impact» и «Immunity Canvas».

В АСУ ТП и SCADA используются несколько протоколов связи. В отличие от Ethernet или Интернет-протоколов (IP), АСУ используют несколько протоколов, часто уникальных для производителя ПЛК-контроллеров. Наиболее популярные Modbus, dnp, dnp3, fieldbus, Ethernet/IP, etherCAT, profinet.

Такая широкая спецификация в первую очередь определяет необходимость формирования уникального вектора непосредственного отображения состояния объекта и среды [6], основанного на диагностической информации по объекту и наиболее полной по состоянию среды – доступной для АСУ ТП и SCADA, будем далее называть такую диагностическую информацию – вектором атаки на инфраструктуру, например КИИ. В то же время нельзя считать, что эта информация идентична уравнению приведенному в работе [1], поэтому:

$$\tilde{X}[k+1] = \tilde{\Phi}(\tilde{X}, U, \tilde{F}, t) \tilde{X}[k] + \tilde{\Gamma}(t) U[k] + \tilde{G}(t) \tilde{F}[k], \quad (1)$$

где: $\tilde{X}[k+1]$, $\tilde{X}[k]$ – наиболее точные возможные оценки векторов состояния объекта и среды, $\tilde{\Phi}(\tilde{X}, U, \tilde{F}, t)$ – функция перехода, определяемая наиболее точно известными параметрами состояния объекта и среды, $\tilde{F}[k]$ – оценка вектора непосредственных воздействий среды, $\tilde{\Gamma}(t)U[k]$, $\tilde{G}(t)\tilde{F}[k]$ – интегральные преобразования наиболее точно представленных управляющих и возмущающих воздействий.

Во вторую очередь приведенная широкая спецификация уникальных для производителя ПЛК-контроллеров требует, адекватных «уникальных» методов информационной безопасности соответствующих АСУ ТП и SCADA от дестабилизирующих факторов [2, 7, 8, 9, 10, 11, 12] (кибератака, вредоносное ПО), учитывающих указанный вектор атаки на инфраструктуру, например на базе ядра комплексной безопасности [6].

Наконец, в третью очередь необходимо внедрение предложенных методов ИБ в состав проектов по информационной и комплексной безопасности КИИ.

Выводы

Предложены компоненты экосистемы для крупных игроков топливно-энергетического рынка с учетом цифровой трансформаций имеющейся инфраструктуры. Показана что обеспечение информационной безопасности такой инфраструктуры может быть представлено на базе информационно-энергетического подхода. Сформулировано новое понятие вектора атаки на инфраструктуру (в частности, критическую информационную инфраструктуру) на базе информационно-энергетического подхода, и показана его актуальность в области информационной безопасности АСУ ТП и SCADA.

Литература

1. Корнеев Н.В., Кустарев Ю.С., Морговский Ю.Я. Теория автоматического управления с практикумом: учебное пособие для вузов (УМО) / Москва, 2008. Сер. Высшее профессиональное образование. Издательский центр «Академия», 2008. 224 с.
2. Корнеев Н.В. Алгоритмические и программные методы и средства оценки альтернативных проектов защиты системы обработки информации предприятия на основе многокритериального анализа: монография. Москва: Изд-во «Спутник+», 2013. 117 с.

3. Sani A. S., Yuan D., Yeoh P. L., Qiu J., Bao W., Vucetic B., Dong Z. Y. CyRA: A real-time risk-based security assessment framework for cyber attacks prevention in industrial control systems // IEEE Power and Energy Society General Meeting. 2019. V. 2019-August. P. 8973948.
4. Assenza G., Faramondi L., Oliva G., Setola R. Cyber threats for operational technologies // International Journal of System of Systems Engineering. 2020. Vol. 10(2). pp. 128-142.
5. Yichao Z., Tianyang Z., Xiaoyue G., Qingxian W. An improved attack path discovery algorithm through compact graph planning // IEEE Access. Vol. 7. pp. 59346-59356.
6. Korneev N.V. Intelligent complex security management system FEC for the industry 5.0 // IOP Conference Series: Materials Science and Engineering. 2020. V. 950(1). P. 012016.
7. Korneev N., Merkulov V. Intellectual analysis and basic modeling of complex threats // CEUR Workshop Proceedings. 2019. V. 2603. pp. 23-28.
8. Korneev N.V. A Neurograph as a Model to Support Control over the Comprehensive Objects Safety for BIM Technologies // IOP Conference Series: Earth and Environmental Science. 2019. V. 224. P. 012021.
9. Dakheel A.H., Dakheel A.H., Abbas H.H. Intrusion detection system in gas-pipeline industry using machine learning // Periodicals of Engineering and Natural Sciences. 2019. V. 7(3). pp. 1030-1040.
10. Wei L., Chuipin K., Qiang N., Jingguo J., Xionghui Z. A method of NC machine tools intelligent monitoring system in smart factories // Robotics and Computer-Integrated Manufacturing. 2020. V. 61. P. 101842.
11. Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУ ТП // Вопросы кибербезопасности. 2015. № 2 (10). С. 56-59.
12. Колосок И. Н., Гурина Л. А. Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния // Вопросы кибербезопасности. 2018. №. 3 (27). С. 63-69.

Analysis of information security critical information infrastructure facilities based on the information and energy methodologies

Korneev N.V.¹¹⁸, Safin I.R.¹¹⁹

Abstract. *The work identified the tasks of digital transformations of the existing infrastructure for players in the fuel and energy market. Ecosystem components are proposed for large players of the fuel and energy market taking into account digital transformations of the available infrastructure. Analysis of information security of automated process control systems (APCS) and supervisory control and data acquisition (SCADA) based on the information and energy methodologies was carried out. The new concept of a vector of the attack on infrastructure (in particular critical information infrastructure) on the basis of information and power methodologies is formulated, and its relevance in the field of information security of APCS and SCADA is shown.*

Keywords: *complex security, APCS, SCADA, digital trace, digital transformation, industry 5.0, cyberattack*

¹¹⁸ Nikolai Korneev, Dr.Sc., professor, Gubkin Russian State University of Oil and Gas (National Research University), Financial University under the Government of the Russian Federation, All-Russian Scientific Research Institute of Civil Defence and Emergencies EMERCOM of Russia, Moscow, niccyper@mail.ru

¹¹⁹ Safin Ilnur, engineer of group implementation Software Development Department of NPO Echelon, Moscow, i.safin@npo-echelon.ru

Подход к анализу влияния защищенности информации на реализацию процесса управления решениями

Костогрызов А.И.¹²⁰

***Аннотация.** Предложен подход, позволяющий осуществлять анализ влияния защищенности информации на реализацию процесса управления решениями в терминах прогнозируемых рисков. Использование предложенного подхода в жизненном цикле систем способствует выявлению «узких мест» и снижению рисков в процессе управления решениями с учетом требований по защите информации. Работоспособность подхода проиллюстрирована на примерах.*

***Ключевые слова:** анализ, защита информации, модель, риск, управление.*

1. Введение

В общем случае главной целью процесса управления решениями является обеспечение аналитической основы для определения, характеристики и оценки множества альтернативных решений, выбора наиболее предпочтительных решений и направлений практических действий на любом этапе жизненного цикла системы. В условиях множественных неопределенностей возникают различного рода риски, требующие рационального управления, в т.ч. риски, связанные с нарушением требований по защите информации. Несмотря на множество работ по управлению рисками (например, [1-10]), проблематика, связанная с анализом влияния защищенности информации на реализацию процесса управления решениями в терминах прогнозируемых рисков, продолжает оставаться актуальной.

2. Общие положения

В общем случае основными выходными результатами процесса управления решениями являются:

- варианты решений, требующих альтернативного системного анализа;
- альтернативные направления действий;
- предпочтительные решения и направления действий;
- задокументированные обоснования решений и принятые при обоснованиях предположения и допущения.

В жизненном цикле систем должны быть обеспечены как надежная реализация самого процесса управления решениями, так и защита связанной с этим процессом информации.

3. Предлагаемые показатели и общий подход к моделированию

Для прогнозирования рисков в процессе управления решениями предлагается использовать следующие количественные показатели:

- риск нарушения надежности реализации процесса без учета требований по защите информации;
- риск нарушения требований по защите информации;
- интегральный риск нарушения реализации процесса с учетом требований по защите информации.

¹²⁰ Костогрызов А.И., д.т.н, проф., Федеральный исследовательский центр «Информатика и управление» Российской академии наук, e-mail: Akostogr@gmail.com

Для расчёта показателей рисков исследуемые сущности могут рассматриваться в виде системы простой или сложной структуры. Модели и методы прогнозирования рисков используют данные, получаемые «по факту наступления событий», по выявленным предпосылкам к наступлению событий, и данные собираемой и накапливаемой статистики и возможным условиям их реализации процесса.

Модель системы простой структуры представляет собой систему из единственного элемента или множества элементов, логически объединённых для анализа как один элемент. Анализ системы простой структуры осуществляют по принципу «чёрного ящика», когда известны входы и выходы, но неизвестны внутренние детали функционирования системы. Модель системы сложной структуры представляется как совокупность взаимодействующих элементов, каждый из которых представляется в виде «чёрного ящика», функционирующего в условиях неопределённости.

Применимые модели для прогнозирования отдельно риска нарушения надежности реализации процесса без учета требований по защите информации $R_{\text{надежн.}}(T_{\text{зад}})$ и - риска нарушения требований по защите информации $R_{\text{наруш.}}(T_{\text{зад}})$ представлены, например, в [6-10], а также по предложению автора включены в ГОСТ Р 58494-2019, ГОСТ Р 59338-2021.

4. Расчет интегрального риска

В сопоставлении с возможным ущербом в предположениях независимости содержательных действий по управлению решениями и специальных действий по защите информации интегральный риск нарушения реализации процесса управления решениями с учетом требований по защите информации $R_{\text{интегр.}}(T_{\text{зад}})$ для прогнозного периода $T_{\text{зад}}$ предлагается вычислять по формуле:

$$R_{\text{интегр.}}(T_{\text{зад.}}) = 1 - [1 - R_{\text{надежн.}}(T_{\text{зад.}})] \cdot [1 - R_{\text{наруш.}}(T_{\text{зад.}})]. \quad (1)$$

где $R_{\text{надежн.}}(T_{\text{зад.}})$ — вероятность нарушения надежности реализации процесса управления решениями в течение периода прогноза $T_{\text{зад}}$ без учета требований по защите информации;

$R_{\text{наруш.}}(T_{\text{зад.}})$ — вероятность нарушения требований по защите информации в системе для процесса управления решениями в течение периода прогноза $T_{\text{зад.}}$

5. Примеры

5.1 Пусть некоторое предприятие организует управление производством, ориентируясь на требования ГОСТ Р МЭК 62264-1 по интеграции систем управления предприятием.

Не вдаваясь в детали интегрируемых систем управления в части производственного процесса, процесса технического обслуживания, процесса контроля качества и процесса инвентаризации, в рамках примера продемонстрирован предлагаемый подход к анализу влияния защищенности информации на реализацию процесса управления решениями. Рассмотрим выполнение следующих действий: действие 1 - планирование управления решениями; 2 - сбор, обработка и анализ информации для принятия решений; 3 - принятие решений и управление решениями.

Для оценки риска нарушения надежности реализации процесса управления решениями без учета требований по защите информации выбраны:

- модели ГОСТ Р 59338-2021 для анализа действий, связанных с планированием управления решениями (действие 1), принятием решений и управлением решениями (действие 3);

- модели, связанные со сбором, обработкой и анализом информации для принятия решений (действие 2) - по ГОСТ Р 59341-2021.

Такое формальное описание позволяет сформировать моделируемую систему в виде структуры следующих последовательных элементов, ассоциируемых с действиями – см. рис. 1.



Рисунок 1 — Формальное описание комплекса действий для оценки риска нарушения надежности реализации процесса управления решениями

По определению надежность реализации процесса управления решениями моделируемой системы считается обеспеченной в течение заданного периода прогноза, если в течение этого периода «И» для производственного процесса, «И» для процесса технического обслуживания, «И» для процесса контроля качества «И» для процесса инвентаризации надежно выполнены действия процесса «И» по планированию управления решениями (по элементам 1, 2, 3, 4), «И» по принятию решений и управлению решениями (по элементам 5, 6, 7, 8). Причем надежность выполнения этих процессов будет приемлемой в течение такого же периода и в будущем. То есть сам период прогноза для отдельного элемента может быть интерпретирован как относящийся как к стадиям создания (по угрозам, свойственным этим стадиям), так и к стадиям эксплуатации и вывода из эксплуатации (по потенциально возможным угрозам), моделируя приемлемость решений, возможности и подтверждение гарантий непревышения допустимых рисков.

Пример 1 посвящен прогнозированию риска нарушения надежности реализации процесса управления решениями без учета качества используемой информации (по результатам сбора, обработки и анализа информации для принятия решений) и требований по защите информации. Пример 2 демонстрирует, как при прогнозировании риска нарушения надежности реализации процесса управления решениями предприятия можно дополнительно учесть качество используемой информации по результатам сбора, обработки и анализа информации для принятия решений. Пример 3 посвящен прогнозированию риска нарушения требований по защите

информации. Пример 4 иллюстрирует анализ влияния защищенности информации на реализацию процесса управления решениями на уровне интегрального риска.

5.2 Пример 1. Прогнозирование риска нарушения надежности реализации процесса управления решениями без учета качества используемой информации (по результатам сбора, обработки и анализа информации для принятия решений) и требований по защите информации проиллюстрировано для структуры моделируемой системы, представленной на рисунке 2.



Рисунок 2 — Структура моделируемой системы без учета требований по защите информации

Исходные данные по каждому из 8 составных элементов представлены в Таблице 1.

Таблица 1 — Исходные данные для прогнозирования риска нарушения надежности реализации процесса без учета качества используемой информации и требований по защите информации

Исходные данные	Значения и комментарии	
	для 1-го/ 2-го/ 3-го/ 4-го элементов при планировании управления решениями	для 5-го/ 6-го/ 7-го/ 8-го элементов при принятии решений и управлении решениями
σ — частота возникновения источников угроз нарушения надежности реализации процесса	5 раз в год (из-за недостаточной квалификации или знаний) / 1 раз в год (из-за персонала) / 1 раз в год (из-за персонала) / 1 раз в год (из-за персонала) — это угрозы программно-технических и человеческих ошибок	2 раза в год (из-за недостаточной квалификации или знаний) / 1 раз в год (из-за персонала) / 1 раз в год (из-за персонала) / 1 раз в год (из-за персонала) — это угрозы ущерба от принятия необоснованных решений
β — среднее время развития угроз для элемента с момента возникновения источников угроз до нарушения с возможным ущербом	2 недели (что соизмеримо со временем моделирования для, обоснования планов) / 1 год (что соизмеримо со временем между критичными ошибками в планировании технического обслуживания)	6 месяцев (что соизмеримо со временем постепенного отказа производственного оборудования) / 6 месяцев (что объясняется сохранением минимальных возможностей системы функционировать в устаревшей среде)

Исходные данные	Значения и комментарии	
	для 1-го/ 2-го/ 3-го/ 4-го элементов при планировании управления решениями	для 5-го/ 6-го/ 7-го/ 8-го элементов при принятии решений и управлении решениями
	/ 1 год (что соизмеримо со временем между критичными ошибками в планировании контроля качества) / 1 год (что соизмеримо со временем между критичными ошибками) – это среднее время до возможного ущерба после критичных программно-технических, технологических или человеческих ошибок, допущенных при планировании	/ 2 месяца (что объясняется средним временем до рекламаций из-за ошибок при контроле качества) / 6 месяцев (что объясняется средним временем до производственных простоев из-за критичных ошибок) – это среднее время до возможного ущерба после критичных программно-технических, технологических или человеческих ошибок, допущенных при принятии решений
Тмеж – среднее время между окончанием предыдущей и началом очередной диагностики возможностей элемента	8 часов / 8 часов / 8 часов / 8 часов — это время определяется регламентом контроля готовности персонала к работе – 1 раз за смену при 8-часовом рабочем дне	1 час - определяется регламентом контроля оборудования / 1 неделя - определяется регламентом технического обслуживания / 1 неделя - определяется регламентом отчетности службы контроля качества / 1 неделя - определяется регламентом отчетности службы контроля качества на предприятии
Тдиаг – среднее время диагностики состояния элемента	10 минут / 10 минут / 10 минут / 10 минут - определяется временем медицинского обследования перед работой	30 секунд – означает длительность автоматического контроля целостности оборудования в производственном процессе / 1 час - диагностика состояния оборудования при техническом обслуживании / 30 секунд – означает длительность автоматического контроля целостности оборудования / 30 секунд - означает длительность автоматической инвентаризации активов
Твосст – среднее время восстановления элемента после выявления нарушений	30 минут / 30 минут / 30 минут / 30 минут — это время замены человека, отстраненного от выполнения обязанностей, и возложения необходимых функциональных обязанностей на заменяющего человека для выполнения функций планирования	4 час – среднее время восстановления оборудования после сбоя или отказа / 8 часов – это время восстановления нарушенного процесса технического обслуживания / 30 минут — это время переинсталляции программного обеспечения системы контроля качества / 8 часов — это время восстановления нарушенного процесса инвентаризации
Тзад – задаваемая длительность периода прогноза	от 1 месяца до 1 года (для определения периода, при котором сохраняются гарантии непревышения допустимого риска нарушения надежности реализации процесса)	

Анализ результатов расчетов показал, что для производственного процесса, процесса технического обслуживания, процесса контроля качества и процесса инвентаризации в вероятностном выражении риск нарушения надежности реализации рассматриваемых действий процесса управления решениями в течение года составит

около 0.142 - см. рисунок 3. Это означает, что действия по планированию управления решениями в производственном процессе (элемент 1) и действия по принятию решений и управлению решениями в процессе контроля качества (элемент 7) являются определяющими в общем риске нарушения надежности реализации процесса управления решениями — см. Таблицу 1. По элементам 2-6, 8 значения оцениваемого риска не превышают 0.019. При изменении периода прогноза от 1 месяца до 1 года риск за все действия возрастает от 0.012 до 0.142. Для допустимого риска на уровне 0.05 обоснован период до 117 дней, при котором сохраняются гарантии неперевышения допустимого риска (см. рис. 4).

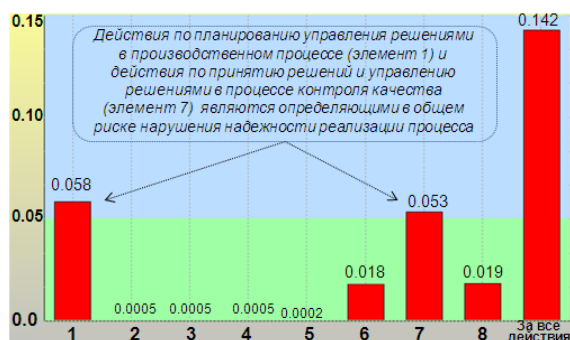


Рисунок 3 — Оценки риска без учета качества используемой информации и требований по защите информации
(период прогноза - 1 год)

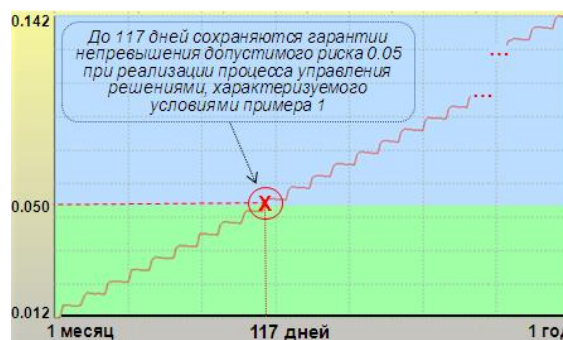


Рисунок 4 — Зависимость риска от периода прогноза длительностью от 1 месяца до 1 года

Примечание — Пилообразный характер зависимости риска от периода прогноза на рисунке 4 объясняется периодическим контролем и восстановлением целостности моделируемой системы при диагностике и тем, что в моделях ГОСТ Р 59338-2021 при расчетах используется целое количество диагностик, входящих в период прогноза. Сразу после диагностики риск нарушения снижается, со временем до следующей диагностики – возрастает, именно это является причиной пилообразности.

5.3 Пример 2 дополнительно к результатам примера 1 позволяет учесть качество используемой информации по результатам сбора, обработки и анализа информации для принятия решений. Для этого использованы примеры ГОСТ Р 59341-2021. С учетом их пусть в предположении отсутствия задаваемых допустимых требований к полноте и достоверности используемой информации и безошибочности действий ответственных лиц в рамках рассматриваемого процесса управления решениями вероятность нарушения надежности реализации процесса управления информацией в течение периода прогноза, равного 1 месяцу, без учета требований по защите информации составит около 0.2. Тогда вероятность нарушения надежности реализации процесса управления решениями $R_{\text{надежн.}}(T_{\text{зад}})$ в течение периода прогноза, равного 1 месяцу, без учета требований по защите информации составит около 0.210. При этом около 95% этого значения определяет достигаемый уровень качества используемой информации. Если же это качество признается приемлемым или неуллучшаемым (например, по причинам технологической невозможности или по экономическим соображениям), то с достигаемым качеством соглашаются и риски нарушения этого качества не учитывают при дальнейшем системном анализе. В этом случае $R_{\text{надежн.}}(T_{\text{зад}}) = 0.012$.

5.4. Пример 3. Продолжая примеры 1 и 2, прогнозирование риска нарушения требований по защите информации проиллюстрировано для комплекса действий

по планированию управления решениями, принятию решений и непосредственно управлению решениями по ГОСТ Р МЭК 62264-1. При этом осуществлена привязка к структуре действий и защищаемых активов, определенных на рисунках 2 и 3. Исходные данные по каждому из 8 составных элементов, учитывающие возможные уязвимости в технологиях защиты активов и сопровождаемые поясняющими комментариями, представлены в Таблице 2.

Таблица 2 — Исходные данные для прогнозирования риска нарушения требований по защите информации в процессе управления решениями

Исходные данные	Значения и комментарии	
	для 1-го/ 2-го/ 3-го/ 4-го элементов при планировании управления решениями	для 5-го/ 6-го/ 7-го/ 8-го элементов при принятии решений и управлении решениями
σ – частота возникновения источников угроз нарушения требований по защите информации	1 раз в год (что соизмеримо с частотой технического отказа оборудования) / 1 раз в год (что соизмеримо с частотой ошибок со стороны специалиста-планировщика средней квалификации) / 2 раза в год (что соизмеримо с частотой ошибок со стороны контролера средней квалификации) / 2 раза в год (что соизмеримо с частотой ошибок по планированию в части инвентаризации со стороны специалиста средней квалификации) – это угрозы ущерба в результате нарушения требований по защите информации	1 раз в год (что соизмеримо с частотой технического отказа оборудования) / 1 раз в 5 лет (что объясняется маскировкой под отказы в процессе технического обслуживания системы специалистами высокой квалификации) / 1 раз в год (что соизмеримо с частотой ошибок со стороны контролера высокой квалификации) / 1 раз в год (что соизмеримо с частотой ошибок по инвентаризации со стороны специалиста высокой квалификации) – это угрозы ущерба в результате нарушения требований по защите информации
β – среднее время развития угроз с момента возникновения источников угроз до нарушения требований	1 сутки / 1 сутки / 1 сутки / 1 сутки (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее суток)	1 сутки / 1 сутки / 1 сутки / 1 сутки (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее суток)
Тмеж – среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы	1 час / 1 час / 1 час / 1 час - определяется регламентом контроля целостности программного обеспечения и активов, используемых при планировании решений	1 час / 1 час / 1 час / 1 час - определяется регламентом контроля целостности программного обеспечения и активов, используемых при управлении решениями
Тдиаг – среднее время диагностики состояния активов и самой системы защиты информации	30 секунд / 30 секунд / 30 секунд / 30 секунд - автоматический контроль целостности программного обеспечения и активов, используемых при планировании управления решениями	30 секунд / 30 секунд / 30 секунд / 30 секунд - автоматический контроль целостности программного обеспечения и активов, используемых при принятии решений и управлении решениями

Исходные данные	Значения и комментарии	
	для 1-го/ 2-го/ 3-го/ 4-го элементов при планировании управления решениями	для 5-го/ 6-го/ 7-го/ 8-го элементов при принятии решений и управлении решениями
Твосст – среднее время восстановления требуемой нормы эффективности защиты информации после выявления нарушений	5 минут / 5 минут / 5 минут / 5 минут (включая перезагрузку программного обеспечения и восстановление данных)	5 минут / 5 минут / 5 минут / 5 минут (включая перезагрузку программного обеспечения и восстановление данных)
Тзад – задаваемая длительность периода прогноза	от одного до сорока месяцев (для определения периода, при котором сохраняются гарантии неперевышения допустимого риска для обеспечения нормы эффективности защиты информации)	

Анализ результатов расчетов показал, что для производственного процесса, процесса технического обслуживания, процесса контроля качества и процесса инвентаризации в вероятностном выражении риск нарушения требований по защите информации в течение месяца составит около 0.016 - см. рисунок 5, составляя для элементов 1-5, 7-8 – около 0.002, для 6-го элемента – 0.0003, т.е. все активы защищены в сравнительно равнопрочной степени. При увеличении периода прогноза от одного до четырех месяцев риск возрастает от 0.016 до 0.062. Для допустимого риска на уровне 0.05 обоснован период до 96 дней, при котором сохраняются гарантии неперевышения допустимого риска при осуществлении действий процесса управления решениями, характеризуемых условиями примера 3 – см. рисунок 6.

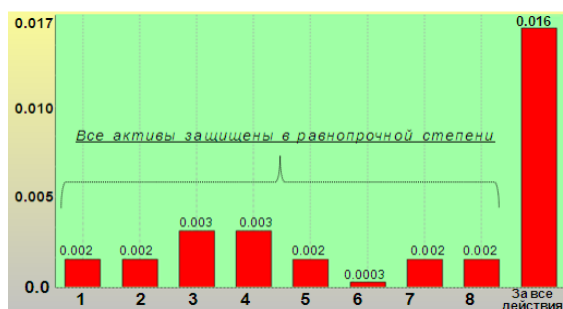


Рисунок 5 — Оценки риска нарушения требований по защите информации

в течение месяца

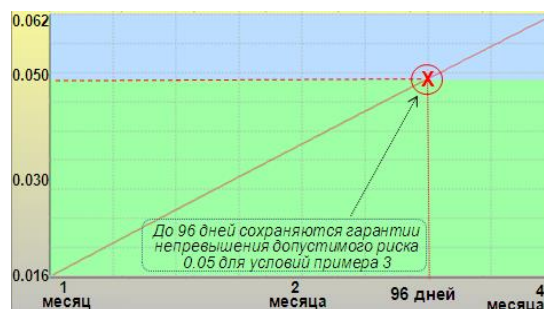


Рисунок 6 — Зависимость риска от периода прогноза длительностью

от 1 до 4-х месяцев

5.5 Пример 4. В продолжение примеров 1, 2 и 3 учитывая, что периода прогноза $T_{\text{зад.}} = 1$ месяц, по результатам 1-го и 2-го примеров выбирается значение $R_{\text{надежн.}}(T_{\text{зад.}}) = 0.210$, а по результатам 3-го примера $R_{\text{наруш.}}(T_{\text{зад.}}) = 0.016$, тогда по формуле (1)

$$R_{\text{интегр.}}(T_{\text{зад.}}) = 1 - (1 - 0.210) \cdot (1 - 0.016) \approx 0.223.$$

В итоге интегральный риск нарушения надежности реализации процесса управления решениями в течение 1 месяца с учетом требований по защите информации составит в вероятностном выражении около 0.223. При этом риск нарушения требований

по защите информации (0.016) в 13 раз меньше риска нарушения надежности реализации процесса управления решениями без учета требований по защите информации (0.210). Основной причиной высокого интегрального риска, который существенно превышает риски нарушения надежности производственного оборудования, является невысокий уровень качества используемой информации (из примера 3). Если этот уровень качества признается приемлемым или неулучшаемым и аналитиком принимается решение не учитывать приемлемое достижимое качество используемой информации в интегральных расчетах, то тогда возможно применение другой полученной в примере 2 оценки: $R_{\text{надежн}}(T_{\text{зад}}) = 0.012$. И тогда

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - (1 - 0.012) \cdot (1 - 0.016) \approx 0.028.$$

Это меньше установленного допустимого уровня 0.05, причем при аналогичных ущербах и обоснованных затратах надежность реализации процесса управления решениями оказывается соизмеримой с эффективностью защиты информации, что подтверждает сбалансированность планируемых к применению или применяемых технических решений с точки зрения достижения целей системной инженерии.

Вывод

Предлагаемый подход позволяют осуществлять анализ влияния защищенности информации на реализацию процесса управления решениями в терминах прогнозируемых рисков. Достоверность подтверждена на уровне реализации подхода по предложениям автора статьи в стандарте ГОСТ Р 59338-2021 «Системная инженерия. Защита информации в процессе управления решениями». Ожидается, что рациональное использование предложенного подхода в жизненном цикле систем будет способствовать выявлению «узких мест» и снижению рисков в процессе управления решениями с учетом требований по защите информации.

Литература

1. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд. "Вооружение, политика, конверсия", 2008. – 404с.
2. Andrey Kostogryzov, Andrey Nistratov, George Nistratov Some Applicable Methods to Analyze and Optimize System Processes in Quality Management // InTech. 2012. P. 127–196. URL = <http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management>
3. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G. Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V. 1. P. 217–244. <http://www.scirp.org/journal/ajor/>
4. Andrey Kostogryzov, Pavel Stepanov, Andrey Nistratov, George Nistratov, Oleg Atakishchev and Vladimir Kiselev Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling // Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186-192. www.dropbox.com/s/a4zw1yds8f4ecc5/AMSM2016%20Full%20Proceedings.pdf?dl=0
5. Костогрызов А.И., Степанов П.В., Нистратов А.А., Григорьев Л.И., Червяков Л.М. Прогнозирование рисков для обеспечения качества информации в сложных системах // Системы высокой доступности №3, т.2, 2016, с. 25-37
6. Vladimir Artemyev, Andrey Kostogryzov, Jury Rudenko, Oleg Kurpatov, George Nistratov, Andrey Nistratov Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20-22, 2017, Milan, Italy, pp. 368-373
7. Vsevolod Kershenbaum, Leonid Grigoriev, Petr Kanygin and Andrey Nistratov / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, pp. 55-79. <http://dx.doi.org/10.5772/intechopen.74963>
8. Probabilistic Modeling in System Engineering. / By ed. A.Kostogryzov, - London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.

9. Костогрызов А.И. Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта / БИТ. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019, сс. 220-229
10. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364.
<https://www.springer.com/gp/book/9783030468941>

Analysis of the impact of information security on the implementation of the decision-making process

Kostogryzov A.I.¹²¹

Abstract

An approach is proposed that allows analyzing the impact of information security on the implementation of the decision management process in terms of predicted risks. The use of the proposed approach in the life cycle of systems helps to identify "bottlenecks" and reduce risks in the process of managing decisions, taking into account the requirements for information protection. The efficiency of the approach is illustrated by examples.

Keywords: analysis, protection of information, model, risk, management.

¹²¹ Kostogryzov A.I., Dr.Sc., Prof., Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow

Сетевое взаимодействие в телемедицинской системе Кривошеева Д.А.¹²², Булдакова Т.И.¹²³

Аннотация. Рассмотрена проблема организации защищенного сетевого взаимодействия в телемедицинских системах, которые активно создаются и внедряются в здравоохранении. В качестве примера систем дистанционного мониторинга рассматривается телемедицинская система удаленного мониторинга состояния человека. Составной частью системы является мобильный измерительный комплекс для приема, записи и обработки биосигналов. В такой системе телемедицины решение о состоянии человека принимается на основе оценки и идентификации передаваемых данных. Отмечается актуальность исследований в области информационной безопасности телемедицинских систем и ставится задача обеспечения целостности, доступности и конфиденциальности данных. Сделан вывод, что основные исследования связаны с обеспечением безопасности взаимодействия отдельных типов компонентов телемедицинской системы и не влияют на ее сетевую структуру. Предложена иерархическая структура телемедицинской системы на основе эталонной модели OSI и описаны уровни представления данных. Выделены задачи обеспечения безопасного взаимодействия компонентов системы телемедицины на каждом иерархическом уровне предложенной модели. Приведены примеры организации защищенного сетевого взаимодействия в системе удаленного мониторинга состояния человека на различных уровнях представления данных. Предлагаются методы и алгоритмы реализации подобного взаимодействия.

Ключевые слова: телемедицина, сетевое взаимодействие, защита данных, система мониторинга состояния человека, биосигналы, РКІ.

Введение

В наши дни в системе здравоохранения активно внедряются и распространяются информационно-коммуникационные технологии, обеспечивающие своевременное взаимодействие между специалистами и пациентами [1, 2]. Одним из ярких примеров развития виртуальных инфраструктур здравоохранения являются системы телемедицины, которые дают возможность пациентам получить высококвалифицированную помощь ведущих врачей медицинских центров удаленно [3]. В настоящее время особую популярность приобрело развитие мобильных телемедицинских комплексов для работы на местах чрезвычайных происшествий.

Возникает необходимость включить подобные телемедицинские системы в единое информационное пространство. Данный шаг позволит осуществлять непрерывный мониторинг состояния здоровья человека вне зависимости от его месторасположения. В процессе подобного мониторинга происходит сбор, передача, хранение и обработка персональных данных пациента, необходимых для формирования и принятия решения о состоянии здоровья пациента. В связи с этим возникает проблема защиты данных, передаваемых и обрабатываемых телемедицинской системой [4, 5]. Нарушение хотя бы одной из составляющих информационной безопасности системы повлечет за собой не только финансовые и репутационные риски, но также нанесет моральных ущерб пациенту. При разработке подобных информационных систем необходимо уделить особое внимание обеспечению безопасности передаваемых данных по каналам связи [6, 7].

¹²² Кривошеева Дарина Александровна, Московский государственный технический университет имени Н.Э. Баумана, darinaaleks@gmail.com

¹²³ Булдакова Татьяна Ивановна, Московский государственный технический университет имени Н.Э. Баумана, buldakova@bmstu.ru

Особенности телемедицинской системы дистанционного мониторинга состояния человека

Одним из перспективных направлений в развитии дистанционного мониторинга является интеграция датчиков в аксессуары, различную одежду и мобильные телефоны [8-10]. На пациенте устанавливается система нательных датчиков, которые регистрируют физиологическую информацию и передают ее по беспроводным каналам связи на сервер (Рис. 1).

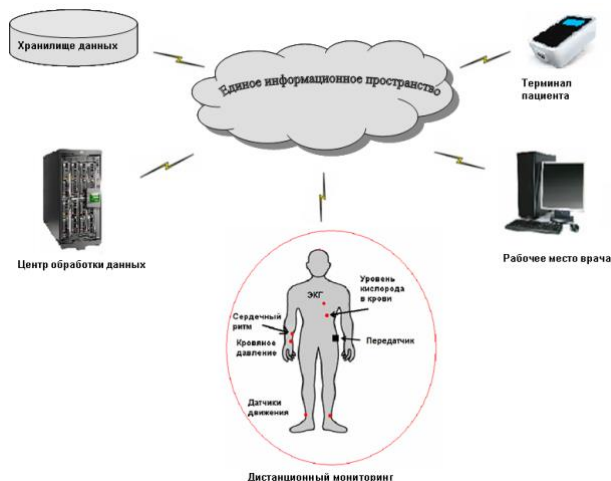


Рис. 1 Основные компоненты системы дистанционного мониторинга

Первоисточниками информации о состоянии пациента выступают различные датчики, регистрирующие биосигналы человека. В связи с этим одним из основных составляющих системы дистанционного мониторинга состояния человека является мобильный измерительный комплекс. Он производит съем, регистрацию и первичную обработку биосигналов. Хранение, вычисление и визуализация собранных данных требует больших вычислительных ресурсов, предоставляемых виртуальной инфраструктурой с помощью облачных технологий. Датчики могут отправлять данные напрямую в облако или же через промежуточную станцию, например, мобильный телефон. Обслуживающий персонал и пациент могут просматривать собранную медицинскую информацию напрямую из облака в режиме реального времени и принимать решения в соответствии с текущим состоянием пациента.

Несмотря на достаточное многообразие предлагаемых вариантов реализации телемедицинских систем, в них не уделяется должного внимания вопросам информационной безопасности персональных данных. Большинство исследований направлено на обеспечение безопасности взаимодействия отдельных компонентов телемедицинской системы, но нет рассмотрения общей безопасности информационной системы телемедицины [5-7, 11]. Сетевое взаимодействие в телемедицинских системах реализуется на разных уровнях, однако вопросы комплексной защиты информационных процессов, протекающих на разных уровнях сетевого взаимодействия, не рассматриваются.

Анализ сетевого взаимодействия в системах телемедицины

Для описания процессов, возникающих при сетевом взаимодействии, будем использовать сетевую модель OSI (Open Systems Interconnection). В данной модели сетевого взаимодействия выделяют семь уровней, каждый из которых необходим для выполнения различных частей процесса взаимодействия открытых систем [12, 13]. В процессе передачи данных каждый уровень модели OSI выполняет определенную функцию. Дополним описание уровней модели задачами обеспечения защищенного сетевого взаимодействия в телемедицинской системе (табл. 1).

Табл. 1.

Уровень	Название	Основные функции	Задачи обеспечения безопасности передачи данных в телемедицине
7	Прикладной уровень	Поддержка прикладных процессов (определение доступности сетевых ресурсов, синхронизации связи)	Идентификация пользователей телемедицинской системы мониторинга
6	Уровень представления	Организация данных при их передаче (преобразование форматов данных, шифрование/дешифрование данных)	Определение способа криптозащиты. Выбор алгоритма шифрования
5	Сеансовый уровень	Управление сеансом связи	Аутентификация пользователей системы и проверка их полномочий
4	Транспортный уровень	Обеспечение надежности и корректности передачи данных	Контроль целостности передаваемых конфиденциальных данных и факта передачи информации
3	Сетевой уровень	Определение пути передачи данных, маршрутизация и пересылка	Разграничение доступа к сетевым ресурсам, мониторинг сетевого трафика, скрытие от злоумышленников таблиц маршрутизации
2	Канальный уровень	Обеспечение взаимодействия сетей на физическом уровне, передача и прием пакетов	Обеспечение достоверности передачи информации (степени соответствия принятого сообщения переданному)
1	Физический уровень	Работа со средой передачи, сигналами и битами	Обеспечение защищенности физической среды передачи данных

Далее сгруппируем уровни модели OSI по типам задач обеспечения безопасности передачи данных:

1) обеспечение доступа к сети на уровне физической среды передачи данных (1 и 2 уровни модели OSI);

2) обеспечение надежной передачи данных на уровне маршрутизации (3 и 4 уровни модели OSI);

3) разграничение доступа к сетевым ресурсам (5 уровень модели OSI);

4) обеспечение защищенного взаимодействия на уровне процессов (6 и 7 уровни модели OSI).

Рассмотрим подходы к решению указанных типов задач обеспечения защищенного сетевого взаимодействия. Каждому типу задач поставим в соответствие уровень представления сетевого взаимодействия.

Первый и второй уровни представления сетевого взаимодействия не накладывают

ограничений на тип системы. Поэтому достаточно применить известные меры защиты. Третий уровень представления сетевого взаимодействия учитывает права пользователей при доступе к сетевым ресурсам. Для решения данного вопроса необходимо будет применить ролевое разграничение доступа. Последний, четвертый уровень, требует применения криптографических алгоритмов для идентификации пользователей и передачи данных.

Существует достаточно больше количество способов для обеспечения защиты данных при идентификации, например, смарт-карты пациентов, USB-токены врачей. Наиболее коммерчески простым и эффективным способ обеспечения безопасности передачи персональных данных будет являться технология PKI (public key infrastructure), которая себя уже зарекомендовала на множестве систем обработки персональных данных.

При применении технологии PKI выделяются следующие преимущества

- Благодаря процессу проверки, проводимому Центром сертификации и использованию закрытого и открытого ключа, PKI обеспечивает бесперебойную аутентификацию пациента или врача.
- Зашифровывая данные между пациентом и врачом PKI поможет обеспечить безопасность исходных данных.
- С помощью хеширования PKI позволяет получателю проверить сохранился ли изначальный вид передаваемых данных.
- PKI предоставляет возможность обеспечения неотрекаемости данных.

Выводы

Было получено, что при определении методов, алгоритмов и протоколов защиты передаваемых данных требуется учитывать различные уровни представления сетевого взаимодействия в телемедицинских системах. Была рассмотрена система дистанционного мониторинга состояния пациентов. Предложенная иерархическая модель представления сетевого взаимодействия в телемедицинской системе полностью описывает основные функции и задачи защиты информации каждого уровня. Были рассмотрены преимущества использования технологии PKI для обеспечения безопасности передаваемых персональных данных.

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] Llinás G., Rodríguez-Iñesta D. et al. Comparison of Websites from Spanish, American and British Hospitals // Methods of Information in Medicine. 2008. Vol. 47; Issue 2. -P. 124-130.
- [3] Perednia D.A., Allen A. Telemedicine technology and clinical applications // JAMA 2006. No. 273. -Pp. 483-488.
- [4] 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.
- [5] Appari A. and Johnson M.E. Information Security and Privacy in Healthcare: Current State of Research // International Journal of Internet and Enterprise Management, vol. 6, no. 4, 2010, Pp. 279-314.
- [6] Buldakova T.I., Dzhalolov A.S. Analysis of data processes and choices of data-processing and security technologies in situation centers // Scientific and Technical Information Processing. 2012. Vol. 39(2). -Pp. 127-132.
- [7] Анализ информационных рисков виртуальных инфраструктур здравоохранения / Т.И. Булдакова, С.И. Суятинов, Д.А. Миков // Информационное общество. 2013. № 4. -С. 6.
- [8] Schmidt S., Schuchert A., Krieg T., Oeff M. Home telemonitoring in patients with chronic heart failure // Deutsches Ärzteblatt International. 2010. Vol. 107(8). -Pp. 131-138.

<https://doi.org/10.3238/arztebl.2010.0131>.

[9] Paradiso R., Loriga G., Taccini N. A Wearable Health Care System Based on Knitted Integrated Sensors // IEEE Transactions on Information Technology in Biomedicine. 2005. V. 9, N. 3. -P. 337-344.

[10] Winters J., Wang Y. Wearable Sensors and Telerehabilitation // IEEE Engineering in Medicine and Biology Magazine. 2003. No. 3. -Pp. 56-65.

[11] 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(1). -Pp. 60-68.

[12] Suresh P. Survey on seven layered architecture of OSI model // International Journal of research in computer applications and robotics. 2016. Vol. 4, Issue 8. -Pp. 1-10.

[13] Chaturvedi A., Verma P. Popularly Used Security Protocols on All Layers of Network Communication // International Journal of Trend in Scientific Research and Development. 2018. Vol. 2, issue 2. -Pp.81-87. <http://www.ijtsrd.com/papers/ijtsrd8312.pdf>.

Networking in the telemedicine system

Krivosheeva D.A.¹²⁴, Buldakova T.I.¹²⁵

Abstract. Problem of the organization of secure network interaction in telemedicine systems, which are actively being created and implemented in healthcare, is considered. As an example, a telemedicine system for remote monitoring of a person's state is considered; the component of system is a mobile measuring complex for picking up, recording and processing biosignals. In such a telemedicine system, the decision on the state of a person is made on the basis of the assessment and identification of transmitted data. The relevance of research in the field of information security of telemedicine systems is noted, and the task of ensuring the integrity, accessibility and consistency of data is posed. It is concluded that the main studies are related to ensuring the security of the interaction of certain types of components of the telemedicine system and do not affect its entire network structure. A hierarchical structure of the system under study is proposed on the basis of the OSI reference model and the levels of data presentation are described. The tasks of ensuring the safe interaction of the components of the telemedicine system at each hierarchical level of the proposed model are highlighted. Examples of the organization of secure network interaction in the system of remote monitoring of the human state at various levels of data presentation are given. Methods and algorithms for the implementation of such an interaction.

Keywords: telemedicine, networking, data protection, human health monitoring system, biosignals, PKI.

¹²⁴ Krivosheeva Darina Aleksandrovna, BMSTU, Moscow, darinaaleks@gmail.com

¹²⁵ Buldakova Tatiana Ivanovna, BMSTU, Moscow, buldakova@bmstu.ru

Улучшение метода аутентификации в алгоритме WPA2-PSK WI-FI

Ларин В.С.¹²⁶

Аннотация. Данная статья направлена на исследования безопасности существующего алгоритма аутентификации WPA2-PSK. В существующей схеме используется схема, в которой главную роль играет парольная фраза, придуманная пользователем. Существующие программные и аппаратные решения позволяют перехватывать 4-стороннее рукопожатие и путём перебора восстановить парольную фразу. В данной статье предлагается использовать вместо пароля ключ, который будет обмениваться между клиентом и точкой доступа на основе эллиптической кривой. Данное решение позволяет использовать ключи на эллиптических кривых, которые имеют небольшую длину, но также надежны, как и длинные ключи RSA порядка 3072 бита.

Ключевые слова: четырёхстороннее рукопожатие, эллиптические кривые, RSA, парольная фраза

Введение

Беспроводные сети в многих местах массового скопления людей: аэропортах, вокзалах, кафе, ресторанах. История разработки стандартов беспроводных сетей началась в 1990 году, когда был образован комитет 802.11 всемирной организацией IEEE (Институт инженеров по электричеству и электронике). Толчок к развитию беспроводных технологий дала Всемирная паутина. В конце XX века пользователям была предложена WAP (Wireless Application Protocol) - услуга, не вызвавшая большого доверия у населения. В основном это были информационные услуги, предоставляющие информацию о погоде, новостях, расписаниях поездов и самолетов и другие услуги [1]. В период с 2000 до 2010 годов количество пользователей беспроводного Интернет дошло до нескольких миллионов. Вопросы безопасности вышли на первый план после появления беспроводной связи. Основной проблемой использования беспроводной связи в коммерческих предприятиях или местах массового скопления людей (кафе, рестораны, вагоны метро) является перехват сообщений пользователей. Для решения данной проблемы необходимо модифицировать стандарт беспроводной связи. Существует несколько механизмов защиты Wi-Fi сетей: WEP, WPA, WPA2. Так механизм защиты WEP является устаревшим, поэтому его не следует применять для защиты в беспроводной сети, потому что в интернете полно различных бесплатных утилит, с помощью которых можно получить ключ для расшифрования трафика. Для домашних сетей сейчас в основном применяется механизм защиты WPA2-PSK, в котором применяются новые алгоритмы шифрования и аутентификации. Существенным для развития беспроводных технологий является и возможность их использования домашними пользователями. Так как число устройств в домашней сети растёт, то количество проводов тоже увеличивается, поэтому в данном случае лучше переходить на беспроводные технологии. Беспроводная передача данных обеспечивает рост производительности доступа к информации, повышает качество обслуживания клиентов, создает конкурентные преимущества (скорость обмена информацией повышается, таким образом уменьшается время ответа).

Описание существующего механизма аутентификации

Механизм аутентификации WPA-PSK уязвим для атак по словарю. Эта атака основана на перехвате четырехстороннего рукопожатия между клиентом и точкой доступа, которые явно предоставляют достаточно информации для начала атаки. PSK

¹²⁶ Ларин Василий Сергеевич, студент, МГТУ им. Н.Э. Баумана, v.larin@npo-echelon.ru

использует псевдослучайную функцию PBKDF2, которая преобразует пароль (от 8 до 63 символов ASCII) в 256-битный ключ (PMK) (рис. 1) [2]. Для вычисления ключа необходимо подать на функцию пять значений: имя wi-fi сети (SSID), длину значения SSID, пароль, 256 (длина ключа), 4096 (количество итераций) [3]. Из всех значений неизвестно только значение пароля.

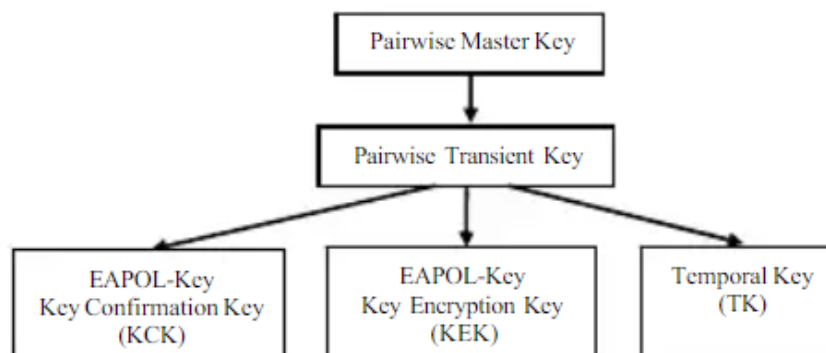


Рис. 1 Иерархия ключей

Так как не используется, сервер аутентификации, то $PMK=PSK$. PSK генерируется с помощью функции PBKDF2, которая принимает на вход параметры (пароль, SSID-имя точки доступа, длину SSID. Функция хэширует данные 4096 раз. Длина парольной фразы от 8 до 64 символов. Для получения ключа РТК используются следующие значения PRF (PMK, Nonce_A, Nonce_C, MAC_A (адрес станции), MAC_C (адрес клиента)). Набор этих значений подаётся в хэш-функцию $PRF = HMAC-SHA1$.

Атакующий с помощью стороннего программного и аппаратного обеспечения может перехватить 4-стороннее рукопожатие: Nonce_A, Nonce_C, MAC_A, MAC_C. Но PMK нужно вычислить. $PMK=PSK$ и для его вычисления нужно знать только парольную фразу.

Возможный вариант улучшения

Для того чтобы предотвратить использование пароля, предполагается использовать ключ вместо passphrase. Точка доступа отправляет открытый ключ клиенту, закрытый ключ хранится у точки доступа. Закрытый и открытый ключи вычисляются на основе эллиптической кривой. Клиент генерирует ключ общий - key и случайное число – k. Отправляет точке доступа два значения:

$$k * G \quad (1)$$

$$key + k * Q, \quad (2)$$

$$Q = n * G \quad (3)$$

Q - открытый ключ, а n – закрытый.

Точка доступа получает:

$$key + k * Q - n * k * G = key \quad (4)$$

Выводы

Таким образом точка доступа и клиент выработали общий ключ на основе эллиптических кривых. Данный способ предотвращает атаку злоумышленника, который прослушивает пассивно трафик между клиентом и точкой доступа.

Данный способ выигрывает по длине ключей, по сравнению с RSA (табл. 1).

Таблица 1.

Рекомендации NIST по выбору длины ключей, для обеспечения, соответствующей безопасности.

№ п/п	Security Bit Level	RSA	ECC
1	80	1024	160

2	112	2048	224
3	128	3072	256
4	192	7680	384
5	256	15360	512

Литература

1. Смирнова Е., Пролетарский А., Ромашкина Е. Технологии современных беспроводных сетей Wi-Fi: Учебное пособие – М.: МГТУ им. Н.Э. Баумана, 2017. – 446 с.
2. Педжман Р., Джонатан Л. Основы построения беспроводных локальных сетей стандарта 802.11.: Пер. с англ – М.: Издательство дом «Вильямс», 2004. -304 с.: ил.
3. Харитонов Е.Г. Анализ уязвимостей беспроводных сетей стандарта IEEE 802.11. Студенческая наука для развития информационного общества. сборник материалов VII Всероссийской научно-технической конференции. 2018. С. 507-511.
4. Василенко К.А. WI-FI сети: Угрозы безопасности и технологии защиты. Российская наука и образование сегодня: проблемы и перспективы. 2019. № 3 (28). С. 89-91.
5. Денисов Д.В., Иванов Д.И. Влияние характеристик пароля на защищенность WI-FI сети. Colloquium-journal. 2019. № 10-2 (34). С. 94-97.
6. Прокопайло А.А., Дьяченко Н.В. Методы взлома и защита WI-FI сетей. В сборнике: Реформирование и развитие естественных и технических наук. сборник материалов XII-ой международной очно-заочной научно-практической конференции. 2019. С. 100-103.
7. Михайлюк А.А. Безопасность WI-FI сетей. Проникновение и защита. В книге: ШКОЛЬНАЯ СЕКЦИЯ: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. материалы 57-й Международной научной студенческой конференции. 2019. С. 38.
8. Coleman D., Westcott D. CWNA Certified Wireless Network Administrator: STUDY GUIDE Fifth Edition, 2018. – 989 p.
9. Badman L., Bartz R. CWSP Certified Wireless Security Professional, 2016. – 461 p.
10. Finn M., Haugen O. Cryptanalysis of IEEE 802.11i TKIP: Norwegian University of Science and Technology, 2009. – 156 p.

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

Improvement of the authentication method in the WPA2-PSK WI-FI algorithm

Larin V.S.¹²⁷

Abstract. *This article aims to investigate the security of the existing WPA2-PSK authentication algorithm. The existing scheme uses a scheme in which a user-invented passphrase plays the main role. Existing software and hardware solutions allow you to intercept a 4-way handshake and recover a passphrase by brute-force. This article proposes to use instead of a password a key that will be exchanged between the client and the access point based on an elliptic curve.*

Keywords: *four-way handshake, elliptic curves, RSA, passphrase.*

¹²⁷ Larin Vasily, student, Bauman Moscow State Technical University, Moscow, v.larin@npo-echelon

Методика разделения областей кода и данных в образе встраиваемого программного обеспечения контроллеров архитектуры ARM
Малахов М.В.¹²⁸, Воронина Е.Н.¹²⁹

***Аннотация.** Актуальность решения задачи поиска уязвимостей и недеklarированных возможностей во встраиваемом программном обеспечении (ВПО) на сегодняшний день не вызывает сомнений. Одной из основных проблем при решении данной задачи является недоступность исходных кодов ВПО. Для проведения поиска уязвимостей в образе или исполняемом коде ВПО используются различные техники, причём практически все они так или иначе используют дизассемблирование, одним из основных этапов которого является разделение областей кода и данных. В работе проводится анализ современных подходов к разделению областей кода и данных в исполняемом коде, выявляются их недостатки и предлагается новая методика, основанная на машинном обучении, для решения поставленной задачи.*

Ключевые слова: информационная безопасность, поиск уязвимостей, дизассемблирование, машинное обучение.

Введение

В настоящий момент времени с развитием вычислительной техники всё большее значение приобретает проблема обеспечения информационной безопасности встраиваемых систем, которые глубоко интегрированы не только в повседневную жизнь современного человека, но и на объекты критической инфраструктуры.

Одной из основных задач, решаемых в процессе обеспечения информационной безопасности встраиваемых систем, является задача поиска уязвимостей и недеklarированных возможностей (НДВ) [1] во встраиваемом программном обеспечении (ВПО) таких систем.

В связи с тем, что на сегодняшний день большинство компонентов встраиваемых систем, а в некоторых случаях и полноценные системы поступают из-за рубежа в качестве законченных решений без доступа к исходному коду, возникает необходимость анализа исполняемого кода указанных компонентов и систем на предмет поиска в них уязвимостей и НДВ.

1 Современные подходы к анализу исполняемого кода ВПО

Разработка отдельных подходов к решению задачи поиска уязвимостей и НДВ в образе ВПО проводится как отечественными, так и зарубежными авторами, причём, если отечественные авторы больше сосредоточены на анализе кода во время его исполнения [2-4], то иностранные авторы, помимо интересных работ, связанных с конколическим исполнением ВПО микроконтроллеров [5], также предлагают достаточно инновационные подходы [6, 7] к поиску уже известных уязвимостей в дизассемблированном исполняемом коде ВПО. Причём, необходимо отметить, что наличие дизассемблированного кода является важным условием успешного применения не только последней группы подходов, но также и всех представленных выше.

Если же говорить об обеспечении информационной безопасности устройств с ВПО с точки зрения регламентирующих документов, то нельзя не упомянуть Методику ФСТЭК [8], направленную на выявление уязвимостей и НДВ в программном

¹²⁸ Малахов Михаил Валерьевич, МГТУ им. Н.Э. Баумана, Москва, misha.malaxow@yandex.ru

¹²⁹ Воронина Екатерина Николаевна, МГТУ им. Н.Э. Баумана, Москва, ekvoro@gmail.com

обеспечении, частным случаем которого является ВПО. В соответствии с указанной Методикой, работами, направленными непосредственно на анализ кода, являются: экспертный анализ, статический анализ, динамический анализ и ручной анализ. В условиях отсутствия исходных кодов Методика регламентирует работы по экспертному анализу, который включает в себя дизассемблирование исполняемого кода; по динамическому анализу, который заключается в фаззинг-тестировании и анализе трасс выполнения, причём по крайней мере анализ трасс выполнения требует наличия восстановленного (т.е. хотя бы дизассемблированного) кода; и по ручному анализу, одной из основных задач которого является анализ отдельных наиболее важных участков кода, что в условиях отсутствия исходных кодов также влечёт за собой необходимость наличия восстановленного кода.

Таким образом, вне зависимости от подходов, применяемых к анализу образа ВПО, задача верного его дизассемблирования является одной из основополагающих. Основными работами, проводимыми в процессе дизассемблирования, являются: разделение кода и данных и замена абсолютных адресов на символические [9]. Настоящая работа посвящена поиску наиболее точного способа выполнения первой из указанных работ, а именно разделению областей кода и данных в образе ВПО.

В данной работе приводится решение задачи разделения областей кода и данных в образе ВПО, функционирующего на ARM контроллерах, в связи с тем, что в настоящий момент времени микроконтроллеры с архитектурой ARM являются наиболее популярными.

2 Существующие подходы к разделению областей кода и данных в образе ВПО

Для решения задачи разделения кода и данных в исполняемом коде обычно применяются методики, опирающиеся на один из следующих подходов [10]:

- применение алгоритма линейной развертки;
- применение алгоритма рекурсивного спуска.

При использовании алгоритма линейной развертки дизассемблирование начинается с первого байта в сегменте кода и последовательно продвигается, обрабатывая команды одну за другой, пока не будет достигнут конец сегмента. При этом не производится попыток понять логику передач управления в программе посредством распознавания команд перехода таких, например, как условия. Основным недостатком данного подхода является невозможность распознать данные, если они смешаны с кодом, что делает данный подход неприменимым для анализа образа ВПО.

Алгоритм рекурсивного спуска использует концепцию передачи управления, определяющую, должна ли команда быть дизассемблирована по наличию или отсутствию на нее ссылок от других команд. Использование данного подхода в чистом виде гарантирует, что данные не будут распознаны как код, однако в таком случае код, вызываемый с помощью динамической адресации, будет распознан как данные. В целях устранения данного недостатка дизассемблерами применяются различные эвристики, однако в данном случае зачастую возникают случаи ошибочного распознавания данных как кода.

Алгоритм рекурсивного спуска используется в дизассемблере IDA Pro, который является наиболее популярным и продвинутым в настоящий момент времени. Данный дизассемблер показывает достаточно высокий процент верного распознавания областей кода и данных для бинарных файлов, скомпилированных для архитектур x86 и x64. Однако при работе с файлами образов ВПО даже IDA Pro допускает непозволительно много ошибок. Так, значение метрики достоверности (отношение числа правильных предсказаний к общему числу меток) образов ВПО проектов с открытым исходным кодом по результатам проведенных экспериментов составляет в среднем около 66%.

Таким образом, в связи с несовершенством существующих подходов и средств их

реализации возникает необходимость в разработке нового подхода к разделению кода и данных в исполняемом коде ВПО; однако необходимо отметить, что в общем случае задача разделения кода и данных является алгоритмически неразрешимой [9]. Именно этот факт обуславливает применение для решения данной задачи разделения кода и данных различных эвристических методов и жадных алгоритмов, но, как было показано, данные подходы имеют недостаточную точность решения поставленной задачи при работе с ВПО, что влечет за собой большие временные затраты исследователя на исправление допущенных при использовании данных подходов ошибок.

В связи с этим возникает необходимость разработки новой методики для решения задачи разделения областей кода и данных в образе ВПО. Причём, в связи с вышеуказанными особенностями решаемой задачи в качестве базового подхода разрабатываемой методики предлагается выбрать машинное обучение.

3 Методика разделения областей кода и данных в образе ВПО

Предлагаемая в настоящей работе методика, представленная на рисунке 1, принимает на вход образ ВПО, а результатом её работы является решение о принадлежности каждого байта принятого образа к классу кода или данных.

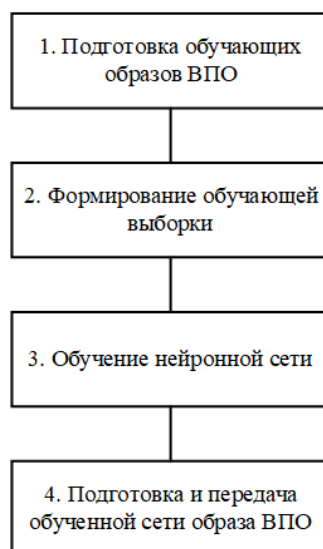


Рисунок 1 – Методика разделения областей кода и данных в образе ВПО

При выполнении первого этапа представленной методики последовательно производятся следующие действия: поиск проектов с открытым исходным кодом, разработанных для исследуемой архитектуры микроконтроллера; балансирование объёма кода и данных в найденных проектах посредством добавления констант; компиляция собранных проектов как в бинарный образ, так и в размеченный исполняемый файл.

На втором этапе сначала производится отнесение каждого байта обучающих образов ВПО к классу кода или данных с использованием полученного на первом этапе размеченного исполняемого файла, а затем производится формирование обучающих векторов, состоящих из последовательности байт, по которым нейронная сеть должна предсказывать класс среднего байта данного вектора.

На третьем этапе происходит непосредственно обучение нейронной сети. По итогам проведенного анализа в качестве архитектуры нейронной сети, подходящей для

решения поставленной задачи, выбрана рекуррентная нейронная сеть, а её параметры подобраны с использованием специальной библиотеки [11].

На четвертом этапе производится разбиение исследуемого образа ВПО на вектора байт, принимаемых нейронной сетью в качестве входных значений, с последующей их передачей на вход нейронной сети.

4 Апробация предложенной методики

Тестирование предложенной методики проводилось на образах ВПО с открытым исходным кодом, собранных для архитектуры ARMv7.

В качестве обучающего образа ВПО был выбран проект с открытым исходным кодом – BusyBox, необходимо отметить, что выбор данного проекта для обучения является достаточно удобным, так как, во-первых, данный проект имеет большую и разнообразную кодовую базу и, во-вторых, он может быть скомпилирован для различных микроконтроллерных архитектур. Балансирование кода выбранного проекта осуществлялось с использованием разработанного специального программного обеспечения. Классификация каждого байта обучающего образа ВПО на основе размеченного исполняемого файла проводилась с помощью разработанного плагина для IDA Pro. В результате применения методики удалось верно классифицировать 94% байт.

Таким образом, результативность процесса разделения областей кода и данных в образе ВПО при применении предложенной методики увеличилась на 17% по сравнению с применением стандартных средств IDA Pro.

Заключение

Необходимость обеспечения информационной безопасности различных электронных устройств и их компонентов не вызывает сомнения. При решении данной задачи исследователям зачастую приходится работать в условиях отсутствия исходных кодов ВПО, что влечёт за собой необходимость дизассемблирования образа ВПО. Одной из важнейших задач указанной процедуры является разделение областей кода и данных в образе ВПО. Решению указанной задачи посвящена настоящая работа.

В работе проведен анализ современных подходов к разделению областей кода и данных в образе программного обеспечения, приведены их достоинства и недостатки, а также проведена попытка автоматического разделения указанных областей с помощью промышленного средства обратной разработки, которое показало весьма посредственную точность решения указанной задачи. Это обуславливает необходимость разработки новой методики для решения задачи разделения областей кода и данных в образе ВПО.

В работе предложена основанная на машинном обучении методика решения поставленной задачи, подробно описаны этапы её применения, а также проведена её апробация на образе ВПО, скомпилированном для архитектуры ARMv7. В результате применения разработанной методики удалось повысить результативность процесса разделения областей кода и данных в образе ВПО на 17% по сравнению с применением стандартных средств промышленного дизассемблера.

Направлением дальнейших исследований является апробация предложенной методики при работе с другими микроконтроллерными архитектурами, а также её внедрение в качестве плагина в дизассемблер IDA Pro.

Литература

1. Осовецкий Л. Г. Технология выявления недекларированных возможностей при сертификации промышленного программного обеспечения по требованиям безопасности информации // Вопросы кибербезопасности. 2015. № 1 (9). С. 60-64.
2. Веселов Ю.Г. Проектирование средства инструментации исполняемого кода контроллеров в интересах обеспечения информационной безопасности промышленных АСУ / Ю.Г. Веселов, А.С. Островский, М.В. Малахов и др. // Промышленные АСУ и контроллеры, 2020, №8, с. 33-39.
3. Аристов Р.С. Разработка программной платформы КОРУСАТ эмуляции сложных вычислительных систем / Р.С. Аристов, А.А. Гладких, В.Н. Давыдов, М.О. Комахин // Наноиндустрия, 2019, № S, с. 350-352.
4. Бугеря А.Б. Программный комплекс для выявления недекларированных возможностей в условиях отсутствия исходного кода / А.Б. Бугеря, В.Ю. Ефимов, И.И. Кулагин и др. // Труды ИСП РАН, 2019, том 31, выпуск 6, с. 33-64.
5. Hernandez G. Toward automated firmware analysis in the IoT era / G. Hernandez, F. Fowze, D. Tian and others // IEEE Security and Privacy Magazine, august 2019, pp. 38-46.
6. Zhao D. CVSkSA: cross-architecture vulnerability search in firmware based on KNN-SVM and attributed control flow graph / D. Zhao, H. Lin, L. Ran // Software Quality Journal, 2019, vol. 27, 25 p.
7. Echweiler S. discov:RE Efficient Cross-Architecture Identification of Bags in Binary Code / S. Echweiler, K. Yakdan, E. Gerhards-Padilla // NDSS'16, 21-24 February, 2016, p. 15.
8. Сердечный А.Л. Методика выявления уязвимостей и недекларированных возможностей в ПО. ИТ на службе оборонно-промышленного комплекса, Екатеринбург, 2019, 15 слайдов.
9. Долгова К.Н. О некоторых задачах обратной инженерии / К.Н. Долгова, Чернов А.В. // Труды ИСП РАН, 2008, том 15, с.119-134.
10. Оголюк А.А. Защита приложений от модификации: учебное пособие. – СПб: СПбГУ ИТМО, 2013. – 56 с.
11. Bursztein E. Cutting Edge TensorFlow. URL: <https://elie.net/static/files/cutting-edge-tensorflow-keras-tuner-hypertuning-for-humans/cutting-edge-tensorflow-keras-tuner-hypertuning-for-humans-slides.pdf> (view date 19.12.2020).

Научный руководитель или консультант: Островский Александр Сергеевич, доцент, доктор технических наук, профессор кафедры ИУ8 МГТУ им. Н.Э. Баумана, oas@bmstu.ru.

The approach for separating code and data in binary firmware of ARM microcontrollers

Malahov M.V.¹³⁰, Voronina E.N.¹³¹

Abstract. *The task of searching vulnerabilities and undeclared features in firmware is very actual in our days. The main challenge of this task is the fact, that firmware source code usually absents. The approaches, that may be used for searching vulnerabilities in binary firmware, need disassembled code. One of the main disassembly challenges is the process of separating code and data in binary. In this paper, we analyze modern approaches for separating code and data in binary, show their disadvantage and propose new technique, based on machine learning, to solve this task.*

Keywords: *information security, vulnerabilities search, disassembling, machine learning.*

¹³⁰ Mihail Malahov, MSTU, Moscow, Russia, misha.malaxow@yandex.ru

¹³¹ Ekaterina Voronina, MSTU, Moscow, Russia, ekvoro@gmail.com

Средство распознавания полиморфных эксплойтов для ARM-систем на основе поведенческих признаков

Маркин Д. О.¹³², Миначев В. М.¹³³

Аннотация. В статье описан алгоритм динамического анализа с выделением поведенческих признаков вредоносного программного обеспечения для процессоров с ARM архитектурой. Описана модель эксплойта полиморфной структуры с применением шелл-кода и его динамические признаки. Представлена схема принятия решения об отнесении исполняемого кода к вредоносному. Разработан метод обнаружения подозрительного поведения, и классификации его, как полиморфный код или шелл-код, а также алгоритмы функционирования отдельных элементов прототипа средства анализа. На тестовом наборе данных была проведена оценка эффективности алгоритма, и выделены направления дальнейшего исследования.

Ключевые слова: обнаружение вредоносного кода, динамический анализ, шелл-код, эмуляция, набор ассемблерных команд, полиморфная структура кода.

Введение

В настоящее время большое распространение набирают портативные и носимые устройства, основным производителем процессоров этих устройств является компания ARM [1]. Данная архитектура относится к так называемым load-store архитектурам (PowerPC, SPARC, RISC-V, MIPS) [2]. Одноименная архитектура имеет многочисленные специфические особенности по сравнению с распространенными Intel x86/x64. Для обеспечения информационной безопасности, средства вычислительной техники и программное обеспечение (ПО) должны быть сертифицированы независимо от их архитектуры.

Необходимость в постоянном совершенствовании и извлечении максимальной возможной экономической выгоды потребляемых ресурсов, могут побудить к переходу на современные технические решения. Для этого необходимо наличие эффективных средств анализа внедряемых средств.

Вопросами анализа уязвимостей, недеklarированных возможностей и способов их обнаружения занимается большое число отечественных и зарубежных исследователей. Работы Маркова А. С. [3], Гайворонской С.А. [4], Мацкевича А. Г. и Горюнова М. Н. [5], Wagas A. [6] описывают методы анализа, построенные на основе статических и динамических методов. Работы Гамаюнова Д. Ю. и Сковороды А. А. [7,8], Jagsir S. и Jaswinder S. [9] – методы анализа с применением машинного обучения.

Для современных устройств характерно отсутствие исходного кода ПО и разнообразие операционных систем. Поэтому статический анализ исполняемых файлов бывает затруднительным и нерезультативным. Принято считать, что автор вредоносного ПО обладает современными и уникальными методами, обнаружить которые не позволит сигнатурный анализ. Чтобы повысить эффективность существующих систем анализа ПО, требуется алгоритм распознавания вредоносного ПО на основе динамических эвристических признаков.

1. Модель вредоносного программного обеспечения

Для разработки алгоритма и проведения начального тестирования прототипа средства динамического анализа был собран набор полезных нагрузок эксплойтов для

¹³² Маркин Дмитрий Олегович, канд. техн. наук, Академия ФСО России, г. Орёл,
mdo@academ.msk.rsnet.ru

¹³³ Миначев Владислав, Академия ФСО России, г. Орёл

процессоров с ARM архитектурой базы данных www.exploit-db.com. Из каталога /bin UNIX-подобной системы Raspbian GNU/Linux 10 аппаратной платформы ARMv6 взяты легитимные бинарные файлы, и извлечен код выполняемой программы этих файлов (секция «.text»). Требуется такой алгоритм, который позволит распознать вредоносное ПО, на основе особенностей построения и использования существующих уязвимостей архитектуры для построения эксплойтов со статичной и полиморфной структурой

Распространённой уязвимостью является применение эксплойтов, число обнаружений которых около 250 тысяч в день согласно сведениям Лаборатории Касперского [10]. Их классифицируют по эксплуатируемым уязвимостям: переполнение стека, переполнение буфера, ошибки конфигурирования, уязвимости конкретного ПО и др. Полезная нагрузка, как и сам эксплойт может быть разной. Шелл-код, выступая в качестве полезной нагрузки позволяет нарушителю запустить программную оболочку компьютерной системы с правами администратора или провести несанкционированное воздействие. Данные возможности шелл-кода, также как и эксплойта заключаются в его полезной нагрузке. Вредоносное ПО полиморфной структуры состоит из трех частей – расшифровщика, шелл-кода и полезной нагрузки. Вторая и третья часть представляет из себя вредоносное ПО статической структуры, и может исследоваться отдельно. Поэтому разрабатываемый алгоритм должен позволять обнаружить вредоносное ПО различных структур.

Зашифрованный шелл-код находится в зараженном приложении, и не обнаруживается методами статического анализа. Расшифровщик производит чтение, изменение (расшифрование) и запись кода приложения в оперативной памяти. Для своей работы расшифровщик использует:

- значение регистра PC (program counter), хранящего адрес текущей инструкции;
- команды обработки данных (xor, eor и др.);
- инструкции чтения и записи памяти – str и ldr соответственно.

После успешной работы расшифровщика в оперативной памяти находится шелл-код с полезной нагрузкой в привычном виде. Шелл-код обеспечивает состояние регистров для запуска системного вызова svc. Выполняемая функция зависит от параметра инструкции svc и значений некоторых регистров. Регистры заполняются инструкцией mov.

2. Алгоритм обнаружения вредоносного приложения

Для работы метода необходима построенная трасса выполнения бинарного кода, представляющая собой совокупность адресов в памяти, инструкций, и значений регистров на каждом шаге. Алгоритм распознавания вредоносного ПО представляет собой схему принятия решения, основными элементами которой являются классификаторы K_i . Каждый K_i по показателям исследуемого объекта O определяет относится ли O к i -ому классу вредоносного ПО. Схема по совокупности решений K_i принимает свое решение об отнесении O к вредоносному ПО.

В трассе выполнения приложения T выделяются поведенческие признаки полиморфного-кода и статического шелл-кода. Для этого T рассматривается как последовательность трансформированных шаблонов W , которая состоит из элементов множества $\{P_1, \dots, P_8\}$. Все инструкции трассы T относятся к одной из восьми категорий, представленных шаблонами P_i этого множества, соответственно:

1. Если инструкция записывает в один или несколько регистров значение из диапазона значений адресного пространства эмулируемого кода, она относится к шаблону P_1 ;

2. Если инструкция использует пару регистр-значение, которая получена от предыдущей инструкции, удовлетворяющей шаблону P_1 , она относится к шаблону P_2 ;

3. Если инструкция производит чтение из памяти по адресу из диапазона значений адресного пространства эмулируемого кода, то она относится к шаблону P_3 ;

4. Если инструкция производит запись в память по адресу, используемому последней инструкцией, удовлетворяющей шаблону P_3 , она относится к шаблону P_4 . Переход по этой ветви обозначает успешный разбор автоматом A_1 последовательности W ;

5. Инструкции, не относящиеся к предыдущим шаблонам, относятся к шаблону P_5 ;

6. Если инструкция помещает в регистр значение не из адресного пространства эмулируемого кода, то она относится к шаблону P_6 ;

7. Если выполняемая инструкция является svc , то она относится к шаблону P_7 . Переход по этой ветви обозначает успешный разбор автоматом A_2 последовательности W ;

8. Инструкции, не относящиеся к шаблонам P_1, P_2, P_6, P_7 относятся к шаблону P_8 .

На основе отнесения инструкции к той или иной категории строятся автоматы A_1 и A_2 . В трассе T наличие полиморфного кода, подтверждается если последовательность W разбирается автоматом A_1 , а наличие шелл-кода – автоматом A_2 . Обнаружение последовательности расшифровщик-шелл-код осуществляется передачей адреса последней инструкции разобранный автоматом A_1 на вход автомату A_2 как адрес первой анализируемой инструкции начального состояния. A_1 и A_2 представлены на рисунках 1 и 2.

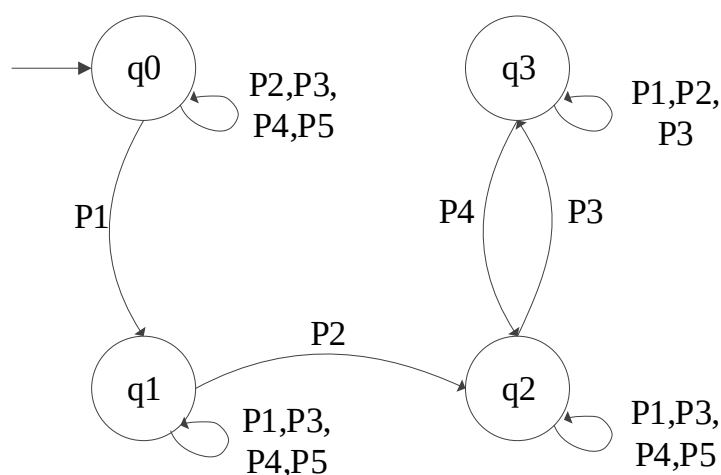


Рис. 3. Графическое представление A_1

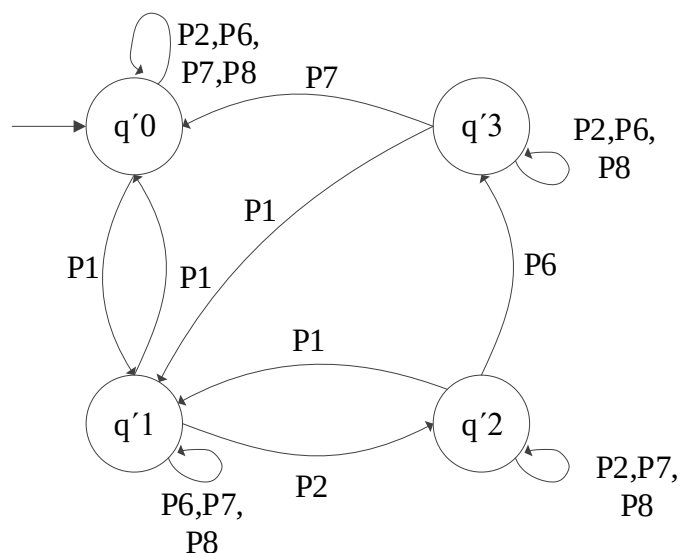


Рис. 2. Графическое представление A_2

Пример разбора автоматом последовательности инструкций представлен на рисунке 3.

0x10000 24608fe2 add r6, pc, #0x24	P1	
0x10004 16ff2fe1 bx r6	P2	
0x1002c f5ffffeb bl #0x10008	P1	
0x10008 e340a0e3 mov r4, #0xe3	P5	
0x1000c 010c54e3 cmp r4, #0x100	P5	
0x10010 leff2f81 bxhi lr	P2	
0x10014 e34044e2 sub r4, r4, #0xe3	P5	
0x10018 0450dee7 ldrb r5, [lr, r4]	P3	цикл
0x1001c 585025e2 eor r5, r5, #0x58	P5	расшифрования
0x10020 0450cee7 strb r5, [lr, r4]	P4	успех A1
0x10024 e44084e2 add r4, r4, #0xe4	P5	
0x10028 f7ffffea b #0x1000c	P5	
0x1000c 010c54e3 cmp r4, #0x100	P8	
0x10010 leff2f81 bxhi lr	P8	
0x10030 01308fe2 add r3, pc, #1	P1	
0x10034 13ff2fe1 bx r3	P2	
0x10038 7846 mov r0, pc	P1	
0x1003a 0a30 adds r0, #0xa	P1	
0x1003c 0190 str r0, [sp, #4]	P8	
0x1003e 01a9 add r1, sp, #4	P8	
0x10040 921a subs r2, r2, r2	P8	
0x10042 0b27 movs r7, #0xb	P6	
0x10044 01df svc #1	P7	успех A2

Рис. 3. Пример идентификации подграфа

Множество классификаторов K_i сформулировано следующим образом:

1. Если последовательность инструкций бинарного файла не совпадает с запущенными в эмуляции инструкциями, то файл относится к классу K_1 ;
2. Если число бесполезных (не вносящих изменения ни в один из регистров, кроме PC) инструкций больше 0, то файл относится к классу K_2 ;
3. Если число инструкций, использующих значение PC регистра больше 0, то файл относится к классу K_2 ;

4. Если число разборов автоматом A1 или A2 последовательности трансформированных шаблонов W больше 0, то файл относится к классу K4 или K5 соответственно.

3. Прототип программного средства динамического анализа

В настоящем прототипе средства реализована схема, в которой решение принимается при положительном результате хотя бы одного классификатора.

Модульная схема разработанного средства представлена на рисунке 4.

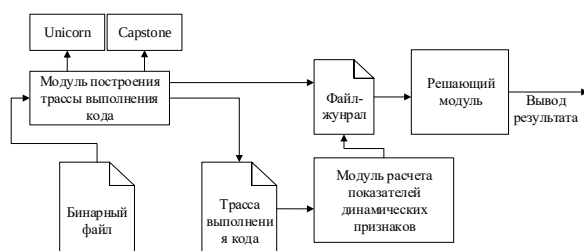


Рис. 4. Модульная схема прототипа средства

Исходные данные для анализа требуют предварительной обработки, это позволит уменьшить объем анализируемого кода и вероятность ошибок первого рода, для проверки этого утверждения был создан отдельный набор данных (содержимое секции «.text»).

Модуль построения трассы выполнения кода (модуль 1) загружает файл в оперативную память эмулируемой среды процессора Unicorn [11] ARM архитектуры. После каждого этапа выполнения инструкции происходит сравнение текущей инструкции с инструкцией в бинарном файле. Количество таких несовпадений, объем файла и объем проанализированных данных записывается в файл журнал. С помощью фреймворка Capstone [12] проводится дизассемблирование кода, который вместе с значениями регистров записывается в файл-трассу.

Модуль расчета показателей динамических признаков (модуль 2) производит подсчет числа бесполезных инструкций, не вносящих изменения в регистры общего назначения), количество инструкций получения и использования значения PC регистра, количество успешных разборов автоматами A1 и A2 последовательности W и общее число запущенных инструкций.

Решающий модуль (модуль 3) реализует схему принятия решения, структура данной схемы не оптимизирована и требует дальнейшего исследования и изменения.

Алгоритм работы прототипа средства представлен на рисунке 5.

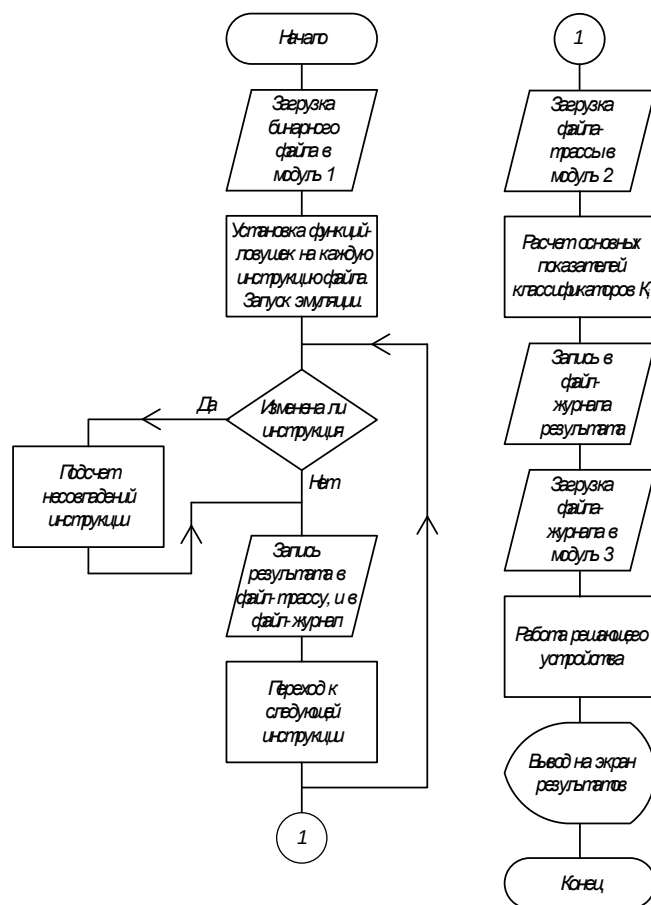


Рис. 5. Схема алгоритма обнаружения

Результаты тестовой работы прототипа средства динамического анализа кода на основе эвристических признаков представлены на таблице 1.

Таблица. 1.

Оценка эффективности прототипа средства			
Результат анализа Анализируемые данные	Решение		Среднее покрытие кода
	Вредоносное ПО	Безопасное ПО	
Шелл-коды.	81.4 %	18.6 %	47 %
Бинарные файлы	100 %	0 %	0.12 %
Исполняемый код бинарного файла	59.3 %	40.7 %	0.02 %

Предварительная подготовка данных снизила покрытие кода и вероятность ошибки первого рода. Причина высокой вероятности ошибки первого рода состоит в низком покрытии кода. Низкое покрытие кода вызвано неспособностью эмулятора CPU Unicorn обрабатывать полезную нагрузку, направленную на функционал операционной системы, и различные реализации средств, для которых был написан шелл-код. Увеличение покрытия кода осуществляется повторным запуском процесса эмуляции с адреса последнего прерывания. Замена эмулятора на виртуальную машину не допустимо, так как полезная нагрузка шелл-кода может вывести из строя машину, что приведет к непредусмотренной перезагрузке. Часть ошибок второго рода возникла из-за системного прерывания выполняемого кода, объясняемое невозможностью эмулятора процессора

выполнить полезную нагрузку. Из-за этого средство анализа не смогло собрать достаточную информацию о трассе выполнения бинарного файла.

Построение оптимальной схемы принятия решения эмпирическим методом, обеспечивающей низкие вероятности ошибок первого и второго рода – является направлением дальнейшего исследования.

Выводы

Таким образом, разработан алгоритм динамического анализа исполняемого кода на процессорах ARM архитектуры. Проведена работа на тестовых данных, оценена эффективность и собрана информация для дальнейшего исследования и совершенствования схемы принятия решения. Программное средство реализовано по упрощенной структуре, что позволяет провести эмпирические исследования на поиск оптимальных параметров основных показателей классификаторов и повысить покрытие кода.

Литература

1. Маркин, Д. О. Особенности поиска уязвимостей программного обеспечения на основе технологии TrustZone / Д. О. Маркин, Т. Ч. Хо, Н. П. Мешков // Проблемы информационной безопасности. Компьютерные системы. – 2020. – № 4. – С. 79–87.
2. Маркин, Д. О. Методика исследования системного программного обеспечения сетевого оборудования семейства Cisco на предмет наличия недеklarированных возможностей / Д. О. Маркин, С. М. Makeев, И. А. Санников, Х. Т. Чунг // Ученые записки Орловского государственного университета. – 2020. – № 3(88). – С. 215–221.
3. Марков, А. С. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов, А. В. Барабанов; под ред. доц. А. С. Маркова. – Москва : Радио и связь, 2012. – 192 с.
4. Гайворонская, С. А. Гибридный метод обнаружения шеллкодов / С. А. Гайворонская, Д. Ю. Гамаюнов // Системы высокой доступности. Том 2, № 8. 2012. С. 33-44.
5. Горюнов, М. Н. Распознавание функциональных объектов программного обеспечения в условиях отсутствия исходных текстов / М. Н. Горюнов [и др.] // Информационные системы и технологии. – 2013. – № 5. – С. 112–120.
6. Waqas A. A framework for analysis and comparison of dynamic malware analysis tools // International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.5, 2014 p. 74
7. Гамаюнов Д. Ю., Сковорода А. А. Анализ мобильных приложений с использованием моделей привилегий и API-вызовов вредоносных приложений // Прикладная дискретная математика. 2017. № 36. С. 84-105. doi <http://doi.org/10.17223/20710410/36/7>.
8. Гамаюнов Д. Ю., Сковорода А. А. Динамический анализ мобильных приложений // Программная инженерия. 2019. № 7-8. С. 324-333. doi <http://doi.org/10.17587/prin.10.324-333>.
9. Jagsir Singh Jaswinder Singh Detection of malicious software by analyzing the behavioral artifacts using machine learning algorithms //Information and Software Technology Volume 121, May 2020, p.35.
10. Интерактивная карта киберугроз // Лаборатория Касперского. – 2020. URL: <https://cybermap.kaspersky.com/ru/stats> (дата обращения: 07.03.2021).
11. Unicorn. The Ultimate CPU emulator. URL: <https://www.unicorn-engine.org> (дата обращения: 07.03.2021).
12. Capstone. The Ultimate Disassembler. URL: https://www.capstone-engine.org/lang_python.html(дата обращения: 07.03.2021).

The tool for recognition polymorphic exploits for ARM systems based on behavioral patterns

Markin D. O.¹³⁴, Minachev V. M.¹³⁵

Abstract. *The article describes a dynamic analysis algorithm with identification of malware behavioral features for processors with ARM architecture. The model and dynamic features of a polymorph exploit with shellcode employment are described. The decision tree scheme of classifying the executable code as malicious is presented. The suspicious behavior detection method, classification of suspicious behavior as polymorph code or shellcode and separate modules operation algorithms of the analysis tool prototype were developed. The efficiency of the algorithm was assessed on test dataset, and future research directions were highlighted.*

Keywords: *malware detection, dynamic analysis, shellcode, emulation, assembler instruction, polymorph code.*

¹³⁴ Dmitry Markin, candidate of technical sciences, The Academy of Federal Security Guard Service of the Russian Federation, Oryol, mdo@academ.msk.rsnnet.ru

¹³⁵ Minachev Vladislav, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

Средство идентификации признаков полиморфного программного обеспечения для ARM-систем на основе статических признаков

Маркин Д. О.¹³⁶, Архипов М. А.¹³⁷

***Аннотация.** В статье описан алгоритм детектирования вредоносного программного обеспечения для компьютерных систем на основе процессоров с архитектурой ARM на основе статических эвристических признаков. Описана модель вредоносного программного обеспечения для компьютерных систем на основе процессоров с архитектурой ARM, разработан эффективный алгоритм детектирования вредоносного программного обеспечения. Экспериментально подтверждена работоспособность и оценена эффективность алгоритма*

***Ключевые слова:** ARM, шелл-код, вредоносное программное обеспечение, сигнатура, детектирование.*

Введение

В последнее время, в частности, с появлением IoT ("Интернета вещей"), ежегодно растет количество мобильных устройств. Телефоны, смартфоны, планшетные компьютеры, смарт-часы, разного рода датчики, сенсоры, контроллеры для технологии "Умный дом", сетевое оборудование, измерительные приборы и т.п. – большая часть этих устройств основана на процессорной архитектуре ARM [1] в виду ее энергоэффективности и достаточной производительности. Вместе с ростом количества мобильных устройств растет и количество обрабатываемой и создаваемой информации, а с ней растет и объем критически важных данных, требующих защиты.

Архитектура ARM имеет многочисленные специфические особенности по сравнению с распространенными архитектурами Intel x86/x64, требующие от исследователей глубокого понимания и компетенций. Данная архитектура относится к так называемым load-store архитектурам (PowerPC, SPARC, RISC-V, MIPS) [2]. Таким образом, существующее противоречие, заключающееся в объективной потребности всестороннего анализа безопасности ПО для процессоров на архитектуре ARM и недостаточной эффективности известных методов и средств для таких объектов оценки, требует разработки новых или совершенствования известных методов и средств выявления уязвимостей и недеklarированных возможностей (НДВ) в ПО.

Проблеме анализа безопасности ПО посвящены многочисленные труды как отечественных, так и зарубежных исследований. Наиболее известные из них труды Аветисяна А. И., Белеванцева А. А., Курмангалеева Ш. Ф., Падаряна В. А., Гайворонской С. А. [4], Гамаюнова Д. Ю. и Сковороды А. А. [7,8], Бегаева А. Н. [18], Маркова А. С. [3], Закалкина П. В. [20], Мацкевича А. Г. и Горюнова М. Н. [5] и других и других. Среди иностранных исследователей наиболее известны труды Pinto S. [22,23], Winter J. [24], Cerdeira D. [25] и других.

1. Постановка задачи

В виду особенностей архитектуры процессора эксплуатация уязвимостей требует использования определенных команд при разработке вредоносного программного обеспечения (ВПО). Таким образом, разработка алгоритма выявления вредоносного программного обеспечения на основе статического анализа позволит эффективно детектировать большинство ВПО на основе выделенных признаков. Эффективность

¹³⁶ Маркин Дмитрий Олегович, канд. техн. наук, Академия ФСО России, г. Орёл, mdo@academ.msk.rsnet.ru

¹³⁷ Архипов Михаил Андреевич, Академия ФСО России, г. Орёл

статического метода детектирования ВПО так же обуславливается отсутствием необходимости исполнения ПО для их анализа, что повышает скорость анализа.

При разработке и оценке эффективности алгоритма используется следующий тестовый набор данных: 863 исполнимых файла, 90 из которых – ВПО, представляющие собой эксплойты на основе шелл-кодов, разработанных для архитектуры ARM из баз данных www.exploit-db.com, shell-storm.org, а также шелл-кодов, сгенерированных при помощи средства ARMSCGen (github.com/alexpark07/ARMSCGen), 773 – легитимное ПО, полученное из каталога /bin микрокомпьютеров Raspberry Pi и Orange Pi. Необходимо разработать эффективный алгоритм выявления ВПО с минимальным количеством ложных срабатываний, то есть детектирования ВПО в легитимном ПО, а также минимальным количеством пропусков цели, то есть распознавании ВПО как легитимного ПО.

2. Модель полиморфного программного обеспечения

В качестве полезной нагрузки в ВПО зачастую используются шелл-коды. Шелл-кодом называется набор исполнимых инструкций, осуществляющих эксплуатацию удаленной уязвимости работы с памятью. Для передачи управления на шелл-код, злоумышленники используют уязвимости работы с памятью. При распознавании шелл-кода применяется сигнатурный метод, основанный на наиболее часто встречающихся признаках. К таким признакам относятся:

Переключение режима работы процессора из ARM, использующего 32 битные команды, в Thumb, использующего 16 битные команды. Данный метод используется с целью уменьшения объема шелл-кода ввиду ограниченности его размера. При смене режима злоумышленнику необходимо проследить, чтобы секция Thumb была выравнена под 4 байта, для чего используются пор-команды. Признак был выделен в результате анализа исходных кодов доступного ВПО.

Использование пор-команд, то есть команд, выполнение которых не меняет значений регистров. Данный метод используется для обеспечения передачи управления на полезную нагрузку в условиях неизвестности особенностей атакуемого узла.

Наличие системного вызова, которому предшествует запись корректного номера системного вызова в регистр. Признак обуславливается особенностью платформы ARM, в которой передача локальных переменных функции производится через регистры, а не через стек. Для этого в регистр r7 (для arm32) или x8 (для arm64) записывается номер требуемого системного вызова, затем происходит системный вызов с номером 1 (exit) или 0 (перезагрузка).

3. Алгоритм идентификации признаков полиморфного программного обеспечения для ARM-систем

На основе сигнатур выделенных признаков разработано программное средство (ПС), реализующее функцию классификацию ПО на легитимное и вредоносное.

ПС загружает анализируемый ELF-файл в фреймворк для реверс-инжиниринга radare2, который выполняет поиск хотя бы одной hex-строки, записанной в массив выделенных сигнатур. Если есть совпадение, ПС классифицирует ELF-файл как ВПО и переходит к следующему файлу, если совпадений нет – ПС классифицирует ELF-файл как легитимное ПО. В результате выполнения программы составляются два отчета: один отображает для каждого проанализированного файла является ли он вредоносным, второй – отображает файлы, в которых был детектирован шелл-код, с указанием, по какому признаку ПС классифицировало ELF как вредоносное ПО. Структурная схема разработанного программного средства представлена на рисунке 1.

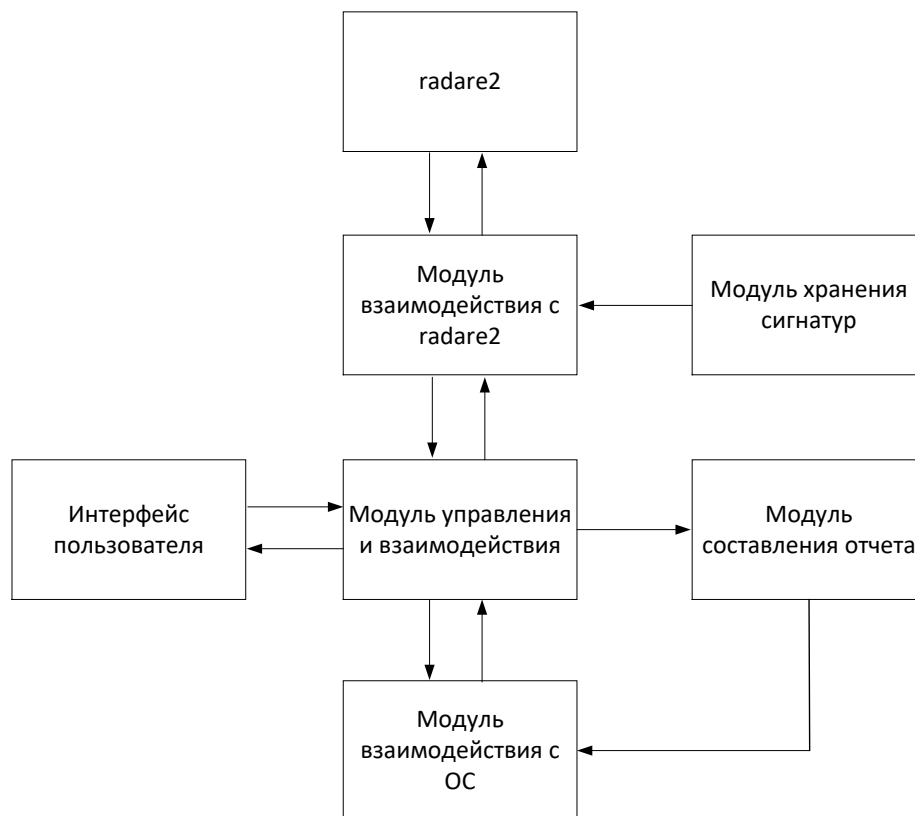


Рис. 4. Структурная схема программного средства

На рисунке 2 представлен алгоритм анализа одного ELF-файла с помощью разработанного ПС.

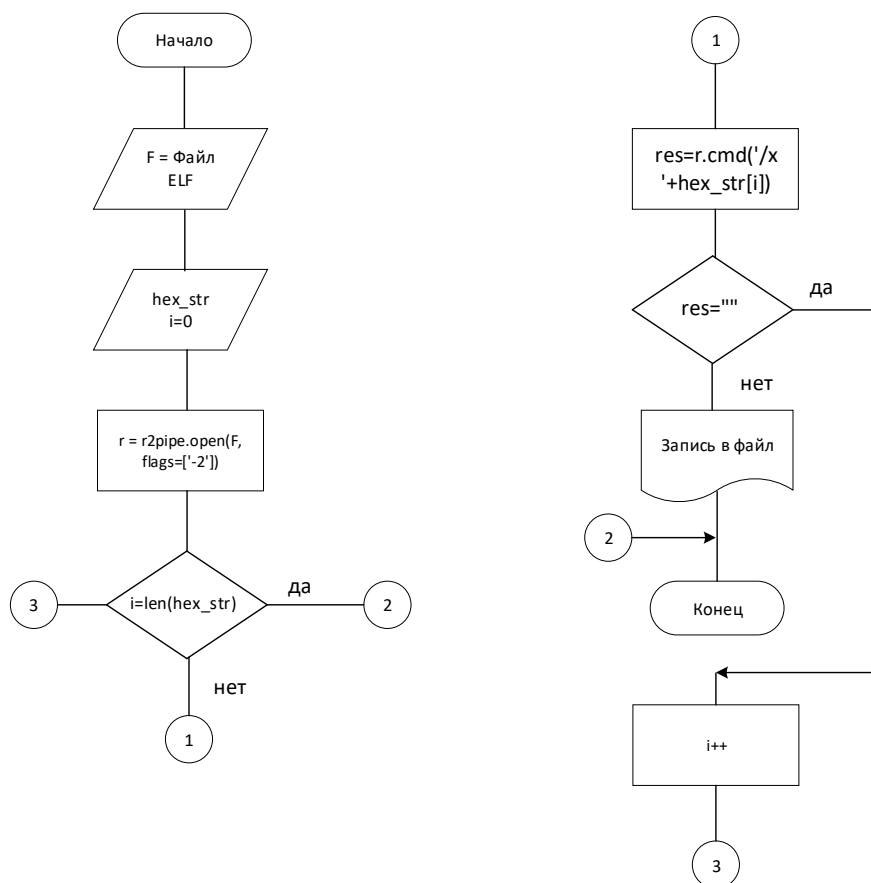


Рис. 2. Алгоритм анализа ELF-файла

Для оценки эффективности работы разработанного алгоритма был проведен анализ каталога, содержащего тестовые данные, описанные выше. Результат работы ПС представлен в таблице 1.

Таблица 1

Оценка эффективности алгоритма распознавания вредоносного ПО		
Имеющиеся тестовые данные \ Результат анализа	ВПО	Легитимное ПО
Детектирован шелл-код	78,9 %	0 %
ELF-файлы	21,1 %	100 %

Таким образом, разработанный алгоритм классифицировал все легитимное ПО как неопасное. При анализе ВПО программное средство детектировало шелл-коды только в 78,9 % случаев. На основе полученных результатов можно сделать вывод, что выявленные признаки ВПО не встречаются в легитимном ПО, но не позволяют безошибочно определять наличие шелл-кода в файле. Это может быть связано с тем, что злоумышленник при разработке ВПО внедрил в него полиморфный код, анализ которого возможен только динамическим методом. Для повышения эффективности алгоритма необходимо выделить новые признаки ВПО. В результате исследования имеющихся тестовых данных, была оценена частота обнаружения каждой из выделенных сигнатур (табл. 2).

Таблица 2

Оценка частоты обнаружения сигнатур

Сигнатура	Количество обнаружений
Переключение режима работы процессора	53
пор-команды	20
Наличие системного вызова, которому предшествует запись корректного номера вызова в регистр	9

Выводы

На основе полученных результатов можно сделать вывод о том, что выделенные сигнатуры способны достаточно эффективно детектировать ВПО без ложных срабатываний на легитимном ПО. С целью дальнейшего повышения эффективности необходимо выделить новые сигнатуры, а также новые статические эвристические признаки для разработки на их основе алгоритма детектирования в качестве дополнения данному.

Литература

13. Маркин, Д. О. Особенности поиска уязвимостей программного обеспечения на основе технологии TrustZone / Д. О. Маркин, Т. Ч. Хо, Н. П. Мешков // Проблемы информационной безопасности. Компьютерные системы. – 2020. – № 4. – С. 79–87.
14. Маркин, Д. О. Методика исследования системного программного обеспечения сетевого оборудования семейства Cisco на предмет наличия недеklarированных возможностей / Д. О. Маркин, С. М. Макеев, И. А. Санников, Х. Т. Чунг // Ученые записки Орловского государственного университета. – 2020. – № 3(88). – С. 215–221.
15. Гайворонская, С. А. Гибридный метод обнаружения шеллкодов / С. А. Гайворонская, Д. Ю. Гамаюнов // Системы высокой доступности. Том 2, № 8. 2012. С. 33-44.
16. Гамаюнов Д. Ю., Скворода А. А. Анализ мобильных приложений с использованием моделей привилегий и API-вызовов вредоносных приложений // Прикладная дискретная математика. 2017. № 36. С. 84-105. doi <http://doi.org/10.17223/20710410/36/7>.
17. Гамаюнов Д. Ю., Скворода А. А. Динамический анализ мобильных приложений // Программная инженерия. 2019. № 7-8. С. 324-333. doi <http://doi.org/10.17587/prin.10.324-333>.
18. Бегаев, А. Н. Выявление уязвимостей и недеklarированных возможностей в программном обеспечении / А. Н. Бегаев, С. В. Кашин, Н. А. Маркевич, А. А. Марченко. – Санкт-Петербург : Университет ИТМО, 2020. – 38 с.
19. Марков, А. С. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов, А. В. Барабанов; под ред. доц. А. С. Маркова. – Москва : Радио и связь, 2012. – 192 с.
20. Закалкин, П. В. Система анализа программного обеспечения на предмет отсутствия недеklarированных возможностей / П. В. Закалкин, П. В. Мельников // Программная инженерия. – 2018. – Т. 9, № 2. – С. 69–75.
21. Горюнов, М. Н. Распознавание функциональных объектов программного обеспечения в условиях отсутствия исходных текстов / М. Н. Горюнов [и др.] // Информационные системы и технологии. – 2013. – № 5. – С. 112–120.
22. Pinto, S. Demystifying Arm TrustZone: A Comprehensive Survey / S. Pinto, N. Santos. // ACM Computing Surveys, 2019. January 10. – p. 36.
23. Pinto, S. Space and time partitioning with hardware support for space applications / S. Pinto, A. Tavares, S. Montenegro // Data Systems in Aerospace, European Space Agency. ESA SP 736, 2016. – p. 250.
24. Winter, J. Experimenting with ARM TrustZone – Or: How I met a friendly piece of trusted hardware // Proc. of the IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, 2012. – P. 1161–1166.

25. Cerdeira, D. SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems / D. Cerdeira, N. Santos, P. Fonseca, S. Pinto // Conference IEEE Symposium on Security and Privacy, San Francisco, CA, January 2020. –p. 17.

Feature identification tool for polymorphic software for ARM systems based on static features

Markin D. O.¹³⁸, Arkhipov M. A.¹³⁹

Abstract. *The article describes an algorithm for detecting malicious software for computer systems based on ARM-based processors based on static heuristic features. A model of malicious software for computer systems based on processors with ARM architecture is described, an effective algorithm for detecting malicious software is developed. The performance of the algorithm has been experimentally confirmed and the efficiency of the algorithm has been evaluated.*

Keywords: ARM, shellcode, malware, signature, detection.

¹³⁸ Dmitry Markin, candidate of technical sciences, The Academy of Federal Security Guard Service of the Russian Federation, Oryol, mdo@academ.msk.rsnnet.ru

¹³⁹ Mikhail Arkhipov, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

Система позиционирования подвижных источников радиосигналов на основе методов прогнозирования

Маркин Д. О.¹⁴⁰, Козин С. С.¹⁴¹

Аннотация. В статье приводятся основные результаты исследований, такие как реализация комплекса моделирующих алгоритмов, осуществляющих ряд случайных процессов: движение подвижных источников радиосигналов и распространение радиоволн; алгоритмы, реализующие аналитический расчет предполагаемой области местоположения на основе аппарата нечеткой логики, а также метод прогнозирования (линейное предсказание). Проведен ряд экспериментов, в том числе натурных, позволяющих использовать в качестве исходных данных реальное распределение статистики уровня мощности принимаемого сигнала сотовой сети стандарта LTE, а также экспериментов, направленных на исследование эффективности математического аппарата нечеткой логики в совокупности с прогнозированием. Сформулированы выводы в отношении результатов проведенных исследований.

Ключевые слова: система позиционирования, беспроводные сети передачи данных, трилатерация, нечёткая логика.

Введение

Современный уровень развития инфотелекоммуникационных технологий предоставляют все больше возможностей по доступу к услугам и данным с использованием беспроводных сетей передачи данных (БСПД). Вместе с тем возникает и угроза использования данных сетей в незаконных целях, связанных с распространением запрещенных сведений, несанкционированным доступом к защищаемой информации, сбором сведений о гражданах и организациях и других. Данное обстоятельство обуславливает объективную потребность в решении задачи оперативного определения местоположения (позиционирования) вероятного источника угрозы нарушения безопасности, в первую очередь, средствами самой беспроводной сети передачи данных.

Исследованиям вопросов использования БСПД в целях позиционирования источников радиоизлучения посвящены многочисленные исследования как отечественных, так и зарубежных ученых. Применение аппарата нечеткой логики для решения задачи позиционирования описано в трудах [1-4]. Вопросами имитационного моделирования систем позиционирования посвящены работы Фокина Г. А. [5], Камалова Ю. Б. [6].

Вместе с тем, точность современных систем позиционирования в совокупности с их сложностью, предъявляют повышенные требования системам определения местоположения, которые в достаточной степени пока не удовлетворены.

1. Комплекс алгоритмов системы определения местоположения подвижных источников радиосигналов на основе методов прогнозирования

Для разработки имитационной модели необходимо разработать алгоритмы, осуществляющие моделирование следующих процессов:

- моделирование псевдослучайного движения подвижного источника радиосигналов по территории города;
- моделирование скорости и ускорения подвижного источника радиосигналов по территории города;

¹⁴⁰ Маркин Дмитрий Олегович, канд. техн. наук, Академия ФСО России, г. Орёл, mdo@academ.msk.rsnet.ru

¹⁴¹ Козин Сергей Сергеевич, Академия ФСО России, г. Орёл

– моделирование псевдослучайного процесса распространения радиосигналов в условиях города.

Для осуществления данных функций выбрана платформа имитационного моделирования AnyLogic. Схема модели представлена на рисунке 1.

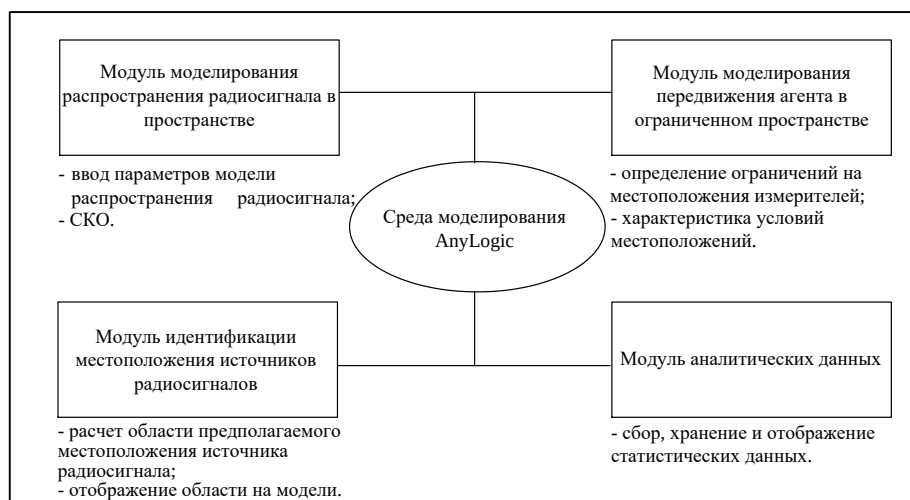


Рис. 1. Схема имитационной модели в среде AnyLogic

Последовательность точек траектории движения реализована в виде цепи Маркова. Модель перемещения пользователей получена за счет анализа статистики перемещения пользователя мобильного устройства и с использованием встроенного приложения сбора данных о его перемещениях.

Для имитации распространения радиосигналов в пространстве используется формула потерь для идеальной изотропной антенны:

$$\frac{P_t}{P_r} = \frac{(4\pi R)^2}{\lambda^2} \quad (1)$$

где P_t – мощность сигнала передающей антенны; P_r – мощность сигнала на приемной антенне; λ – длина волны радиосигнала, находящаяся из соотношения скорости света к частоте, несущей радиосигнала; R – расстояние, пройденное сигналов между двумя антеннами.

2. Трилатерация и нечёткая логика как способ позиционирования подвижного объекта

Применение технологий трилатерации и нечеткой логики для решения задач позиционирования подробно описаны в работах [5,6]. В идеальных условиях уравнение для нахождения координат точки пересечения выглядят так:

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = R_1^2 \\ (x - x_2)^2 + (y - y_2)^2 = R_2^2 \\ \dots \\ (x - x_n)^2 + (y - y_n)^2 = R_n^2 \end{cases} \quad (2)$$

где (x, y) – координаты источника БСПД; (x_i, y_i) – координаты точек измерений агента, а n – их количество; R_i – рассчитанное расстояние

от источника радиосигналов до точек измерения.

Из (1) получаем формулу для расчета радиуса для заранее известного источника радиосигналов:

$$R = \frac{\lambda}{4\pi} \sqrt{\frac{P_t}{P_r}}. \quad (3)$$

Реализация метода трилатерации в разрабатываемой системе представлена на рисунке 2.



Рис. 2. Работа алгоритма трилатерации в разрабатываемой системе

В идеальных условиях радиусы, вычисленные по формулам (2) и (3) будут равны, так как не вносятся погрешность. Математический аппарат, позволяющий учитывать погрешность в расчётах, реализован в нечёткой логике. Для поиска местоположения на основе нечеткой логики используется накопленная статистика с данными о максимальной и минимальной ошибке позиционирования. Благодаря такому подходу, зона предполагаемого местонахождения объекта из круга уменьшается до кольца (в двумерной плоскости). Демонстрация данного эффекта и работа данного метода в разрабатываемой системе показаны на рисунке 4.

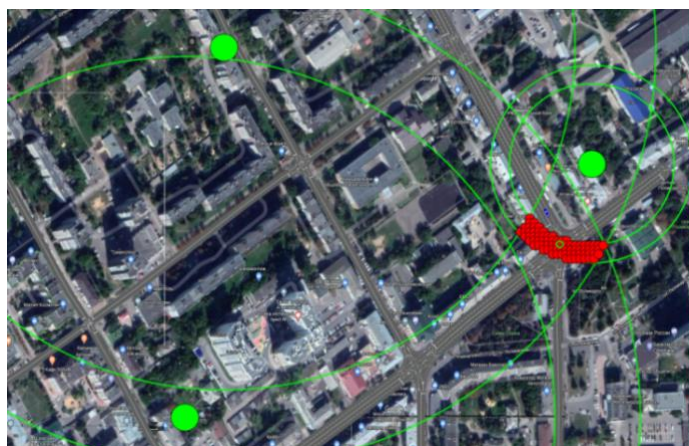


Рис. 4. Работа алгоритма нечёткой логики в разрабатываемой системе

3. Метод Монте-Карло

При построении множества окружностей, необходимо выбрать способ расчета площади криволинейных сложных фигур. Существуют различные способы расчета площади криволинейных фигур, необходимо выбрать менее затратный с точки зрения

потребления памяти и более точный с точки зрения расчета, так как площадь является основным показателем качества алгоритма. Для расчета площади был выбран метод Монте-Карло. Данный метод работает по алгоритму, приведенному ниже.

1. Криволинейная площадь вносится в простую фигуру, чья площадь заранее известна, в нашем случае это прямоугольник ограниченный контролируемой зонной и горизонтом исследования.

2. Случайно вносятся точки на данную простую фигуру так, что координаты принадлежат простой фигуре и они случайны, так же координаты не должны повторяться. Для нашей системы случайность убрана, с целью более точного расчета площади. Для этого были перебраны все пиксели в простой фигуре. Для полной картины понимания, представлен рисунок 5 для двух точек измерения агентом.

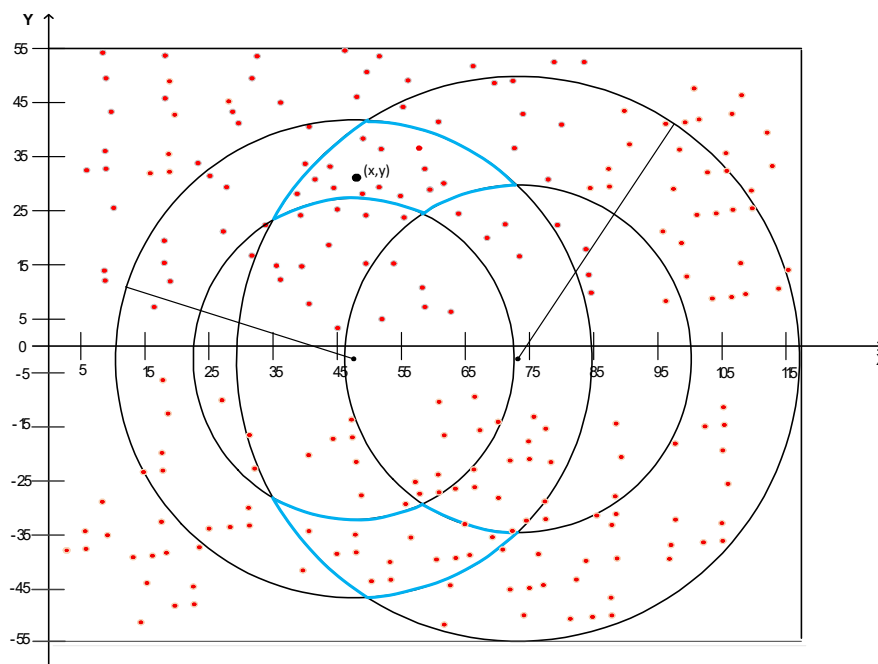


Рис. 5. Демонстрация работы метода Монте-Карло

3. После построения сложной фигуры, рассчитывается площадь по формуле: $S_{иск} = S \frac{K}{N}$, где $S_{иск}$ – площадь искомой (сложной) фигуры; S – площадь известной фигуры; K – количество точек, попавших в сложную фигуру; N – количество всех сгенерированных точек.

4. Эвристический метод позиционирования

Для определения более точного местоположения, необходимо произвести несколько расчетов, так как при большем количестве измерений, площадь поиска потенциального местоположения подвижного источника радиоизлучения уменьшается.

Как видно из рисунка 5, при работе 2 БС возникают ситуации, когда при работе алгоритма нечёткой логики областей возможного нахождения подвижного объекта, удовлетворяющих необходимым условиям, не одна, а две. Для устранения таких погрешностей и общего увеличения точности работы системы определения местоположения подвижного источника радиосигналов, был разработан эвристический алгоритм позиционирования на основе разбиения области возможного местонахождения объекта.

Алгоритм данного метода представлен на рисунке 6.

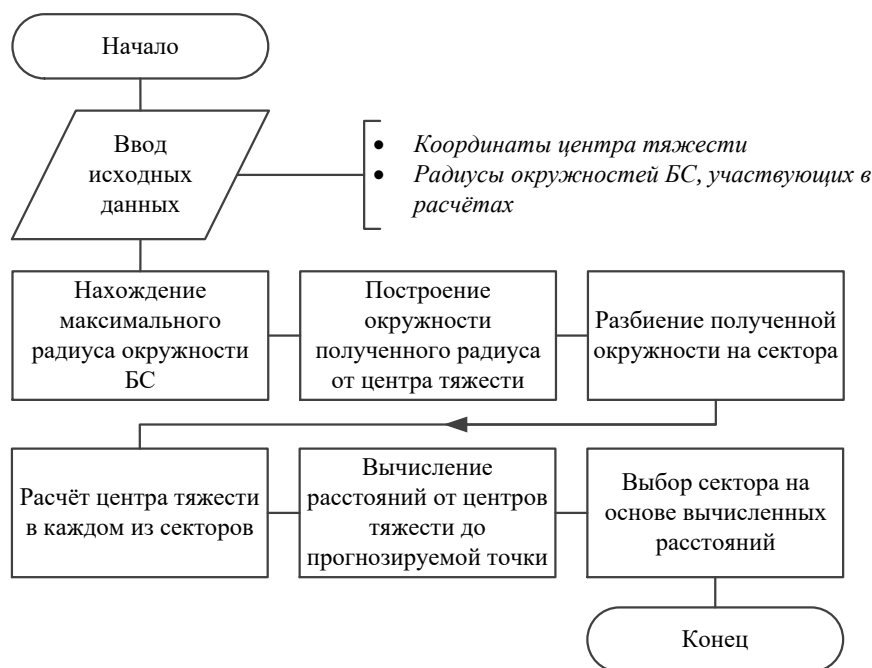


Рис. 6. Блок-схема эвристического алгоритма позиционирования

Центром тяжести области в рассматриваемой системе является точка, координаты которой вычисляются как среднее арифметическое между всеми точками, попавшими в заданную область.

В данном алгоритме под прогнозируемой точкой подразумевается точка, полученная на основе метода линейного предсказания (в качестве разницы выступает разница между координатами основного центра тяжести, то есть того, от которого строилась окружность, необходимая для разбиения области возможного местоположения объекта).

Выбор сектора зависит от вычисленных расстояний между частными центрами тяжести каждого сектора и прогнозируемой точки, предпочтительным является меньшее значение расстояния из получившихся.

Реализация данного алгоритма в разрабатываемой системе определения местоположения подвижного объекта представлена на рисунке 7 (в момент проведения вычислений).

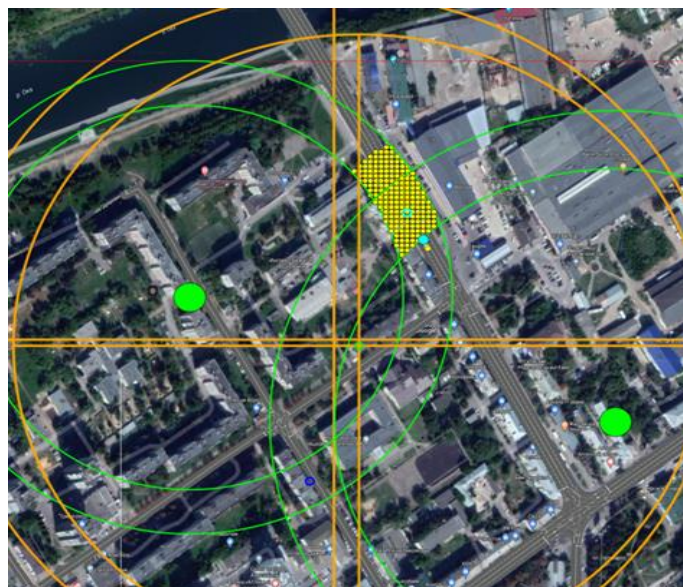


Рис. 7. Работа эвристического алгоритма позиционирования в разрабатываемой системе

5. Оценка эффективности

Для оценки эффективности методов и алгоритмов в разработанной системе определения местоположения подвижного источника радиосигналов был проведён ряд экспериментов при работе различного числа БС и различных алгоритмах определения местоположения. Указанные алгоритмы реализованы в ряде программ для ЭВМ [9,10].

Основными параметрами, относительно которых производится расчет эффективности разработанного прототипа программного средства, являются площадь области предполагаемого местоположения объекта наблюдения, а также расстояние от самого объекта до прогнозируемой, при помощи различных алгоритмов, точки.

Среднее число экспериментов для каждого из рассматриваемых случаев различно, и выбирается таким образом, чтобы именно при таком количестве испытаний процесс изменения параметров был наиболее приближен к эргодическому. Результаты эксперимента сведены в таблице 1 и 2.

Таблица 1.

Среднее значение площади возможного местоположения подвижного источника радиосигналов

Алгоритм Кол-во БС	Трилатерация, м ²	Нечёткая логика, м ²	Эвристический алг. прогн., м ²
Одна БС	7859,7	2092	2092
Две БС	1343,5	247	131,6
Три БС	386	33	16

Таблица 2.

Среднее значение расстояния от прогнозируемой точки до подвижного
источника радиосигналов

Алгоритм Кол-во БС	Трилатерация, м	Нечёткая логика, м	Эвристический алг.прогн., м
Одна БС	487,5	487,5	487,5
Две БС	286	270,7	11.2
Три БС	133	8,74	3,52

Из таблиц, представленных выше, видно, что наиболее точные результаты по двум рассматриваемым критериям эффективности разрабатываемой системы даёт использование эвристического алгоритма позиционирования. В свою очередь, метод трилатерации даёт наименее точные результаты по сравнению с другими алгоритмами рассматриваемой системы определения местоположения подвижных источников радиоизлучения, связано это с простотой реализации данного алгоритма по сравнению с другими предложенными.

Выводы

В работе реализован комплекс моделирующих алгоритмов, реализующих ряд случайных процессов, таких как движение подвижных источников радиосигналов и распространение радиоволн, а также алгоритмы, осуществляющие аналитический расчет предполагаемой области местоположения на основе аппарата нечеткой логики, а также методов прогнозирования: линейное предсказание, эвристический алгоритм прогнозирования на основе секторного разбиения областей; проведен ряд экспериментов, в том числе натурных, позволяющих использовать в качестве исходных данных реальное распределение статистики уровня мощности принимаемого сигнала сотовой сети стандарта LTE, а также экспериментов, направленных на исследование эффективности математического аппарата нечеткой логики в совокупности с прогнозированием; получена сравнительная оценка эффективности алгоритмов определения местоположения подвижных источников радиосигналов.

Экспериментально проверена и подтверждена работоспособность данной системы определения местоположения подвижных источников радиосигналов. Программные реализации методов, реализованные в данной системе, зарегистрированы в ФИПС [9,10].

Литература

1. Michał Socha, Wojciech Górka, Iwona Kotorz Fuzzy logic in indoor position determination system. Theoretical and Applied Informatics, 2016. Vol. 27, pp 1-15.
2. Orujov, F., Maskeli, R., Damaševičius, R. Wei Wei, Ye Li Smartphone based intelligent indoor positioning using fuzzy logic. Future Generation Computer Systems, 2018. No. 89. P. 335–348.
3. Chih-Yung Chen, Yu-Ju Chen, Shen-Whan Chen, Chi-Yen Shen, Rey-Chue Hwang A Fuzzy Indoor Positioning System with ZigBee Wireless Sensors. Journal of Electrical and Electronic Engineering, 2016. No 4(5). P. 97-102.
4. Sérgio Onofre, Bernardo Caseiro, João Paulo Pimentão, Pedro Sousa Using Fuzzy Logic to Improve BLE Indoor Positioning System. Proc. of Doctoral Conference on Computing, Electrical and Industrial Systems. Technological Innovation for Cyber-Physical Systems, 2016. pp. 169-177.
5. Фокин, Г. А. Технологии сетевого позиционирования 5G [монография] / Г. А. Фокин; СПбГУТ : Санкт-Петербург, 2020. – 466 с.
6. Камалов, Ю. Ю. Имитационное моделирование мобильных систем связи в условиях городской застройки / Ю. Б. Камалов, М. Н. Служивый // Известия Самарского научного центра РАН. – 2010. – Т. 12, № 4(2). – С. 341–345.
7. Вишнякова, О. А. Математическая модель обнаружения точки беспроводного доступа по измерениям мощности излучения разнесенными наблюдателями / О. А. Вишнякова, Д. Н.

Лавров, С. Ю. Лаврова // Математические структуры и моделирование / Ом. гос. ун-т. Фак. компьютер. наук. – Омск : Изд-во ОмГУ. 2013. № 2(28). С.49–59.

8. Маркин, Д. О. Исследование эффективности алгоритмов определения местоположения мобильных устройств внутри помещений / Д. О. Маркин // Вестник РГРТУ. – 2015. – № 54-1. – С. 32–39.

9. Программное средство определения местоположения подвижных источников радиосигналов на основе методов прогнозирования : свидетельство о государственной регистрации программы для ЭВМ № 2020666496 Российская Федерация / С. С. Козин, А. А. Кузькин, Д. О. Маркин, В. В. Рябоконь, Д. А. Свечников, О. А. Субботенко; авторы и правообладатели С. С. Козин, А. А. Кузькин, Д. О. Маркин, В. В. Рябоконь, Д. А. Свечников, О. А. Субботенко. – № 2020665135 ; заявл. 24.11.2020; опубл. 10.12.2020; зарегистрировано в Реестре программ для ЭВМ 10.12.2020 г.

10. Средство идентификации нелегитимных неподвижных источников радиосигналов беспроводных сетей передачи данных : свидетельство о государственной регистрации программы для ЭВМ № 2020611627 Российская Федерация / Д. О. Маркин, С. С. Козин, М. К. Бирюков, Т. А. Кравчук, В. А. Сидорова ; авторы и правообладатели Д. О. Маркин, С. С. Козин, М. К. Бирюков, Т. А. Кравчук, В. А. Сидорова. – № 2020615423 ; заявл. 01.06.2020; зарегистрировано в Реестре программ для ЭВМ 11.06.2020 г.

The positioning system of mobile sources of radio signals based on forecasting methods

Markin D. O.¹⁴², Kozin S. S.¹⁴³

Abstract. *The article presents the main research results, such as the implementation of a complex of modeling algorithms that carry out a number of random processes: the movement of mobile sources of radio signals and the propagation of radio waves; algorithms that implement the analytical calculation of the estimated location area based on the fuzzy logic apparatus, as well as the forecasting method (linear prediction). A number of experiments, including full-scale ones, were carried out, allowing to use as initial data the real distribution of statistics of the received power level of the cellular network of the LTE standard, as well as experiments aimed at studying the effectiveness of the mathematical apparatus of fuzzy logic in conjunction with forecasting. Conclusions are formulated regarding the results of the studies.*

Keywords: *positioning systems, wireless data networks, trilateration, fuzzy logic.*

¹⁴² Dmitry Markin, candidate of technical sciences, The Academy of Federal Security Guard Service of the Russian Federation, Oryol, mdo@academ.msk.rnet.ru

¹⁴³ Sergey Kozin, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

Подход по оцениванию уровня защищенности информации, обрабатываемой программным обеспечением доверенных сред исполнения на основе технологии TrustZone

Маркин Д. О.¹⁴⁴, Хо Т. Ч.¹⁴⁵

Аннотация. В работе описана модель оценки уровня защищенности информации, обрабатываемой трастлетами доверенной среды исполнения на основе технологии TrustZone. Предложен алгоритм, позволяющий извлекать признаки потенциально опасных конструкций из бинарных файлов трастлетов. Приведена формальная постановка задач моделирования оценки защищенности уровня информации, обрабатываемой трастлетами, и алгоритма кластеризации бинарных файлов трастлетов по уровню защищенности (потенциальной опасности)

Ключевые слова: TrustZone, ARM, статическая инструментация, поиск уязвимостей, выявление недеklarированных возможностей.

Введение

В сложившихся геополитических обстоятельствах доверие к программно-аппаратным техническим решениям иностранного производства исключено. Однако в связи с отсутствием аналогичных отечественных технологий и элементной базы применяются специальные процедуры оценки соответствия (сертификация, аттестация) [20], позволяющие повысить уровень доверия к подобным техническим решениям. Исследование безопасности программного обеспечения (ПО) для доверенных сред исполнения (ДСИ) связано с рядом сложностей:

техническая документация для ряда распространенных реализаций ДСИ закрыта для исследователей;

формат бинарных файлов ПО для ДСИ, как правило, нестандартный, его подробное описание также недоступно;

для динамического анализа требуется создания специфической среды исполнения, что невозможно в виду специфики технологии реализации ДСИ и, соответственно, требует от исследователей применения специальных методов инструментации для подготовки ПО к анализу;

архитектура ARM имеет многочисленные специфические особенности по сравнению с распространенными архитектурами Intel x86/x64, требующие от исследователей глубокого понимания и компетенций, в связи с чем существует объективная потребность в квалифицированных специалистах в данной области.

Таким образом, существующее **противоречие**, заключающееся в объективной потребности всестороннего анализа безопасности ПО для ДСИ на основе ARM-процессоров и недостаточной эффективности известных методов и средств для таких объектов оценки, требующее разработки новых или совершенствования известных методов и средств выявления уязвимостей и недеklarированных возможностей в ПО для ДСИ на основе технологии TrustZone.

Проблемой анализа безопасности ПО посвящены многочисленные труды как отечественных, так и зарубежных исследований. Наиболее известные из них труды Аветисяна А. И., Белеванцева А. А., Курмангалеева Ш. Ф., Падаряна В. А., Гамаюнова Д. Ю. [27,28], Сковороды А. А. [27,28] и Гайворонской С.А. [29,27], Казарина О. В., Варнавского Н. П., Захарова В. А., Кузюрина Н. Н. и

¹⁴⁴ Маркин Дмитрий Олегович, канд. техн. наук, Академия ФСО России, г. Орёл, mdo@academ.msk.rsnet.ru

¹⁴⁵ Хо Тхай Чунг, Академия ФСО России, г. Орёл

Шокурова А. В. [30, 31], Зегжды П. Д., Бойко В. П., Заборовского В. С., Подловченко Р. И., Иванникова В. П., Бегаева А. Н. [18], Маркова А. С. [3], Закалкина П. В. [20], Мацкевича А. Г. и Горюнова М. Н. [5] и других. Среди иностранных исследователей наиболее известны труды Ruan X. [34], Costan V. [35,36], Pinto S. [22], Cerdeira D. [25] и других.

1. Постановка задачи

Основными источниками угроз безопасности обрабатываемой информации в программном обеспечении являются [18]:

- 1) потенциально опасные функциональные возможности;
- 2) опасные функциональные объекты;
- 3) уязвимости конфигураций;
- 4) архитектурные уязвимости;
- 5) уязвимости кода.

При решении задачи выявления уязвимостей и НДВ в трастлетах для ДСИ на основе технологии *TrustZone* в современных условиях исследователю доступен только бинарный файл и некоторая информация о его вероятной структуре и содержимом. Учитывая отсутствие доступных средств эмуляции компонентов ДСИ на основе *TrustZone* и выше указанные обстоятельства, наиболее подходящими методами исследования [18] трастлетов являются: методы дизассемблирования, декомпилирования, восстановления формата данных, анализа документации, направленного анализа участков кода, синтаксического анализа, межпроцедурного контекстно-чувствительного анализа.

Результаты применения указанных методов позволят получить некоторые сведения об объекте оценки – трастлете, которые могут быть интерпретированы как источники угроз безопасности обрабатываемой информации.

Исходные данные:

множество реализаций программного обеспечения (трастлетов) S , извлеченных из ДСИ на основе технологии *TrustZone* "Aladdin TSM", "OP-TEE", "TrustTonic Kinibi";

Требуется:

разработать модель оценки уровня защищенности информации, обрабатываемой программным обеспечением ДСИ на основе технологии *TrustZone*, отличающаяся от известных учетом логических признаков потоков ввода-вывода информации и API-вызовов.

Ограничения и допущения:

- 1) отсутствует исходный код трастлетов;
- 2) исследуемые трастлеты имеют один из следующих форматов:
 - "HSTO" (OC Linaro OP-TEE);
 - "MCLF" (OC TrustTonic Kinibi);
- 3) формат трастлетов (ELF-подобный) не позволяет исполнять их в традиционной среде (недоверенной UNIX-подобной операционной системе – *Android*, *Debian*, *Ubuntu* и др.).

2. Модель оценки уровня защищенности информации, обрабатываемой программным обеспечением ДСИ на основе технологии *TrustZone*

Целью разработки модели является формирование признакового пространства, описывающего реализации ПО, функционирующего в ДСИ на основе технологии *TrustZone*, позволяющего оценить уровень защищенности информации, обрабатываемой данным ПО.

Анализ открытых источников информации [27,29,18,5] позволил выделить признаки, наличие которых в реализации ПО, может свидетельствовать о потенциальной опасности данного ПО с точки зрения возможной реализации угроз безопасности обрабатываемой информации. К ним относятся:

- наличие и количество точек входа и точек выхода данных (N_{in} и N_{out} соответственно), объем вводимых/выводимых данных (V_{in} и V_{out} соответственно);

- множество вызовов API-функций $F_{API\_TEE}^{unsafe}$, в том числе конкретных API-функций ДСИ, обрабатывающие критическую информацию и данные (учетные и аутентификационные данные, ключевую информацию для криптографической подсистемы, идентифицирующую(адресную) сетевую информации, сведения о технических характеристиках ЭВМ и т.п.);

- наличие вызовов функциональных объектов (функций) стандартных системных библиотек F_{system}^{unsafe} , в том числе обрабатывающих критически важную информацию и данные;

- наличие заданных последовательностей вызовов функциональных объектов, включающих вызов определенных API-функций и вызовов функциональных объектов стандартных системных библиотек IF^{unsafe} ;

- объем V_{WSM} и частота N_{WSM} обработки данных, поступающих из "недоверенной" ОС посредством буфера WSM (World Shared Memory) $\langle V_{in}^{WSM}, N_{in}^{WSM} \rangle$ и передаваемой из ДСИ в "недоверенную" ОС – $\langle V_{out}^{WSM}, N_{out}^{WSM} \rangle$.

Таким образом, модель оценки уровня защищенности информации, обрабатываемой программным обеспечением ДСИ на основе технологии *TrustZone* может быть представлена в виде кортежа:

$$Z = \langle N_{in}, N_{out}, V_{in}, V_{out}, F_{API\_TEE}^{unsafe}, F_{system}^{unsafe}, IF^{unsafe}, \langle V_{in}^{WSM}, N_{in}^{WSM} \rangle, \langle V_{out}^{WSM}, N_{out}^{WSM} \rangle \rangle. \quad (1)$$

В целях идентификации перечисленных признаков была разработана программа [40]. Структурная схема данной программы показана на рисунке 5.

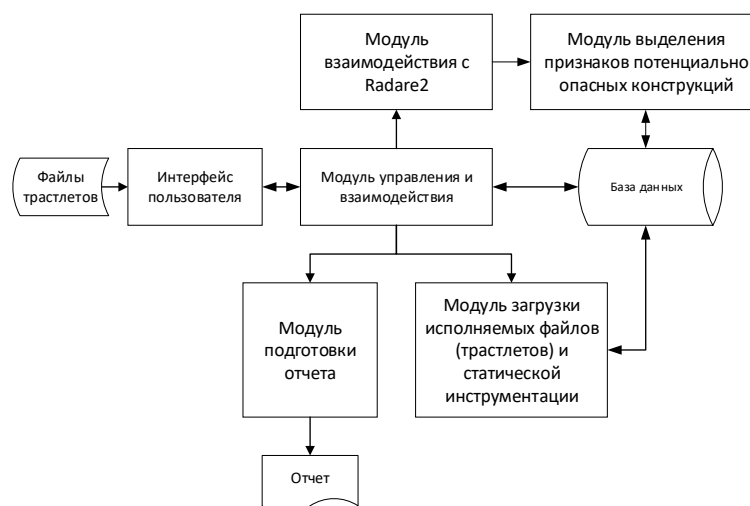


Рис. 5. Структурная схема программы идентификации признаков потенциально опасных конструкций

В основе данной программы лежит алгоритм, целью которого является анализ множества бинарных файлов ПО ДСИ на основе технологии *TrustZone* на предмет

наличия потенциально опасных конструкций, позволяющий определить уровень угроз безопасности обрабатываемой данным ПО информации и данных с учетом разработанной модели оценки защищенности.

Постановка задачи кластеризации трастлетов по наличию в них признаков потенциально опасных конструкций приведена ниже.

Исходные данные:

1) множество реализаций программного обеспечения (трастлетов) S , извлеченных из ДСИ на основе технологии *TrustZone "Aladdin TSM"*, *"OP-TEE"*, *"TrustTonic Kinibi"*;

2) модель Z оценки уровня защищенности информации, обрабатываемой программным обеспечением ДСИ на основе технологии *TrustZone*, отличающаяся от известных учетом логических признаков потоков ввода-вывода информации и API-вызовов.

3) множество пороговых значений частных показателей эффективности: $H = \{P_\alpha \leq P_\alpha^{\text{треб}}, P_\beta \leq P_\beta^{\text{треб}}, T_{\text{расп}} \leq T_{\text{расп}}^{\text{доп}}\}$, где P_α, P_β – вероятности ошибок 1-го и 2-го рода.

Требуется:

разработать алгоритм A кластеризации программного обеспечения доверенных сред исполнения на основе технологии *TrustZone*, учитывающий логические признаки потенциально опасных функциональных возможностей:

$$\left\{ \begin{array}{l} S \xrightarrow{A(Z)} \{L_i\}, i = \overline{1, N_L}, \\ \{P_\alpha \leq P_\alpha^{\text{треб}}, P_\beta \leq P_\beta^{\text{треб}}, T_{\text{расп}} \leq T_{\text{расп}}^{\text{доп}}\}. \end{array} \right. \quad (1)$$

3. Анализ бинарных файлов трастлетов

В файловых системах компьютерных систем на основе процессоров ARM файлы трастлетов, как правило, доступны непривилегированным пользователям. Пример наименования трастлетов в ОС Kinibi Trustonic представлены в таблице 1.

Таблица 1

Имена трастлетов формата *MCLF* в ОС *Kinibi Trustonic*

vendor.app.mcRegistry
07010000000000000000000000000000.tlbin
07060000000000000000000000000000.tlbin
ffffff000000000000000000000000b.tlbin
ffffff000000000000000000000000f.tlbin
system.app.mcRegistry
00060308060501020000000000000000.tlbin
ffffff000000000000000000000000c.tlbin
ffffff000000000000000000000000d.tlbin
ffffffd0000000000000000000000004.tlbin

Примеры наименования трастлетов в ОС на базе *Aladdin TSM* и *OP-TEE* представлены в таблице 2.

Таблица 2.

Имена трастлетов формата *HSTO* в ДСИ
на основе *OP-TEE* и *Aladdin TSM (JakartaBox)*

Aladdin TSM (JakartaBox)
5b9e0e40-2636-11e1-ad9e0002a5d5c51b.ta

48002366-708f-4b23-ab0921ce46766a11.ta
e6a33ed4-562b-463a-bb7eff5e15a493c8.ta
e13010e0-2ae1-11e5-896a0002a5d5c51b.ta
OP-TEE
5b9e0e40-2636-11e1-ad9e-0002a5d5c51b.ta
5ce0c432-0ab0-40e5-a056-782ca0e6aba2.ta
5dbac793-f574-4871-8ad3-04331ec17f24.ta
ffd2bded-ab7d-4988-95ee-e4962fff7154.ta

В целях исследования инструкций машинного кода в бинарных файлах траслетов было разработано и реализовано на языке *Python* средство для анализа бинарных файлов траслетов.

Данное средство функционирует по средствам API-вызовов к дизассемблеру *Radar2*, который в дальнейшем передается бинарный код, извлеченный из файлов траслетов. Поскольку форматы траслетов отличаются от известных для дизассемблера форматов, в частности, формата *ELF*, то в сценарии предусмотрено извлечение бинарного кода программы из файлов траслетов.

Данное средство позволяет идентифицировать строки форматов *ASCII* и *UNICODE*. Некоторые из этих строк являются названием переменных или функций. Далее если провести соответствия этих строк с системными вызовами операционной системы, то можно выявить, что траслет использует системные вызова для работы с файлами, сетевыми подключениями, обмена данными между защищенной оболочкой и незащищенной.

В таблице 3 приведен список некоторых функций, найденных с помощью программного средства на языке *Python*.

Таблица 3.

Имена системных функций в файле ffd2bded-ab7d-4988-95ee-e4962fff7154.ta

utee_storage_free_enum, utee_storage_reset_enum, utee_storage_start_enum, utee_storage_next_enum, utee_storage_obj_read, utee_storage_obj_write, utee_storage_obj_trunc, utee_storage_obj_seek	Работа с файловой системой
utee_hash_final, utee_cipher_init, utee_cipher_update, utee_cipher_final, utee_cryp_obj_get_info, utee_cryp_obj_restrict_usage, utee_cryp_obj_get_attr	Криптографическая функция
utee_open_ta_session, utee_invoke_ta_command, utee_close_ta_session	Работа с сессиями (обмен данными между траслетом и приложением посредством ОС)

Изучив последнюю группу системных вызовов, можно сделать вывод, что всем вызовам предшествует вызов функции *utee_open_ta_session*. Данная функция возвращает индикатор сессии, который используется в последующих вызовах. И после работы с системными функциями сессия закрывается *utee_close_ta_session*. То есть обмен информации траслета с другими приложениями будет происходить между вызовом *utee_open_ta_session* и *utee_close_ta_session*.

В результате исходя из данной информации можно выявить места системных вызова в машинном коде и определить тип функций для дальнейшей классификации по степени уязвимости или обрабатываемой информации.

Выводы

В рамках работы проведен анализ форматов исполняемых файлов для ДСИ на основе технологии TrustZone – трастлетов для ОС Kinibi Trustonic (смартфоны Samsung), OP-TEE (Linaro) и JacartaBox (Aladdin TSM). Выявлены их отличительные особенности и подходы, такие как статическая инструментация, позволяющие применять в дальнейшем в отношении трастлетов методы динамического анализа.

Методами статического анализа идентифицирован ряд логических (эвристических) признаков потенциально опасных конструкций кода, позволяющих оценить уровень защищенности информации, обрабатываемой трастлетами:

определены сигнатуры последовательностей машинных инструкций, обрабатывающих ввод-вывод данных от программного обеспечения "недоверенной" операционной системы;

идентифицированы вызовы системных API-функций в бинарном коде трастлетов;

выделены вызовы функциональных объектов стандартных системных библиотек "доверенной" ОС на основе TrustZone.

Литература

26. Закалкин, П. В. Система анализа программного обеспечения на предмет отсутствия недеklarированных возможностей / П. В. Закалкин, П. В. Мельников // Программная инженерия. 2018. Т. 9. № 2. С. 69–75.

27. Гамаюнов Д. Ю., Скворода А. А. Анализ мобильных приложений с использованием моделей привилегий и API-вызовов вредоносных приложений // Прикладная дискретная математика. 2017. № 36. С. 84-105. doi <http://doi.org/10.17223/20710410/36/7>.

28. Гамаюнов Д. Ю., Скворода А. А. Динамический анализ мобильных приложений // Программная инженерия. 2019. № 7-8. С. 324-333. doi <http://doi.org/10.17587/prin.10.324-333>.

29. Гайворонская, С. А. Гибридный метод обнаружения шеллкодов / С. А. Гайворонская, Д. Ю. Гамаюнов // Системы высокой доступности. Том 2, № 8. 2012. С. 33-44.

30. Варнавский, Н. П. Современное состояние исследований в области обфускации программ: определение стойкости обфускации / Н. П. Варнавский, В. А. Захаров, Н. Н. Кузюрин, А. В. Шокуров // Труды ИСП РАН. – Т. 26. Вып. 3. – 2014.

31. Казарин, О. В. Надежность и безопасность программного обеспечения / О. В. Казарин, И. Б. Шубинский. Москва : Издательство Юрайт. 2018. 342 с.

32. Бегаев, А. Н. Выявление уязвимостей и недеklarированных возможностей в программном обеспечении / А. Н. Бегаев, С. В. Кашин, Н. А. Маркевич, А. А. Марченко. Санкт-Петербург : Университет ИТМО, 2020. 38 с.

33. Марков, А. С. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов, А. В. Барабанов; под ред. доц. А. С. Маркова. Москва : Радио и связь, 2012. 192 с.

34. Ruan, X. Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine / X. Ruan // Apress, 2014.

35. Costan, V. Intel SGX Explained / V. Costan, S. Devadas // <https://eprint.iacr.org/2016/086.pdf>, 2016.

36. Costan, V. Sanctum: Minimal hardware extensions for strong software isolation / V. Costan, I. Lebedev, S. Devadas. // Proceedings of the USENIX Security Symposium. USENIX Association, 2016. P. 857–874.

37. Pinto, S. Demystifying Arm TrustZone: A Comprehensive Survey / S. Pinto, N. Santos. // ACM Computing Surveys, 2019. January 10. p. 36.

38. Cerdeira, D. SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems / D. Cerdeira, N. Santos, P. Fonseca, S. Pinto // Conference IEEE Symposium on Security and Privacy, San Francisco, CA, January 2020. p. 17.

39. Горюнов, М. Н. Распознавание функциональных объектов программного обеспечения в условиях отсутствия исходных текстов / М. Н. Горюнов [и др.] // Информационные системы и технологии. – 2013. – № 5. – С. 112–120.

40. Программное средство статического анализа бинарных файлов программ для доверенных сред исполнения на основе технологии TrustZone : свидетельство о государственной регистрации программы для ЭВМ № 2021610311 Российская Федерация / Н. П. Мешков, А. А. Полков, Д. О. Маркин, Н. Ю. Жуков, Д. В. Шibaков, Хо Т. Ч.; авторы и правообладатели Н. П. Мешков, А. А. Полков, Д. О. Маркин, Н. Ю. Жуков, Д. В. Шibaков, Хо Тхай Чунг. – № 2020665229 ; заявл. 24.11.2020; опубл. 13.01.2021; зарегистрировано в Реестре программ для ЭВМ 13.01.2021 г.

The approach to assessing the level of security of information processed by the software of trusted execution environments based on TrustZone technology

Markin D. O.¹⁴⁶, Kho T. Ch¹⁴⁷

Abstract. *The paper describes a model for assessing the level of security of information processed by bracelets of a trusted execution environment based on TrustZone technology. An algorithm is proposed that allows extracting signs of potentially dangerous constructions from binary files of trustlets. A formal statement of the problems of modeling the security assessment of the level of information processed by trustlets and the algorithm for clustering binary files of trustlets by the level of security (potential danger) is given)*

Keywords: TrustZone, ARM, static instrumentation, vulnerability search, detection of undeclared features.

¹⁴⁶ Dmitry Markin, candidate of technical sciences, The Academy of Federal Security Guard Service of the Russian Federation, Oryol, mdo@academ.msk.rsnnet.ru

¹⁴⁷ Kho Thai Chung, The Academy of Federal Security Guard Service of the Russian Federation, Oryol

Профиль защиты для бортовой ОС реального времени

Медведев Н.В.¹⁴⁸, Карташова Ж.К.¹⁴⁹

Аннотация. Рассматривается проблема разработки профиля защиты (ПЗ) для обеспечения информационной безопасности (ИБ) бортовой операционной системы (БОС) гражданского воздушного судна в соответствии с требованиями межгосударственного стандарта ГОСТ Р ИСО/МЭК 15408, определяющего проектирование, разработку и сопровождение подсистем защиты информации для любой автоматизированной информационной системы, в том числе операционных систем реального времени.

Ключевые слова: информационная безопасность, БВС, объект оценки, проблема безопасности, профиль защиты, задание по безопасности.

Введение

Организация (Заказчик), заинтересованная в приобретении конкретного типа продукта безопасности в рамках любой информационной технологии, излагает свои потребности в информационной безопасности в ПЗ, затем обеспечивает его оценку и выпуск [1]. Разработчик получает этот ПЗ, разрабатывает задание по безопасности (ЗБ), которое содержит утверждение о соответствии данному ПЗ, и обеспечивает оценку этого ЗБ [2]. Всё сказанное выше в полной мере можно отнести к операционным системам воздушных судов, которые являются системами реального времени [3].

- угрозы;
- политики безопасности;
- предположения безопасности [3, 4].

Взаимосвязь между содержанием ПЗ, ЗБ и ОО

Эти действия выполняются в рамках построения Профиля Защиты (ПЗ) на ПО, которое в рамках терминологии ГОСТ Р ИСО/МЭК 15408 обычно называется объектом оценки (ОО)¹⁵⁰. Также для стандартизации требований к любому ПО, включая ОС РВ, можно использовать Задания по Безопасности (ЗБ) и Пакеты защиты¹⁵¹.



¹⁴⁸Медведев Николай Викторович, МГТУ им. Н.Э. Баумана. Кафедра «Информационная безопасность»
medvedevnick54@yandex.ru

¹⁴⁹ Карташова Жанна Константиновна, МГТУ им. Н.Э. Баумана. Кафедра «Информационная безопасность», hannak@bmstu.ru

¹⁵⁰ docs.cntd.ru/document/1200101777

¹⁵¹ www.niisva.su/wp-content/uploads/2014/09/ГОСТ_Р_ИС...МЭК_15408-1-2012.pdf

Рис.1 Подсистема бортового управления

Угрозы, возникающие в процессе функционирования БОС

Угроза определяется негативным действием, выполняемым источником угрозы по отношению к некоторому активу¹⁵².

Негативные действия - действия, выполняемые источником угрозы по отношению к некоторому активу. Эти действия влияют на одну или более характеристик актива, которые связаны со значимостью данного актива.

Источники угроз могут быть описаны как отдельные сущности, но в некоторых случаях может оказаться предпочтительным описать их как типы сущностей, группы сущностей и т.п.

Примеры источников угроз - хакеры, пользователи, компьютерные процессы и инциденты. Далее источники угроз могут быть описаны через такие аспекты, как компетентность, доступные ресурсы, возможности и мотивация.

Примеры угроз:

- хакер (со значительной компетентностью, стандартным оборудованием и профинансированный для реализации угрозы), осуществляющий удаленное копирование конфиденциальных файлов из сети компании;
- компьютерный "червь", существенно снижающий производительность глобальной сети;
- системный администратор, нарушающий приватность пользователя;
- пользователь интернета, прослушивающий трафик конфиденциального электронного обмена.



Рис. 2. Модель угроз информационной безопасности в виде таблично-текстового описания

Модель злоумышленника

Использование беспроводных технологий подразумевает доступ к радиосвязи. Например, на борту планируется использовать мобильные телефоны, ноутбуки, RFID-тэги, повышающие угрозу НСД к беспроводным узлам "связанного" самолёта [1, 5-9].

Общей целью "врага" может считаться получение привилегированного доступа к операциям "связанного" самолёта путём атаки информационных активов. Враг для сети может быть внешним и внутренним. Он может использовать пассивные атаки (анализ сетевого трафика) и активные атаки (создавать ложный узел, компрометировать информацию от сенсоров/пользователей/контроллеров). Предполагается, что злоумышленник может глушить беспроводные каналы. С точки зрения прикладного ПО наиболее сложным представляется анализ принципов структурной организации

¹⁵² moluch.ru/archive/58/8087/

подсистемы защиты информации, а именно обеспечения блокировки НСД, сохранения целостности и поддержания конфиденциальности в режиме реального времени.

Именно поэтому для выбора математического аппарата формального выстраивания моделей нарушителя и противодействия оправданным оказался подход моделирования БОС РВ сетями Петри [10, 11]. Сети Петри представляют собой математическую модель для представления структуры и анализа динамики функционирования систем в терминах «условие-событие».

Общая структура модели противодействия угрозам для программного обеспечения БОС РВ представлена на рисунке 3.

Модели сетей Петри позволяют исследовать работоспособность моделируемых систем, оптимальность их структуры по некоторому критерию, эффективность процесса функционирования, а также возможность достижения в процессе функционирования определенных состояний. Сети Петри и их обобщения являются удобным средством моделирования параллельных систем, представляют динамику функционирования и составляющих их элементов.

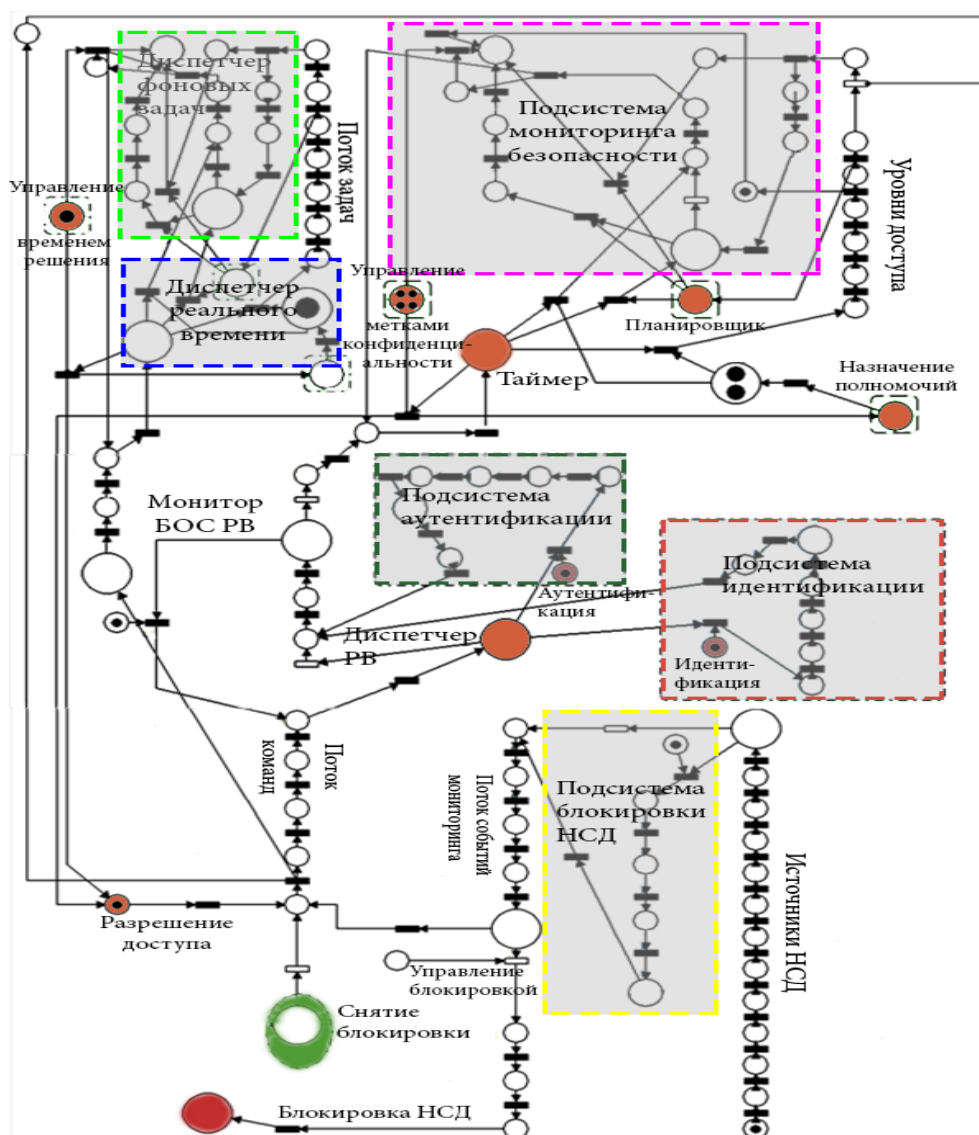


Рис. 3. Модель противодействия информационным угрозам на базе сетей Петри

Исследование показало высокую корреляцию применения мета-стандарта ГОСТ Р ИСО/МЭК 15408 («Общих критериев» [2-4]) и представленных в открытом доступе статистических данных [12-16].

Выводы

Для того, чтобы в процессе разработки ОС реального времени была заложена защита от угроз кибербезопасности, необходимо руководствоваться стандартами в области защиты информации.

Главным стандартом в данной области является стандарт ГОСТ Р ИСО/МЭК 15408, состоящий из трёх частей и регламентирующий стадии и содержание разработки требований к проектированию программного обеспечения, составляющего основу операционной системы.

Литература

1. Чичварин Н.В., Медведев Н.В. Угрозы информационной безопасности гражданского воздушного судна // В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019. С. 367-370.
2. Барабанов А.В., Марков А.С., Рауткин Ю.В. Оценка соответствия средств защиты информации требованиям высших оценочных уровней доверия//Труды НИИР. -2012. -№ 3. -С. 67-73.
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. 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.
5. Волосатова Т.М., Чичварин Н.В. Способы моделирования аппаратуры модульной авионики в условиях вредоносных воздействий // В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 58-63.
6. Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. 2016. № 6 (111). С. 85-96.
7. Глинская Е.В., Чичварин Н.В. Специфика конструирования бортовой аппаратуры модульной авионики с учетом требований информационной безопасности// В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 43-57.
8. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна // Вопросы кибербезопасности. 2018. № 4 (28). С. 9-20.
9. Елифанов В.Н. Открытые архитектуры в концепции авионики пятого поколения // Бодрунов С.Д. - Мир авионики. – 2014. – № 5. – С. 20–28.
10. Шрейдер М.Ю., Боровский А.С. Разработка моделей описания обработки информации в задачах управления системой защиты объекта на основе Сетей Петри // Вопросы кибербезопасности. 2018. № 1 (25). С. 46-53.
11. Болычев М.В., Мирошниченко Е.Л., Пасечник Р.М. Алгоритм построения диаграммы достижимости модели состояния работоспособности информационной системы // Вопросы кибербезопасности. 2019. № 6 (34). С. 79-91.
12. Интернет-ресурс: Документы ИКАО - Библиотека - Авиационный портал Airspot, airspot.ru/library/dokumenty-ikao, последний доступ – 01.04.2021.

13. Интернет-ресурс: Управление инспекции по безопасности полетов РФ/Анализ состояния безопасности полетов в гражданской авиации в 2013 году. www.dvmtu-favt.ru/upload/medialibrary/. Последний доступ – 01.04.2021.
14. Воздушный кодекс РФ от 19.03.1997 N 60-ФЗ / Консультант Плюс, w.consultant.ru/popular/air/. Последний доступ – 01.04.2021.
15. Интернет-ресурс: Радиосвязное оборудование (PCO). ooobskspetsavia.ru/, последний доступ – 01.04.2021.
16. Интернет-ресурс: <https://niika.dn.ua/public/dockfiles/Liman.pdf>, Последний доступ - 01.04.2021

Real time security profile for on-board OS

Medvedev N.V.¹⁵³, Kartashova J.K.¹⁵⁴

Abstract. *The problem of developing a protection profile (PP) to ensure information security (IS) of an on-board operating system (BOS) of a civil aircraft in accordance with the requirements of the interstate standard GOST R ISO / IEC 15408, which defines the design, development and maintenance of information security subsystems for any an automated information system, including real-time operating systems.*

Keywords: *information security, UAV, object of assessment, security problem, protection profile, security task.*

¹⁵³ Medvedev N.V., Ass Professor, Bauman Moscow State Technical University, medvedevnick54@yandex.ru

¹⁵⁴ Kartashova J.K., Ass Professor, Bauman Moscow State Technical University, hannak@bmstu.ru

Методика учета утечки излучения в оптическом волокнеМедведев Н.В.¹⁵⁵, Завадская Т.Е.¹⁵⁶

Аннотация. Как показывает анализ современных исследований оптическое волокно (ОВ), по существу, не имеет полной защиты от сторонних подключений и прослушивания. В настоящее время по оптическим каналам связи передается огромное количество критической и чувствительной информации и есть риск того, что она может попасть в руки нежелательных лиц, имеющих необходимые ресурсы и оборудование. Подключение к ОВ (fiber tapping) – процесс, при котором безопасность оптического канала компрометируется вставкой или извлечением световых сообщений. Подключение к ОВ может быть интрузивным либо неинтрузивным. Первый метод требует перерезания волокна и подсоединения его к промежуточному устройству для съема сообщений, в то время как при использовании второго метода, подключение выполняется без нарушения потока данных и перерыва сервиса. Противодействие именно таким несанкционированным подключениям – актуальнейшая задача в сегодняшнем комплексе проблем обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, ОВ, угрозы, методика, изгибы, микроизгибы, тестер.

Введение

Требования, предъявляемые к оптическим волноводам (ОВ), используемым в качестве передающей среды, а также к минимизации утечек и защита от НСД, накладывают и особые требования к модельному представлению ОВ, как объекта проектирования, а именно сочетания модели, построенной на основе волнового уравнения с модельными приближением на основе скалярной теории дифракции [1].

Концепция методики

Как известно, волноведущие участки достаточно велики между центрами связи, ретрансляторами и оконечными станциями, расположенными на расстоянии от нескольких сот метров до сотен километров¹⁵⁷. Потери при передаче сигналов, зависящие от фактического расстояния, однако должны превышать 100 дБ/км¹⁵⁸. Для волновода длиной в несколько километров они должны быть даже ниже 10 дБ/км. Дополнительное требование состоит в том, что сигналы не должны претерпевать слишком большого искажения даже при длине волноводов 10 км и более [2]. Кроме того, высокая протяженность и неизбежные «повороты» при монтаже волоконнооптической линии связи (ВОЛС) увеличивает вероятность НСД [1-7]. Для перекрытия расстояний в сотни и тысячи километров через каждые несколько километров или, возможно, через каждые несколько десятков километров неизбежно размещение ретрансляторов («повторителей»). Эти повторители поддерживают уровень сигналов путем усиления и при необходимости их регенерации для компенсации потерь мощности излучения. Это неизбежное проектное решение повышает возможность РСД¹⁵⁹. Как показал вышеприведенный анализ, для контролирования факта НСД на приемной станции ВОЛС устанавливается ответвитель с интерферометром Майкельсона [2]. При возникновении

¹⁵⁵Медведев Николай Викторович, МГТУ им. Н.Э. Баумана. Кафедра «Информационная безопасность» medvedevnick54@yandex.ru

¹⁵⁶ Завадская Татьяна Евгеньевна, МГТУ им. Н.Э. Баумана. Кафедра «Информационная безопасность», tzavadskaya@bmstu.net

¹⁵⁷ <https://pk-region.ru/raznoe-2/optovolokonnoe-podklyuchenie-k-internetu-optovolokonnoe-podklyuchenie-k-internet-osnovnye-principy-tekhnologii.html>

¹⁵⁸ <https://fac.ksu.edu.sa/sites/default/files/hfathallah/files/06149809-Optical%20Fiber%20Tapping%20Methods%20%20and%20Precautions.pdf>

¹⁵⁹ <https://habr.com/ru/post/176677/>

НСД между ретрансляторами таким способом ее регистрация невозможна¹⁶⁰. Поэтому к методике моделирования физических условий возникновения несанкционированной утечки излучения предъявляются особые требования. Как показал анализ, несанкционированная утечка осуществляется двумя способами [8]:

- Организация изгибов и микроизгибов.
- Создание в ОВ акустической решетки, обеспечивающей дифракцию Брегга.

Модельное представление ОВ для учета влияния изгибов и микроизгибов

При разработке этой части инженерной методики рассматривается геометрооптическое приближение¹⁶¹. Как известно [2, 8-12], передача сигналов на большие расстояния требует использования оптических волноводов с возможно низкими потерями и дисперсией. Поэтому они должны изготавливаться из материала наивысшего качества с точки зрения поглощения, рассеяния и дисперсии волн.

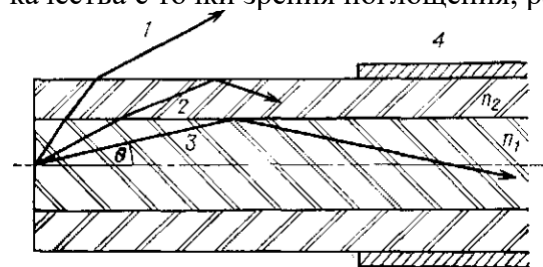


Рис 1. Двухслойное волокно с меридиональными световыми лучами.

1 — моды излучения; 2 — моды оболочки; 3 — моды сердцевины; 4 — защитный (поглощающий) чехол;

Исходными материалами для таких волноводов являются в основном высокопрозрачные и весьма однородные многокомпонентные стекла и чистый плавленый кварц. Волноводными структурами, наиболее полно сохраняющими высокое качество исходных материалов, являются волокна. Даже простые стеклянные волокна с постоянным показателем преломления можно использовать для того, чтобы улавливать свет и направлять его с использованием явления полного внутреннего отражения от стенок. Однако любые посторонние тела, которые соприкасаются с незащищенным волокном при его поддержке или размещении в трубе, нарушают полное внутреннее отражение и, следовательно, передачу излучения. Как показано выше, оптические волноводы в виде стеклянных волокон обычно состоят из стеклянной сердцевины, которая окружена стеклянной оболочкой с несколько меньшим значением показателя преломления. Световые волны, используемые для передачи сигналов, захватываются сердцевинкой и направляются с использованием полного отражения от границы сердцевина — оболочка. На рис. 1 представлено продольное сечение такой двухслойной модели волокна.

Кроме сердцевинки с показателем преломления и коаксиальной оболочки с показателем n_2 эту модель окружают второй оболочкой в виде чехла. Чехол является механической защитой волокна; он также может служить поглотителем света, падающего изнутри или снаружи волокна. Для этой цели чехол должен иметь соответствующие показатель преломления и постоянную поглощения; тогда он будет препятствовать перекрестной связи с другими волокнами в связке. Более того, поглощающий чехол подавляет любую вредную интерференцию со световыми лучами, выходящими из сердцевинки волокна; не претерпевая полного отражения от внешней границы оболочки, они поглощаются чехлом.

¹⁶⁰ <https://td-osz.ru/istorii-uspeha/kak-soedinit-dlya-optovolokonnyh-provoda-optovolokno-ot-operatora/>

¹⁶¹ <https://bezoblog.ru/raznye-stati/pochemu-dve-zhily-optovolokna-ispolzuyutsya-dlya-odnogo-optovolokonnogo-podklyucheniya.html>

Луч, падающий на торец волокна в центр сердцевины, принадлежит к классу меридиональных лучей, у которых плоскости падения включают ось волокна. Такой меридиональный луч, падающий из свободного пространства с показателем преломления $n = 1$ под углом θ_0 к оси, преломляется при вхождении в сердцевину и распространяется в ней под углом θ . До тех пор, пока угол θ остается меньше предельного угла

θ_{0c} полного внутреннего отражения от границы сердцевина — оболочка, определяемого соотношением $\cos \theta_{0c} = n_2/n_1$, сердцевина волокна будет удерживать этот луч. Следовательно, все меридиональные лучи, которые падают на переднюю поверхность волоконной сердцевины под углом θ_0 , меньшим θ_{0c} , для которого

$$\sin \theta_0 = \frac{\sqrt{n_1^2 - n_2^2}}{n_0} \quad (1)$$

будут удерживаться, благодаря полному отражению внутри сердцевины. Величина $\sin \theta_{0c}$ представляет собой числовую апертуру (NA) сердцевины волокна, т. е.

$$NA = \sin \theta_{0c} = \sqrt{n_1^2 - n_2^2} \quad (2)$$

Нарушение полного внутреннего отражения вследствие кривизны стенки в плоскости падения по-настоящему возникает только тогда, когда угол θ_c превышает угол θ_c . Такое нарушение только наличием кривизны полное внутреннее отражение будет иметь место до тех пор, пока угол распространения в плоскости падения остается меньше угла θ_c вплоть до значения $\psi_a = \theta_c$.

$$\cos \varphi = \cos \theta / \cos \psi \quad (3)$$

Соотношения (1), (2), (3) составляют модель ОВ для учета влияния микроизгибов [2, 11].

Структурная схема экспериментального стенда

Для проведения теоретико – экспериментальных исследований с использованием разработанной методики представляется целесообразным использовать стенд, структурная схема которого представлена на рис. 2 [2, 11].

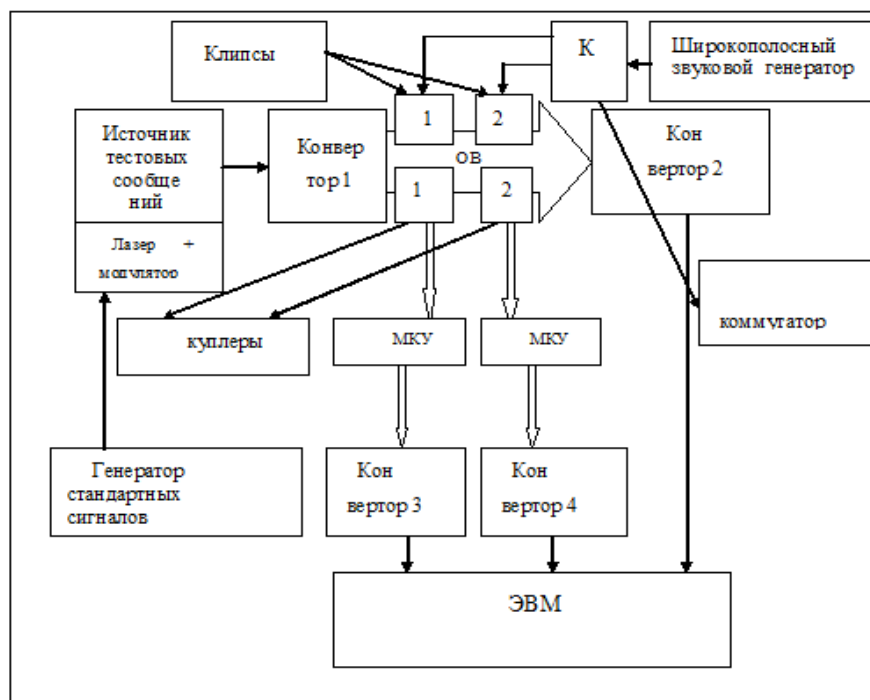


Рис. 2 Структурная схема экспериментального стенда

На Рис. 2: Клипсы – источники акустического излучения. Клипса 1 предназначена для создания микроизгиба в inspected ОБ. Клипса 2 предназначена для создания акустической дифракционной решетки, с помощью которой нарушается условия полного внутреннего отражения в ОБ. Коммутатор К обеспечивает переключение сигнала с широкополосного генератора. Источник тестовых сообщений формирует оптический сигнал с помощью генератора тестовых сигналов и модулятора лазерного излучения. Конвертор 1 формирует излучение, соответствующего протоколу ВОЛС. Конвертор 2 преобразует излучение, снимаемое с ОБ. Куплеры 1 и 2 осуществляют съем излучения из ОБ, возникающего на микроизгибах и акустической дифракционной решетке. Микроканальные усилители (МКУ) осуществляют усиление излучения, снятого куплерами. Это излучение преобразуется конверторами 1 и 2 в электрический сигнал, поступающий для последующего анализа в ЭВМ.

Выводы

На основе проводимых исследований следует такой вывод: уязвимость ВОЛС доказана на практике. А потому в связи с возможностью компрометации передаваемых данных или их модификации необходимо использовать средства криптографической защиты информации, передаваемой по ВОЛС. Для криптографической защиты следует выбрать средства, которые не вносят существенных временных задержек при криптографическом преобразовании передаваемой/принимаемой информации и обеспечивают шифрование/расшифровку для всего диапазона скоростей передачи данных [13, 14].

Литература

1. Филиппов М.В., Чичварин Н.В. Метод мониторинга информационной безопасности волоконной оптической линии связи // Инженерный журнал: наука и инновации. 2014. № 8 (32). С. 4.
2. Планарные и волоконные оптические волноводы / Угнер Х.Г. - М.: Мир, 1980, 640 с.
3. Sandra Kay Miller, «Hacking at the Speed of Light », Security Solutions Magazine, April 2016
4. Davis, USN, RADM John P.«USS Jimmy Carter (SSN-23): Expanding Future SSN Missions». Undersea Warfare, Fall 1999 Vol.2, No. I
5. Optical Illusion by: Sandra Kay Miller Information security Issue: Nov 2016.
6. Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for detection and Prevention, Keith Shaneman & Dr. Stuart Gray, IEEE Military Communications Conference 2014.
7. R. Jedidi and R. Pierre, High-Order Finite-Element Methods for the Computation of Bending Loss in Optical Waveguides, ILT, Vol. 25, No. 9, pp. 2618-30, SEP 2017.
8. Горлов Н.И., Шайгараева Т.Н. Способы несанкционированных подключений к ВОЛС // Инновационные, информационные и коммуникационные технологии. 2017. № 1. С. 192-195.
9. Зотова А.В., Петренко С.А. Безопасные сетевые технологии нового поколения // Защита информации. Инсайд. 2014. № 2 (56). С. 26-31.
10. Каталог "Средства противодействия экономическому шпионажу" / под ред. С.А.Петренко // Защита информации. Инсайд. 2017. № 1 (73). С. 63-112.
11. Модели, методы и средства обеспечения информационной безопасности и непрерывности информационного взаимодействия при использовании транспортных сетей передачи данных на базе ВОЛС / Волков А.Н., Галайко И.В., Грищенко С.А. и др. - Москва, 2019. 200 с.
12. Рахимов Н.Р., Трушин В.А., Бакшун Д.И., Кнутов В.А. Современные методы разработки информационной безопасности ВОЛС // Автоматика и программная инженерия. 2015. № 4 (14). С. 85-89.
13. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова, Т.И., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г., Медведев Н.В., Троицкий И.И., Чичварин Н.В. и др.: Под ред. Матвеева В.А. - М.: НИИ РИЛ МГТУ им.Н.Э.Баумана, 2013. - 244 с.

14. Комарова А.В., Менщиков А.А., Коробейников А.Г. Анализ и сравнение алгоритмов цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012// Вопросы кибербезопасности. 2017. №1(19). С 51-55.

Method for accounting the leakage in the optical fiber

Medvedev N.V.¹⁶², Zavadskaya T.E.¹⁶³

Abstract. *As the analysis of modern research shows, optical fiber (OF), in fact, does not have complete protection against third-party connections and eavesdropping. Currently, a huge amount of critical and sensitive information is transmitted over optical communication channels, and there is a risk that it may fall into the hands of undesirable persons who have the necessary resources and equipment. Fiber tapping is a process in which the safety of an optical channel is compromised by inserting or extracting light messages. The connection to the OB can be intrusive or non-intrusive. The first method requires cutting the fiber and connecting it to an intermediate device to retrieve messages, while using the second method, the connection is made without disrupting the data flow and interrupting the service. Countering such unauthorized connections is the most urgent task in today's complex of information security problems.*

Keywords: *information security, fiber optics, threats, technique, bends, microbends, tester.*

¹⁶² Medvedev N.V., Ass Professor, Bauman Moscow State Technical University, medvedevnick54@bmstu.ru

¹⁶³ Zavadskaya T.E., Ass Professor Bauman Moscow State Technical University, tzavadskay@bmstu.net

Информационная безопасность бортовой операционной системы гражданского воздушного судна с учетом требований ГОСТ Р ИСО/МЭК 15408

Медведев Н.В.¹⁶⁴, Глинская Е.В.¹⁶⁵

Аннотация. Рассматривается проблема разработки требований по обеспечению информационной безопасности (ИБ) бортовой операционной системы (БВС) самолета гражданской авиации в свете главного на сегодняшний день межгосударственного стандарта, определяющего проектирование, разработку и сопровождение подсистем защиты информации для любой автоматизированной информационной системы, в том числе операционных систем реального времени.

Ключевые слова: информационная безопасность, БВС, угрозы, профиль защиты, «связанные воздушные суда».

Введение

Основные требования к защите от киберугроз любой ОС, в нашем случае бортовой ОС (БОС) устанавливаются на уровне системного проектирования [1]. С точки зрения информационной безопасности, прежде всего, необходимо определить [2]:

- угрозы;
- политики безопасности;
- предположения безопасности.

Эти действия выполняются в рамках построения Профиля Защиты (ПЗ) на ПО, которое в рамках терминологии ГОСТ Р ИСО/МЭК 15408 обычно называется объектом оценки (ОО). Также для стандартизации требований к любому ПО, включая ОС РВ, можно использовать Задания по Безопасности (ЗБ) и Пакеты защиты.

Концепция «связанных» воздушных судов

Если в ЗБ утверждается о соответствии одному или более пакету и/или профилю защиты, оценка данного ЗБ будет (среди других характеристик данного ЗБ) демонстрировать, что ЗБ действительно соответствует этим пакетам и/или ПЗ, по отношению к которым утверждается о соответствии.

Это делает возможным организовать следующую последовательность действий:

- организация (Заказчик), заинтересованная в приобретении конкретного типа продукта безопасности ИТ, излагает свои потребности в безопасности в ПЗ, затем обеспечивает его оценку и выпуск;
- разработчик получает этот ПЗ, разрабатывает ЗБ, которое содержит утверждение о соответствии данному ПЗ, и обеспечивает оценку этого ЗБ;
- разработчик (потенциально, совместно с Заказчиком) создает ОО (или использует существующий) и обеспечивает его оценку на соответствие ЗБ. В этой ситуации необходимо наличие третьей стороны – независимого Оценщика, обеспечивающего доверие к ОО, ПЗ и ЗБ.

В современном мире гражданская авиация сталкивается с глобальной проблемой: мощный рост воздушного трафика, стоимость топлива, загрязнение окружающей среды [3-8]. Следствием этого являются крупномасштабные инициативы, рассчитанные на

¹⁶⁴Медведев Николай Викторович, МГТУ им. Н.Э. Баумана. Кафедра «Информационная безопасность» medvedevnick54@yandex.ru

¹⁶⁵ Глинская Елена Вячеславовна, МГТУ им. Н.Э. Баумана. Кафедра «Информационная безопасность», glinskaya@bmstu.ru

следующие два десятилетия и призванные построить систему воздушного транспорта нового поколения.

Среди них выделяется система "Связанных" воздушных судов, обещающая революцию в отрасли. (Прим.: eEnabled - реализующая работу и связь посредством Интернета, переведена как "Связанная", имея в виду постоянную связь с глобальной сетью). "Связанные" воздушные суда будут обладать новейшей авионикой и выгодными готовыми беспроводными решениями для упрощения работы, обслуживания, контроля. Например, модули GPS и ADS-B для контроля воздушного трафика, беспроводные точки доступа для передачи ПО и данных, RFID и беспроводные сенсоры для мониторинга состояния системы. Со всем этим на борту, "Связанным" воздушным судам необходимо будет быть самостоятельными узлами в *Авиационных самоорганизующихся сетях (AANET)*, повсеместно общаясь с наземной инфраструктурой и другими бортами. Увеличение информационных потоков от самолётов к земле, от земли к самолётам, между самолётами при помощи AANET позволит повысить безопасность полётов, точность расписания, эффективность обслуживания, уровень обслуживания пассажиров [9-12].

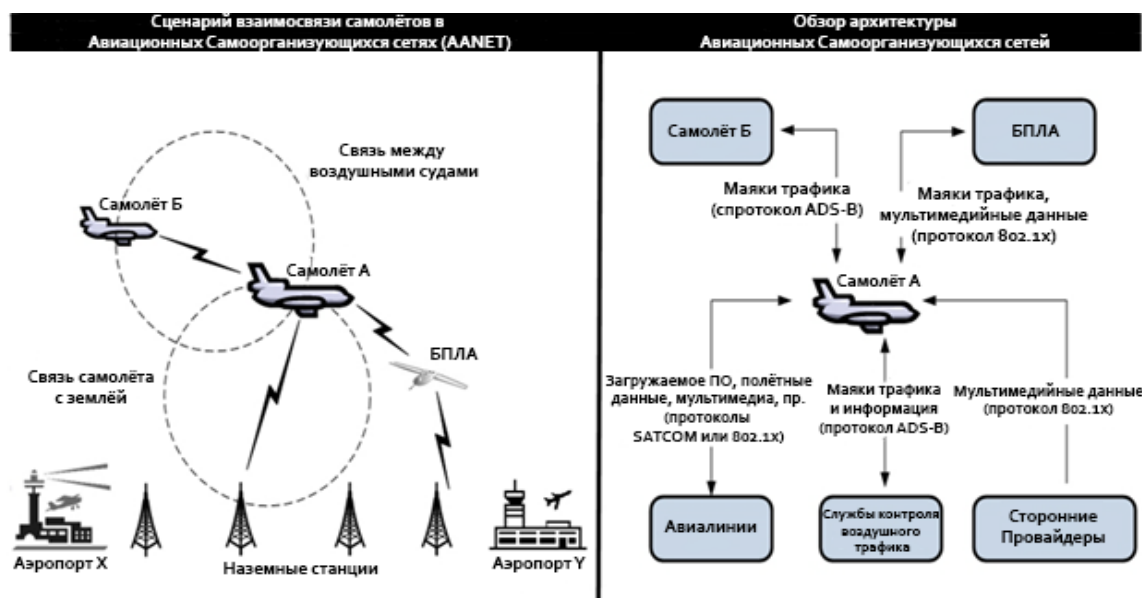


Рис. 1. "Связанные" воздушные суда

Однако же готовые беспроводные решения могут иметь уязвимости, понижающие уровень безопасности "Связанных" воздушных судов. При этом существующие хорошо известные стандарты в области не покрывают потребности безопасности в случае беспроводных решений. Для защиты предлагаемой сети необходимо обеспечивать защиту волновых соединений систем бортового судна.

Использование беспроводных технологий подразумевает доступ к радиосвязи. Например, на борту планируется использовать мобильные телефоны, ноутбуки, RFID-тэги, повышающие угрозу НСД к беспроводным узлам "связанного" самолёта.

Реализация возможных угроз

Общей целью "врага" может считаться получение привилегированного доступа к операциям "связанного" самолёта путём атаки информационных активов. Враг для сети может быть внешним и внутренним. Он может использовать пассивные атаки (анализ сетевого трафика) и активные атаки (создавать ложный узел, компрометировать информацию от сенсоров/пользователей/контроллеров). Предполагается, что злоумышленник может глушить беспроводные каналы.

Повреждение активов. Враг может попытаться повредить критически-важные активы ААNET-сети для создания благоприятных условий входа в сеть на фоне снижения её эффективности, или для извлечения выгоды от ложных тревог и позднего обнаружения взлома, ведущего к задержкам рейсов.

Несанкционированное использование активов. Активы могут содержать информацию, способную помочь в атаках другими способами, например, местоположения самолётов, уровни топлива. Также информация может представлять коммерческую ценность для конкурентов.

Помехи. Любой узел ААNET-сети может оказаться заблокированным после обнаружения в нём подозрительной деятельности.

Задержки активов. Активы можно сделать недоступными, глуша беспроводное соединения или прерывая выполнение приложений.

Целостность и аутентичность. Для предотвращения повреждения активов злоумышленником необходим механизм проверки целостности и аутентичности передаваемых сообщений.

Авторизация. Каждый пользователь и процесс, имеющие доступ к информации в ААNET-сети должны быть идентифицированы, их разрешения и уровень доступа должны быть проверены.

Конфиденциальность. Не должен иметься доступ к важным активам без соответствующих прав.

Раннее обнаружение. Любая манипуляция с активами должна быть обнаружена как можно быстрее для предотвращения временных срывов.

Доступность. Каждый актив должен быть доступен по первому требованию.

Отслеживаемость и неотказуемость. Все действия в сети должны быть авторизованы, иметь автора, получателя, исполнителя.

Пример построения модели угроз ИБ системы:

№№	Тип угрозы	Возможные последствия
1.	Анализ сетевого трафика	Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
2.	Сканирование сети	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
3.	Угроза выявления пароля	Выполнение любого действия, связанного с получением несанкционированного доступа
4.	Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации

Табл. 1. Вербальная модель угроз БОС РВ гражданского воздушного судна
На основе таблицы 1 можно дать экспертную оценку угроз информационной безопасности.

Угроза ИБ $i, i = 1, \dots, m$	Вероятность реализации угрозы нарушителем категории $j, j = 1, \dots, n$						Ущерб			
	1	2	3	4	5					
Анализ сетевого трафика U1	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}	P_{18}	P_{19}	P_{110}
Сканирование сети U2	P_{21}	P_{22}	P_{23}	P_{24}	P_{25}	P_{26}	P_{27}	P_{28}	P_{29}	P_{210}
Угроза выявления пароля U3	P_{31}	P_{32}	P_{33}	P_{34}	P_{35}	P_{36}	P_{37}	P_{38}	P_{39}	P_{310}
Подмена доверенного объекта сети U4	P_{41}	P_{42}	P_{43}	P_{44}	P_{45}	P_{46}	P_{47}	P_{48}	P_{49}	P_{410}

Табл. 2. Пример экспертной оценки вероятности реализации угрозы безопасности различными категориями нарушителей $j, j = 1, \dots, n$

Выводы

На основе представленной модели угроз можно выстроить требования к подсистеме обеспечения кибербезопасности системного и прикладного программного обеспечения БОС РВ. С точки зрения прикладного ПО наиболее сложным представляется анализ принципов структурной организации подсистемы защиты информации, а именно обеспечения блокировки НСД, сохранения целостности и поддержания конфиденциальности в режиме реального времени.

Литература

1. Чичварин Н.В., Медведев Н.В. Угрозы информационной безопасности гражданского воздушного судна // В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019. С. 367-370.
2. 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.
3. Волосатова Т.М., Чичварин Н.В. Способы моделирования аппаратуры модульной авионики в условиях вредоносных воздействий // В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 58-63.
4. Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. 2016. № 6 (111). С. 85-96.
5. Глинская Е.В., Чичварин Н.В. Специфика конструирования бортовой аппаратуры модульной авионики с учетом требований информационной безопасности// В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 43-57.
6. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования гражданского судна // Вопросы кибербезопасности. 2018. № 4 (28). С. 9-20.
7. Чичварин Н.В. Базовые программные средства рабочих станций анализа ГИС-информации // Вопросы кибербезопасности. 2014. № 5 (8). С. 7-16.

8. Чичварин Н.В. Оптическая система связи и навигации для обеспечения безопасной посадки самолета // Информационно-измерительные и управляющие системы. 2018. Т. 16. № 10. С. 43-51.
9. Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing model 7878 airplane; systems and data networks securityisolation or protection from unauthorized passenger domain systems access, [Docket No. NM364 Special Conditions No. 250701SC], Federal Register, Vol. 72, No. 71., 2015, <http://edocket.access.gpo.gov/2015/pdf/E7-7065.pdf>
10. Federal Aviation Administration, 2014, 14 CFR Part 25, Special Conditions: Boeing model 7878 airplane; systems and data networks securityprotection of airplane systems and data networks from unauthorized external access, [Docket No. NM365 SpecialConditions No. 250702SC], Federal Register, Vol. 72, No. 72., 2014, <http://edocket.access.gpo.gov/2014/pdf/07-1838.pdf>
11. C. Wargo and C. Dhas, "Security considerations for the e-enabled aircraft," Proceedings of Aerospace Conference, 2014.
12. G. Bird, M. Christensen, D. Lutz, and P. Scandura, "Use of integrated vehicle health management in the field of commercial aviation," in Proceedings of NASA ISHEM Forum, 2015.

Information security of the on-board operating system of a civil aircraft, taking into account the requirements of GOST R ISO / IEC 15408

Medvedev N.V.¹⁶⁶, Glinskaya E.V.¹⁶⁷

Abstract. *The problem of developing requirements for ensuring information security (IS) of an on-board operating system (BOS) of a civil aviation aircraft is considered in the light of today's main interstate standard that defines the design, development and maintenance of information security subsystems for any automated information system, including operational real time systems.*

Keywords: *information security, UAV, threats, security profile, “linked aircraft”.*

¹⁶⁶ Medvedev N.V., Ass Professor, Bauman Moscow State Technical University, medvedevnick54@bmstu.ru

¹⁶⁷ Glinskaya E.V., Ass Professor Bauman Moscow State Technical University, glinskaya@bmstu.ru

Подход к интеграции разнородных рисков на примере анализа целей, задач и угроз по доктрине энергетической безопасности

Нистратов А.А.¹⁶⁸

***Аннотация.** Для систем, опирающихся в жизненном цикле на реализацию стандартизованных процессов, предложен подход к интеграции разнородных рисков, способствующий формированию логико-вероятностной основы создания иерархической системы управления рисками. Фрагментарная демонстрация подхода осуществлена в приложении к действующей доктрине энергетической безопасности Российской Федерации.*

***Ключевые слова:** анализ, интеграция, модель, риск, управление.*

1. Введение

В настоящей работе рассматриваются различного рода сложные системы и реализуемые типовые процессы согласно ГОСТ Р 57193. При этом под системой понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких целей. Методический подход к интеграции разнородных рисков изложен вне привязки к функциональному назначению систем и составных элементов (например, [1-8]). Такая зависимость учитывается опосредовано – лишь на уровне состава элементов и структуры системы, сценария использования стандартизованных процессов (включая выполняемые при этом действия, влияющие на временные характеристики реализации процессов), возможных угроз реализации процессов, дополнительных требований и условий, выражаемых во временных характеристиках и подлежащих учету.

С практической точки зрения актуальность работы объясняется, с одной стороны, важностью обеспечения качества и безопасности современных систем, а с другой – сложностью этих систем негативными последствиями при реализации разнородных угроз в условиях множественных неопределенностей. В основе интеграции разнородных рисков лежат достаточно общие идеи системной инженерии, логически обуславливающие практическую полезность предлагаемого подхода к широкому кругу систем, апробированные на практике вероятностные модели, разработанные ранее [9-16], и предлагаемый в настоящей работе метод для задаваемой совокупности стандартизованных процессов, применяемых в жизненном цикле различного рода систем. Демонстрация подхода рассмотрена на примере анализа целей, задач, рисков и угроз по доктрине энергетической безопасности РФ.

2. Общие положения

Предполагается, что при создании (модернизации, развитии), эксплуатации и выведении из эксплуатации сложных современных систем ориентируются на процессный подход. Используются типовые процессы соглашения (приобретения и поставки), процессы организационного обеспечения проекта (управления моделью жизненного цикла, инфраструктурой, портфелем проекта, человеческими ресурсами, качеством, знаниями), процессы технического управления (планирования, оценки и контроля проекта, управления решениями, управления рисками, управления

¹⁶⁸ Нистратов А.А., к.т.н., ФБУ «НТЦ Энергобезопасность», e-mail: andrey.nistratov@gmail.com

конфигурацией, управления информацией, измерений, гарантии качества) и технические процессы (анализа бизнеса или назначения системы, определения потребностей и требований заинтересованной стороны, определения системных требований, архитектуры, проекта, системного анализа, реализации, комплексирования, верификации, передачи, аттестации, функционирования, сопровождения, изъятия и списания системы). Всего 30 стандартизованных процессов, $I = 30$.

С инженерной точки зрения в любой момент времени у лиц, принимающих решение (ЛПР) о качестве и безопасности выполнения типового процесса или функционирования мониторируемого объекта в сложной системе, есть объективное или субъективно экспертное представление о том, какое состояние текущего процесса или объекта «приемлемо», а какое «неприемлемо» и требует управляющей реакции для улучшения (полагается, что субъективные оценки используются тогда, когда формальные нормы не установлены или практически не применимы). Т.е. в каждый отчетный момент времени по объективным значениям каждого из отслеживаемых критичных показателей (или по экспертному мнению ЛПР) можно с однозначной уверенностью определить, что значения выбранного показателя находятся в зоне, которая может быть охарактеризована как «Приемлемое» состояние (т.е. такое состояние, характеризующееся соответствующими нормальными условиями и ресурсами, при котором обеспечивается достижение целей функционирования системы или соответствующего элемента системы) или как состояние «Приемлемое с отклонением» от нормы (когда требуются определенные организационные или плановые усилия по улучшению значения показателя до состояния «Приемлемое») или как «Неприемлемое» состояние (когда требуются кардинальные решения по восстановлению нормальных условий и/или ресурсов, которые в существующем виде уже не обеспечивают требуемого качества или безопасности выполнения типового процесса и при бездействии ведут к неприемлемому ущербу для системы) [14–18]. Состояния «Приемлемое», «Приемлемое с отклонением», «Неприемлемое» – это элементарные состояния, в которые может переходить во времени критичный показатель, характеризующий выполнение типового процесса. Примером может служить процесс функционирования оборудования в опасном производстве – см., например ГОСТ Р 58494, в рамках которого реализованы некоторые авторские модели [10-18].

3. Предлагаемый подход к интеграции разнородных рисков

Интегральный риск нарушения приемлемого выполнения совокупности стандартизованных процессов предлагается оценивать в зависимости от реальных или гипотетичных исходных данных, характеризующих каждый типовой процесс, от возможного сценария использования процессов в период прогноза. Период прогноза может охватывать любой промежуток времени при создании (модернизации, развитии) и/или эксплуатации и/или выведении из эксплуатации сложных систем, включающий в себя как минимум один законченный процесс каждого из типов, задействованных в рассматриваемой совокупности стандартизованных процессов в задаваемом сценарии. Пример выполняемых стандартизованных процессов на временной оси представлен на рисунке 1. В общем случае сценарий использования стандартизованных процессов $i_1, i_2, \dots, i_k$ (включая выполняемые при этом действия) предлагается определять реальной или гипотетичной частотой выполнения этих процессов. Учитывается, что любой типовой процесс может входить в состав работ, выполняемых в рамках других стандартизованных процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

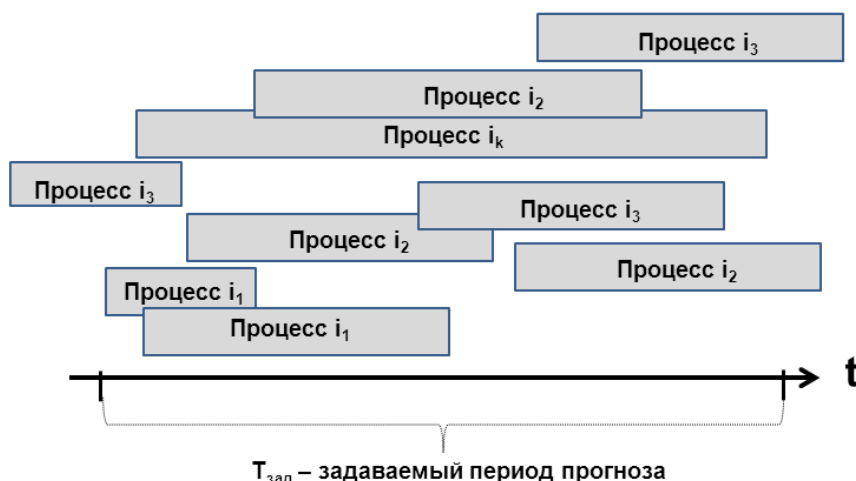


Рисунок 5 – Пример выполняемых стандартизованных процессов на временной оси

Интегральный риск нарушения приемлемого выполнения совокупности стандартизованных процессов $R_{\text{интегр}}(T_{\text{зад}})$ за задаваемый период прогноза $T_{\text{зад}}$ предлагается оценивать по формуле

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - \sum_{i=1}^I \lambda_i \{1 - R_i(T_{\text{зад}} i) [Ind(\alpha_i)]\} / \sum_{i=1}^I \lambda_i, \quad (1)$$

где λ_i — частота выполнения стандартизованных процессов i -го типа за период прогноза. Если длительность выполняемого процесса может выходить за рамки периода прогноза (что зависит от выполняемых действий и их временных характеристик), эта частота может быть дробным числом, характеризующим количество выполнений процесса каждого типа, большим единицы;

$R_i(T_{\text{зад}} i)$ — риск нарушения реализации i -го типа процессов, $i = 1, \dots, I$, $I=30$. Для расчета могут быть использованы любые приемлемые методы, см., например ГОСТ Р 58494-2019, ГОСТ Р 59329 – ГОСТ Р 59357-2021, в рамках которых реализованы некоторые из предложенных авторских моделей [10-18].

$T_{\text{зад}}$ - задаваемый период прогноза, покрывающий длительность всех задаваемых периодов $T_{\text{зад}} i$ каждого из стандартизованных процессов, задействованных в сценарии. Предположение о частично выполненном процессе, который может начаться в конце периода прогноза и не закончиться (при общем количестве процессов каждого из типов, большем, чем один), может быть удовлетворено заданием дробного значения λ_i .

При этом критерий выполнения требований и условий (α_i) по каждому типу процессов, включая требования по допустимым рискам и ущербам, устанавливают с использованием индикаторной функции $Ind(\alpha)$:

$Ind(\alpha)$

$$= \begin{cases} 1, & \text{если задаваемые требования и условия выполняются, т.е. условие } \alpha \text{ истинно,} \\ 0, & \text{в противном случае, т.е. если условие } \alpha \text{ ложно.} \end{cases}$$

Предлагаемые подход применимы для решения практических задач системной инженерии, связанных с прогнозированием и интеграцией разнородных рисков, обоснованием эффективных предупреждающих мер по снижению рисков или их удержанием в допустимых пределах.

4. Пример интеграции разнородных рисков

Согласно "Доктрине энергетической безопасности Российской Федерации", утвержденной Указом Президента Российской Федерации от 13.05.2019 № 216 (далее по тексту – Доктрина) и «Энергетической стратегии Российской Федерации на период до 2035 года», утвержденной распоряжением Правительства Российской Федерации от 9 июня 2020 г. № 1523-р, энергетика РФ вносит значительный вклад в национальную безопасность и социально-экономическое развитие страны. С учетом множества факторов неопределенности состоянию энергетической безопасности РФ присущи долговременные разнородные вызовы, угрозы и риски.

Имея ввиду предложенное выражение (1) для прогнозирования и интеграции разнородных рисков, из вербального описания Доктрины возможно составить логико-вероятностную схему интеграции рисков, например, для иерархического уровня федерального округа: «Цели – направления деятельности – решаемые задачи – риски для достижения цели – угрозы, определяющие риски – характеристики угроз для моделирования» – см. фрагмент предлагаемой схемы на рис. 1. Обозначения непосредственно привязаны к нумерации и тексту Доктрины.

В качестве корня дерева (0-й ярус) выступает сам федеральный округ. А характеристики угроз, используемые в качестве исходных данных при моделировании и расчетах критериев, образуют вершины последнего яруса дерева. Эти последние вершины могут быть представлены с помощью универсальной вспомогательной модели показателя (см., например, ГОСТ Р 59349-2021). Применительно к 0-му ярусу - корню (т.е. применительно к рассматриваемому федеральному округу) выбирают свойственные цели по п. 22 а)-22о) Доктрины. Они образуют 1-й ярус дерева, т.е. каждая цель по п.22 а)-22о) Доктрины – это вершина 1-го яруса. Всего для условно i-го федерального округа РФ максимально может быть 14 вершин 1-го яруса: i.1-я вершина обозначена 22а), i.14-я вершина – обозначена 22о). В качестве вершин 2-го яруса рассматриваются направления деятельности из Доктрины для достижения цели, 3-го яруса - решаемые задачи в рамках направления деятельности, на 4-м ярусе - риски для достижения целей путем решения конкретных задач, на 5-м ярусе – угрозы, определяющие эти риски, на 6-м ярусе – характеристики угроз для моделирования. Например, каждое направление по п.24 а)-24д) Доктрины образует вершину 2-го яруса, всего – 5 вершин 2-го яруса. Так, на рисунке 1 от i.2-й вершины 1-го яруса идут ветви к вершинам 2-го яруса, тогда соответствующие вершины 2-го яруса обозначаются от 22б)-НД24а) до 22б)-НД24д), а для i.12-й вершины 1-го яруса – соответственно от 22м)-НД24а) до 22м)-НД24д).

Решаемые задачи для каждого из направлений деятельности образуют 3-й ярус дерева, т.е. каждая задача по пп. 25-29 Доктрины – это вершины 3-го яруса. Таким образом, для направления деятельности 24а) Доктрины может быть до 13 вершин 3-го яруса. На ветвях от первой вершины 2-го яруса 22а)-НД24а) (такое обозначение для вершины 2-го яруса означает цель, связанную с воспроизводством минерально-сырьевой базы ТЭК согласно п. 22а) Доктрины и направление деятельности «совершенствование государственного управления в области обеспечения энергетической безопасности» согласно п. 24а) Доктрины) образуются вершины 3-го яруса. В частности, первая вершина будет означать первую решаемую задачу – «а)совершенствование нормативно-правовой базы по вопросам обеспечения безопасного, надежного и устойчивого функционирования инфраструктуры и объектов энергетики» согласно п. 25а) Доктрины, эта вершина будет обозначаться 22а)-НД24а)-325а), а 13-я вершина 3-го яруса, относящаяся к задаче «н) стимулирование энергосбережения и повышения энергетической эффективности экономики» по п.25н) Доктрины будет обозначаться 22а)-НД24а)-325н). Для 5-го направления деятельности 24д) Доктрины всего будет до 6 вершин 3-го яруса. Тогда для этого направления деятельности 1-я вершина яруса обозначается 22а)-НД24д)-329а), а 6-я вершина, относящаяся к задаче по п.29е) Доктрины, будет обозначаться 22а)-НД24д)-329е).

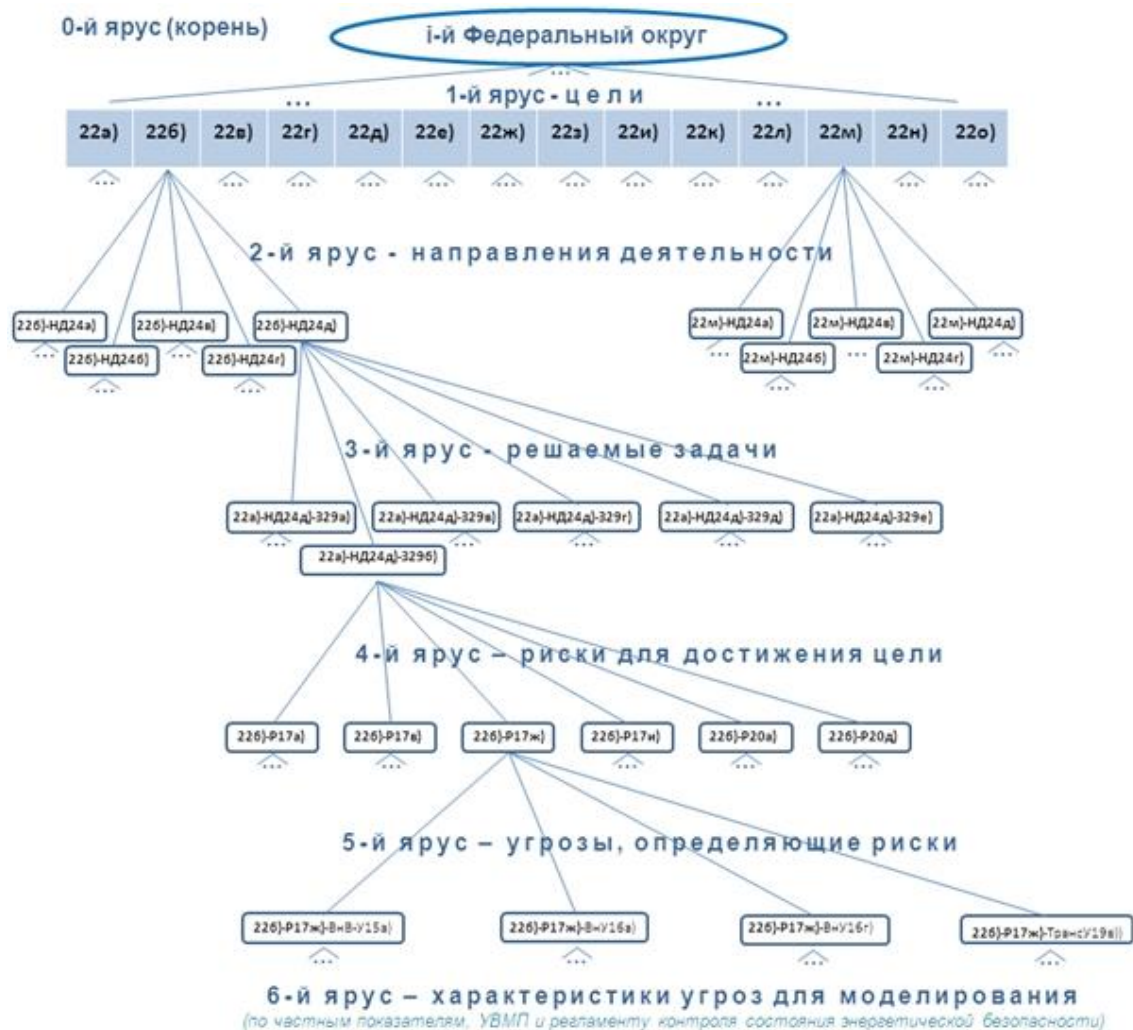


Рисунок Г.3 - «Логическое дерево» для описания связи «цели – направления деятельности - решаемые задачи - риски - угрозы – характеристики угроз»

Предложенный вариант интеграции рисков на уровне «логических деревьев», образуемых из вербального описания Доктрины, и формульное выражение (1) образуют логико-вероятностную основу создания иерархической системы управления рисками для обеспечения энергетической безопасности РФ.

Вывод

Предлагаемый подход позволяет осуществлять интеграцию разнородных рисков для систем, опирающихся в жизненном цикле на реализацию стандартизованных процессов. Демонстрация подхода осуществлена в приложении к действующей доктрине энергетической безопасности Российской Федерации. Рациональное использование предложенного метода интеграции в жизненном цикле энергетических систем может составить логико-вероятностную основу создания иерархической системы управления рисками для обеспечения энергетической безопасности РФ. Достоверность подтверждена на уровне демонстрации метода по предложениям автора статьи в примерах стандарта ГОСТ Р 59349-2021 «Системная инженерия. Защита информации в процессе системного анализа».

Литература

1. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Концептуальная модель анализа риска безопасности информационных технологий // Вопросы кибербезопасности. 2020. №2. С. 2-10. DOI: 10.21681/2311-3456-2020-02-2-10.
2. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1 (25). С. 28-38.
3. Братченко А. И., Бутусов И.В., Кобелян А.М., Романов А.А. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления // Вопросы кибербезопасности. 2019. №. 1 (29). С. 18-24.
4. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB // Вопросы кибербезопасности. 2015. № 4 (12). С. 53-61.
5. Госькова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. №2. С.42-49. DOI: 10.21681/2311-3456-2019-2-42-49.
6. Костогрызов А.И., Лазарев В.М., Любимов А.Е. Прогнозирование рисков для обеспечения эффективности информационной безопасности в их жизненном цикле // Правовая информатика. 2013. № 4. С. 4-16.
7. Петренко С.А., Беляев А.В. Управление рисками ИТ-безопасности: SOA 404 // Защита информации. INSIDE. - 2007. - № 5. - С. 24-29.
8. Цирлов В., Марков А. Управление рисками -нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. № 8. С. 63-67.
9. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд. "Вооружение, политика, конверсия", 2008. – 404с.
10. Andrey Kostogryzov, Andrey Nistratov, George Nistratov Some Applicable Methods to Analyze and Optimize System Processes in Quality Management // InTech. 2012. P. 127–196. URL = <http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management>
11. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G. Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V. 1. P. 217–244. <http://www.scirp.org/journal/ajor/>
12. Andrey Kostogryzov, Pavel Stepanov, Andrey Nistratov, George Nistratov, Oleg Atakishchev and Vladimir Kiselev Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling // Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186-192.
www.dropbox.com/s/a4zw1yds8f4ecc5/AMSM2016%20Full%20Proceedings.pdf?dl=0
13. Костогрызов А.И., Степанов П.В., Нистратов А.А., Григорьев Л.И., Червяков Л.М. Прогнозирование рисков для обеспечения качества информации в сложных системах // Системы высокой доступности №3, т.2, 2016, с. 25-37
14. Vladimir Artemyev, Andrey Kostogryzov, Jury Rudenko, Oleg Kurpatov, George Nistratov, Andrey Nistratov Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20-22, 2017, Milan, Italy, pp. 368-373
15. Vsevolod Kershenbaum, Leonid Grigoriev, Petr Kanygin and Andrey Nistratov / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, pp. 55-79. <http://dx.doi.org/10.5772/intechopen.74963>
16. Probabilistic Modeling in System Engineering. / By ed. A.Kostogryzov, - London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
17. KOSTOGRYZOV Andrey, Nistratov Andrey Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. Safety and Reliability of Systems and Processes / Gdynia Maritime University, 2020. pp. 153-174, <https://ssars.umg.edu.pl/>

18. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364. <https://www.springer.com/gp/book/9783030468941>

Approach to the integration of heterogeneous risks on the example of the analysis of goals, objectives and threats according to the Energy Security Doctrine

Nistratov A.A.¹⁶⁹

Abstract

For systems that implement standardized processes in the life cycle, an approach to the integration of heterogeneous risks is proposed. It can form a logical and probabilistic basis for creating a hierarchical risk management system. The demonstration of the approach is carried out in fragment application to the current Energy Security Doctrine of the Russian Federation.

Keywords: *analysis, integration, model, risk, control.*

¹⁶⁹ Nistratov A.A., Ph.D., “Scientific&Technical Center Energobezопасnost”, Moscow

Применение методов машинного обучения при проведении фаззинг-тестирования Осипова Н.С.¹⁷⁰

Аннотация. В наши дни большинство обнаруженных ошибок в программном обеспечении, связанных с удаленным выполнением кода и повышением привилегий, найдены при помощи фаззинга. Интеграция фаззинг-тестирования в процесс разработки программного кода позволяет выявлять ошибки и уязвимости на ранних стадиях. Вследствие существующих ограничений методов анализа программ, фаззинг-тестирование может быть недостаточно эффективным. В данной статье рассмотрены существующие подходы к применению методов машинного обучения на разных этапах фаззинга, а также предложены актуальные направления для дальнейших исследований.

Ключевые слова: программные дефекты, фаззинг-тестирование, машинное обучение.

Введение

Согласно ГОСТ Р 50922-2006 под уязвимостью понимается свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации [1]¹⁷¹. Обнаружение уязвимостей можно проводить в ручном режиме или же используя различные средства автоматизации.

Безопасное программное обеспечение – программное обеспечение (ПО), разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы.

В соответствии с руководящими документами по безопасной разработке разработчик ПО должен реализовать функциональное тестирование программы, тестирование на проникновение, динамический анализ кода программы, а также фаззинг-тестирование.

Фаззинг – методика тестирования, при которой на вход программы подаются невалидные, непредусмотренные или случайные данные, которые могут привести её к аварийному завершению или неопределённому поведению. Чтобы предотвратить действия нарушителей, необходимо оперативно выявлять и устранять уязвимости. Среди множества доступных сегодня методов обнаружения уязвимостей программного обеспечения фаззинг по-прежнему пользуется большой популярностью благодаря своей концептуальной простоте, удобству развертывания и большому количеству эмпирических доказательств обнаружения реальных уязвимостей программного обеспечения.

1. Классическая схема фаззинг-тестирования

С момента своего появления в начале 1990-х годов фаззинг оставался одним из наиболее широко применяемых методов обнаружения уязвимостей безопасности ПО. Целью фаззинг-тестирования является выполнение следующих частных задач:

- поиск программных дефектов;
- исследование уязвимостей методом изучения и эксплуатации ошибок;

¹⁷⁰ Осипова Наталья Сергеевна, сотрудник, Академия ФСО России, г. Орел, email: osipova_nc@mail.ru

¹⁷¹ «Эшелон», НПО. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения [текст] / НПО "Эшелон". — М.: Стандартинформ, 2006.

–получение информации о внутренней структуре, так как ошибки или иная реакция на фаззинг может раскрывать системную информацию;

–поиск ошибок в логике ПО. [2]

Классическая схема работы фаззера изображена на рисунке 1. Множество действий в классической схеме работы требует ручного анализа, что является трудоемкой задачей.

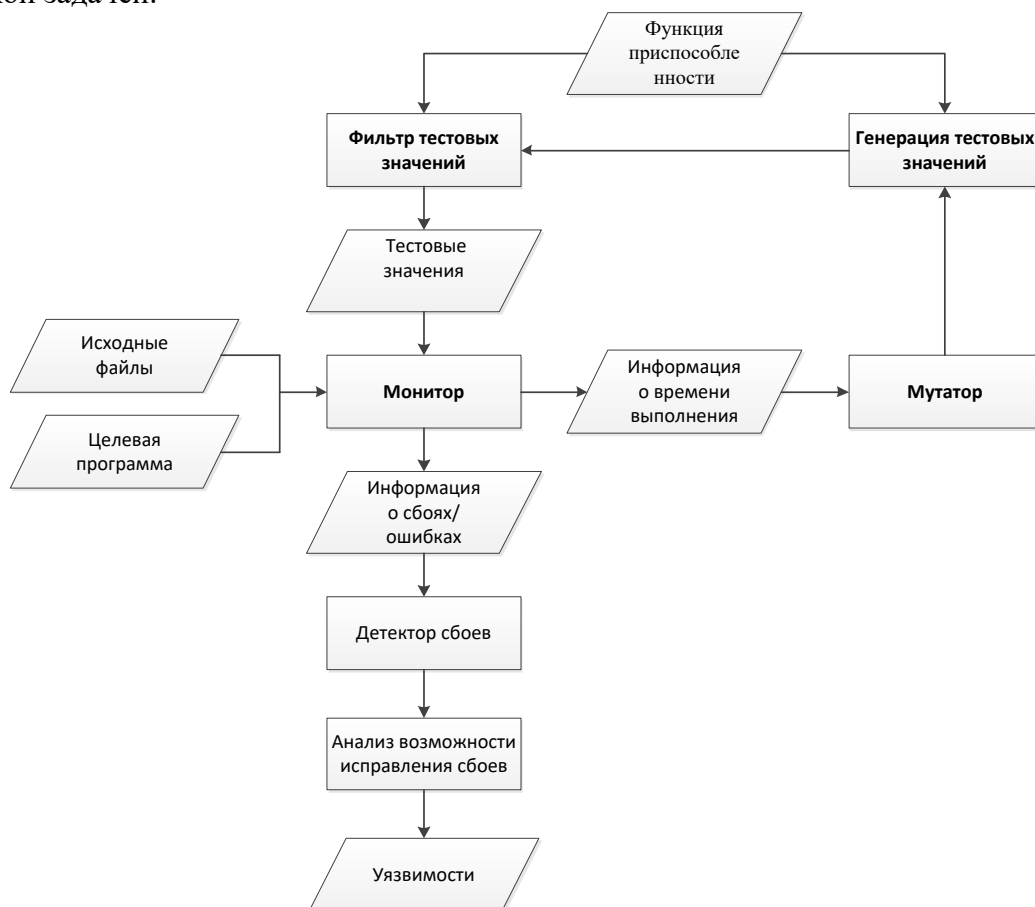


Рис.1. Рабочий процесс фаззинга

2. Существующие варианты применения методов машинного обучения в фаззинге

Задачи фаззинг-тестирования, которые могут быть решены методами МО:

– задачу классификации (для фильтрации тестовых наборов или выявленных сбоев);

– задача проверки формата входных данных;

– задача формирования набора размеченных данных для обучения с учителем.

В соответствии с задачами, решаемыми с помощью машинного обучения, его использование целесообразно на следующих этапах фаззинга:

1. Генерации исходного файла:

Исходный файл преобразуется во входные данные для фаззинга с помощью различных операций мутации. Качество входного и исходного файлов является важным фактором, влияющим на результат тестирования. С помощью методов МО могут быть изучены общие закономерности в исходных файлах, которые приводят к большому

покрытию кода, увеличению количества аварийных завершений программы и получению уникальных трасс выполнения в фаззинге, а также дает возможность генерировать больше исходных файлов с использованием полученных знаний с помощью генерационного, либо мутационного подходов. Данное направление исследовалось в работах [3-9].

2. Создания тестового набора:

Тестовый набор может быть сгенерирован путем изменения исходного файла, созданного на основе известных форматов входных файлов. Так как именно тестовый набор подается на вход тестируемой программе, он напрямую влияет на то, будет ли найдена ошибка. Следовательно, построение тестового набора с высоким уровнем покрытия кода или ориентированного на уязвимости может эффективно повысить обнаружение уязвимостей в фаззере. Данное направление исследовалось в работах [10-20].

3. Фильтрации тестового набора:

Цель фильтрации тестового набора – выбрать тот минимальный набор, который с большей вероятностью обнаружит новые пути или уязвимости в тестируемой программе. Входные данные могут быть проанализированы и классифицированы с помощью методов машинного обучения, чтобы определить, какие наборы следует использовать в дальнейшем для поиска уязвимостей безопасности. Данное направление исследовалось в работах [21-23].

4. Выбор оператора мутации:

Концепция операторов мутации в фаззинге основана на генетическом алгоритме. Оператор мутации в фаззинге включает такие операции, как добавление, изменение и удаление байтов. Различные мутации в разных местах кода могут иметь разную эффективность. Стратегия выбора оператора мутации заключается в достижении повышения эффективности фаззинга, например, увеличения покрытия кода или включения новых путей. Данное направление исследовалось в работах [24-29].

5. Расчета функции приспособленности:

В генетических алгоритмах функция приспособленности – вещественная или целочисленная функция одной или нескольких переменных, подлежащая оптимизации в результате работы генетического алгоритма, направляет эволюцию в сторону оптимального решения. Функция приспособленности относится к методу оценки, используемому для разграничения удовлетворительных и неудовлетворительных стандартов тестового набора в фаззере на основе генетического алгоритма.

В работе [30] предложена новая функция приспособленности, на основе генетического программирования, которая отличается от распространенного основного метода, основанного на покрытии кода.

6. Анализа дефектов:

Неотъемлемым свойством уязвимости является возможность ее использования злоумышленником. Результатом фаззинга ПО являются множество аварийных завершений работы, а также сообщений об ошибках, но лишь некоторые из них являются уязвимостями. Найти настоящие уязвимости в этом множестве – сложная задача специалиста, проводящего фаззинг.

В разработке ExploitMeter [31] используется алгоритм байесовского машинного обучения, чтобы делать первоначальные суждения о статических функциях, извлеченных из ПО. В разработке Exniffer [32] предлагается использование методов МО для автоматического определения более общих правил предсказания возможности использования аварийных завершений ПО. В работе [33] генерируются сжатые отпечатки пальцев для динамического выполнения отслеживания каждого входного набора данных, вызвавшего аварийное завершение программы, на основе анализа п-

граммов и хеширования функций. Затем отпечаток пальца подается в онлайн-классификатор для построения отличительной модели.

Заключение

Данное направление активно развивается зарубежными учеными, и количество работ по этой теме увеличивается с каждым днем. Данная область огромна и пока еще не полностью изучена и в ней содержится множество интересных перспективных направлений для исследований.

Дальнейшие исследования могут быть реализованы по следующим трем направлениям:

1. Создание общедоступных тестовых наборов данных: на данный момент, универсального общедоступного набора данных, который можно было бы использовать в качестве эталона в текущей области фаззинга, не существует. Качество тестового набора данных серьезно повлияет на производительность модели обнаружения уязвимостей.

2. Использование предварительной обработки данных, с целью извлечения полезной информации: МО создает модель классификации, изучая характеристики наборов данных. Выбор различных характеристик приведет к различной точности классификации и точности модели. В настоящее время технологии обработки естественного языка постоянно развиваются, поэтому следует рассмотреть возможность использования передовых технологий для извлечения полезной информации из данных, с целью последующего использования этой информации.

3. Выбор наиболее эффективных алгоритмов обучения для конкретных задач: для разных сценариев подходят разные методы МО, и разные конфигурации нейронной сети могут привести к разным результатам. Прежде всего, при выборе алгоритма следует использовать предварительно собранные характеристики на различных этапах фаззинга, а также преимущества и недостатки конкретных алгоритмов. Также необходимо изучить более сложные и подходящие модели нейронных сетей для конкретных задач фаззинга, с целью повышения эффективности фаззинга в конкретном рассматриваемом случае.

Литература

1. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5. С. 2-10.
2. Томилов И.О., Карманов И.Н., Звягинцева П.А., Грицкевич Е.В. Разработка методики применения фаззинга для анализа уязвимостей программного обеспечения // Электронный научный журнал: Системы управления, связи и безопасности. 2018. № 4.
3. Wang J, Chen B, Wei L, Liu Y. Skyfire: Data-Driven Seed Generation for Fuzzing. In: 2017 IEEE Symposium on Security and Privacy (SP). IEEE; 2017. p. 579–94;
4. She D, Pei K, Epstein D, Yang J, Ray B, Jana S. NEUZZ: Efficient Fuzzing with Neural Program Smoothing; IEEE Symposium on Security & Privacy; 2019, 89(46). p. 38;
5. Nichols N, Raugas M, Jasper R, Hilliard N. Faster Fuzzing: Reinitialization with Deep Neural Models. arXiv preprint arXiv:1711.02807; 2017Zalewski M 2016
6. Zalewski M. American fuzzy lop. 2016. [cited 2019 Jul 17]. Available from: <http://lcamtuf.coredump.cx/afl/>
7. Lv C, Ji S, Li Y, Zhou J, Chen J, Chen J. SmartSeed: Smart Seed Generation for Efficient Fuzzing; arXiv preprint arXiv:1807.02606; 2018.
8. Cheng L, Zhang Y, Zhang Y, Wu C, Li Z, Fu Y, et al. Optimizing seed inputs in fuzzing with machine learning. In: Proceedings of the 41st International Conference on Software Engineering: Companion Proceedings. IEEE Press, 2019. p. 244-5.

9. Wang Y, Wu Z, Wei Q, Wang Q. NeuFuzz: Efficient Fuzzing With Deep Neural Network. IEEE Access; 2019, 7 .p. 36340–52;
10. Godefroid P, Peleg H, Singh R. Learn&Fuzz: Machine learning for input fuzzing. In: 2017 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE; 2017. p. 50–9;
11. Fan R, Chang Y. Machine Learning for Black-Box Fuzzing of Network Protocols. In: International Conference on Information and Communications Security. 2017. p. 621–32.
12. Hu Z, Shi J, Huang Y, Xiong J, Bu X. Ganfuzz: A Gan-based industrial network protocol fuzzing framework. In: /Proceedings of the 15th ACM International Conference on Computing Frontiers. ACM; 2018. p. 138–45.
13. Cummins C, Petoumenos P, Murray A, Leather H. Compiler fuzzing through deep learning. In: Proceedings of the 27th ACM SIGSOFT International Symposium on Software Testing and Analysis. ACM, 2018: 95-105.
14. Sablotny M, Jensen BS, Johnson CW. Recurrent Neural Networks for Fuzz Testing Web Browsers. In: International Conference on Information Security and Cryptology; 2018. p. 354–70;
15. Nasrabadi MZ, Parsa S, Kalaei A. Format-aware Learn&Fuzz: Deep Test Data Generation for Efficient Fuzzing. arXiv Prepr arXiv:1812.09961; 2018 Dec 24;
16. She D, Pei K, Epstein D, Yang J, Ray B, Jana S. NEUZZ: Efficient Fuzzing with Neural Program Smoothing; IEEE Symposium on Security & Privacy; 2019, 89(46). p. 38
17. Paduraru C, Melemciuc M-C. An Automatic Test Data Generation Tool using Machine Learning. In: Proceedings of the 13th International Conference on Software Technologies. SCITEPRESS - Science and Technology Publications; 2018. p. 506–15.
18. Li Z, Zhao H, Shi J, Huang Y, Xiong J. An Intelligent Fuzzing Data Generation Method Based on Deep Adversarial Learning. IEEE Access. 2019b; 7. p. 49327–40.
19. Liu X, Li X, Prajapati R, Wu D. DeepFuzz: Automatic Generation of Syntax Valid C Programs for Fuzz Testing. In: Proceedings of the... AAAI Conference on Artificial Intelligence; 2019b;
20. Li Y, Ji S, Lv C, Chen Y, Chen J, Gu Q, et al. V-Fuzz: Vulnerability-Oriented Evolutionary Fuzzing. arXiv preprint arXiv:1901.01142. 2019a;
21. Gong W, Zhang G, Zhou X. Learn to Accelerate Identifying New Test Cases in Fuzzing. In: /International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, Cham; 2017. p. 298–307;
22. Rajpal M, Blum W, Singh R. Not all bytes are equal: Neural byte sieve for fuzzing; 2017 Nov 9; 1–10.
23. Karamcheti S, Mann G, Rosenberg D. Improving Grey-Box Fuzzing by Modeling Program Behavior. arXiv Prepr arXiv:1811.08973. 2018b
24. Becker S, Abdelnur H, State R, Engel T. An Autonomic Testing Framework for IPv6 Configuration Protocols. In: IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer, Berlin, Heidelberg, 2010. p. 65-76.
25. Fang K, Yan G. Emulation-Instrumented Fuzz Testing of 4G/LTE Android Mobile Devices Guided by Reinforcement Learning. In: European Symposium on Research in Computer Security. 2018. p. 20–40.
26. Böttinger K, Godefroid P, Singh R. Deep reinforcement fuzzing. In: 2018 IEEE Security and Privacy Workshops (SPW). IEEE, 2018. p. 116-122.
27. Drozd W, Wagner MD. FuzzerGym: A Competitive Framework for Fuzzing and Learning. arXiv preprint arXiv:1807.07490, 2018. Karamcheti et al. 2018a
28. Karamcheti S, Mann G, Rosenberg D. Adaptive Grey-Box Fuzz-Testing with Thompson Sampling. In: Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security. ACM; 2018a. p. 37–47.
29. Liu Xiao, Prajapati, Rupesh, Li Xiaoting WD. Reinforcement Compiler Fuzzing; 2019.
30. Sun X, Fu Y, Dong Y, Liu Z, Zhang Y. Improving Fitness Function for Language Fuzzing with PCFG Model. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE; 2018. p. 655–60;
31. Yan G, Lu J, Shu Z, Kucuk Y. ExploitMeter: Combining Fuzzing with Machine Learning for Automated Evaluation of Software Exploitability. In: 2017 IEEE Symposium on Privacy-Aware Computing (PAC). IEEE; 2017 .p. 164-75;

32.Tripathi S, Grieco G, Rawat S. Exniffer: Learning to Prioritize Crashes by Assessing the Exploitability from Memory Dump. In: 2017 24th Asia-Pacific Software Engineering Conference (APSEC). IEEE; 2017 .p. 239-48;

33.Zhang G, Zhou X, Luo Y, Wu X, Min E. PTfuzz: Guided Fuzzing With Processor Trace Feedback. IEEE Access; 2018, 6 .p. 37302–13;

Научный руководитель: Козачок Александр Васильевич – д-р техн. наук, сотрудник, Академия ФСО России, г. Орел, email: a.kozachok@academ.msk.rsnet.ru

Applying machine learning methods when conducting fuzzing testing

Osipova N.S.¹⁷²

Annotation. Nowadays, most of the detected software bugs related to remote code execution and privilege escalation are found using fuzzing. Integration of fuzzing testing into the code development process allows you to identify errors and vulnerabilities at an early stage. Due to the existing limitations of program analysis methods, fuzzing testing may not be effective enough. This article discusses the existing approaches to the application of machine learning methods at different stages of fuzzing, and also suggests topical directions for further research.

Keywords: software defects, fuzzing testing, machine learning.

¹⁷² Osipova Natalya Sergeevna, employee, Academy of the Federal Guard Service of the Russian Federation, Orel, email: osipova_nc@mail.ru

Применение алгоритма Саймона для поиска линейных структур булевых отображений Поляков М.В.¹⁷³

Аннотация. В данной статье предлагается модификация квантового алгоритма Саймона для эффективного поиска линейных структур булевых операторов, составляющих основу итерационных симметричных алгоритмов шифрования. Применение подобной модификации алгоритма позволяет проводить квантовые предвычисления для проведения разностного криптоанализа.

Ключевые слова: квантовые вычисления, задача Саймона, квантовый криптоанализ, разностная атака, линейные структуры булевых функций.

Введение

Квантовый компьютер представляет из себя мощное вычислительное устройство, позволяющее решать ряд задач намного эффективнее, чем любой самый мощный классический компьютер. Одной из основных задач квантовых вычислений является синтез алгоритмов для различных вычислительно сложных задач, дающих экспоненциальное ускорение относительно сложности решения. Здесь под сложностью понимается время работы алгоритма, объем предвычисленных данных или количество обращений к некоторому оракулу.

Классическим примером здесь является алгоритм Шора [1], позволяющий решать задачи дискретного логарифмирования и дискретной факторизации с полиномиальной сложностью относительно длины битовой записи числа. С другой стороны, всем известный алгоритм Гровера [2], осуществляющий поиск в неотсортированном массиве, дает приращение в корень раз относительно размера массива, т.е. $O(\sqrt{n})$ вместо $O(n)$ в классическом случае. Однако, алгоритм Гровера представляет наибольший интерес в вопросах криптоанализа симметричных криптографических примитивов, т.к. позволяет снизить сложность атаки полным перебором.

Разностный криптоанализ, предложенный в 1990 г для атаки на DES-подобные алгоритмы шифрования [3], остается одним из самых известных и универсальных методов криптоанализа блочных и поточных алгоритмов шифрования. Применимость разностного метода напрямую связана с внутренней структурой преобразований криптографического примитива. К таковым, в частности, относятся *линейные структуры булевых функций*. Линейные структуры преобразований (блочных алгоритмов шифрования) рассматривались в работах [4-7] и др. Наличие нетривиальной линейной подструктуры является уязвимостью шифрсистемы и позволяет применять разностный криптоанализ или строить факторсистемы для данной системы и применять метод гомоморфизмов [4].

Разностным атакам с применением квантового компьютера также посвящен ряд работ [см. 8-10], в которых имеется общий подход – построить матрицу разностных соотношений, с ее помощью вычислить некоторые биты ключа и на битах, оставшихся неизвестными, запустить квантовый поиск с помощью алгоритма Гровера. В данной работе предлагается модификация алгоритма Саймона [11] для поиска линейных

¹⁷³ Поляков Михаил Вадимович, аспирант кафедры ИУ-8 МГТУ им. Н.Э. Баумана, Москва, m.polyakov@bmstu.ru

структур булевых функций на квантовом компьютере, что позволяет эффективнее строить матрицы разностных соотношений.

Алгоритм Саймона

Пусть имеется булево отображение $F: \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$, про которое известно, что существуют два таких набора x и x' , при чем $x' = x \oplus a$, что $F(x) = F(x')$. Требуется найти вектор $a \in \mathbb{Z}_2^n$. В классическом случае для решения этой задачи потребуется $O(2^{n/2})$ обращений к функции F . Квантовый алгоритм Саймона позволяет решить эту задачу за $O(n)$ обращений.

1. Инициализируется два n -кубитных регистра состояниями $|0\rangle^{\otimes n}|0\rangle^{\otimes n}$. После чего к одному из них применяется квантовое преобразование Адамара:

$$|0\rangle^{\otimes n}|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} |x\rangle|0\rangle \quad (1)$$

2. Далее следует обращение к квантовому оракулу («черному ящику» или оракулу Дойча [12])

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} |x\rangle|F(x)\rangle \quad (2)$$

3. Проводится измерение состояния второго регистра. При этом состояние первого коллапсирует в следующее:

$$\frac{1}{\sqrt{2}} (|z\rangle + |z \oplus a\rangle) \quad (3)$$

4. И к нему же применяется преобразование Адамара:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \mathbb{Z}_2^n} ((-1)^{\langle y, z \rangle} + (-1)^{\langle y, a \rangle}) |y\rangle \quad (4)$$

Если $\langle y, a \rangle = 0$, то вся сумма равняется 0. Поэтому в (4) должны остаться такие $y \in \mathbb{Z}_2^n$, что $\langle y, a \rangle \neq 0$. После $O(n)$ повторений шагов 1-4 получится система из n линейно независимых уравнений вида $\langle y, a \rangle = 0$, решение которой даст искомый вектор a .

Линейные подструктуры булевых функций и модификация алгоритма Саймона

Пусть $F: \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ – некоторое булево отображение. Известно, что любое такое отображение можно задать с помощью его n координатных функций $(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$, где $f_i(x_1, \dots, x_n): \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ – булева функция от n переменных.

Определение 1. Будем говорить, что булево отображение F обладает линейной структурой, если для любого $x \in \mathbb{Z}_2^n$ $F(x) + F(x + a) = \delta$, где $a \neq 0$. Пару (a, δ) назовем *линейной структурой* отображения F .

Как уже говорилось во введении, поиск линейных подструктур раундовых отображений представляет огромный интерес для криптоанализа, т.к. наличие нетривиальных линейных структур позволяет применять в т.ч. разностный криптоанализ.

Пусть отображение $F: \mathbb{Z}_2^n \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ – функция шифрования некоторого блочного алгоритма, где $\mathbb{Z}_2^n$ – алфавит открытого и шифрованного текстов, а $\mathbb{Z}_2^m$ – ключевое множество. Без ограничения общности будем считать, что F задает r -раундовую функцию шифрования, т.е.

$$F = F^{(r)} \circ \dots \circ F^{(1)} \quad (5)$$

В основе разностного криптоанализа лежит поиск таких пар (a, δ) , называемыми *разностными парами*, с максимальной вероятностью для раундовой функции $F^{(i)}$:

$$p_{(a, \delta)}^{(F)} = \frac{1}{2^{n+m}} |\{(x, k) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^m : F_k^{(i)}(x \oplus a) \oplus F_k^{(i)}(x) = \delta\}| \quad (6)$$

Нетрудно заметить, что определение разностного соотношения полностью совпадает с определением линейной структуры булевого отображения.

Для эффективного нахождения линейных структур булевых отображений предлагается модифицировать алгоритм Саймона. Схема выполнения модифицированного алгоритма представлена на рисунке (рис. 1)

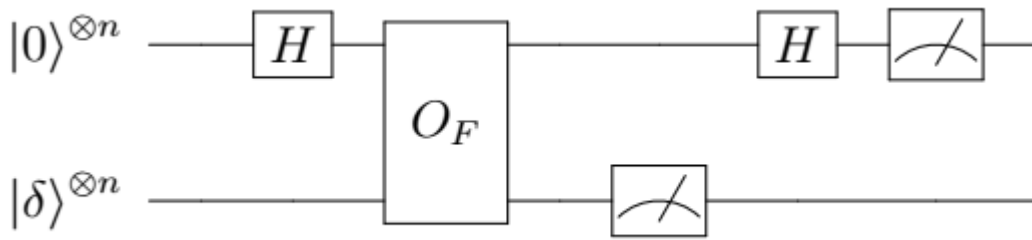


Рис. 1. Схема выполнения модифицированного алгоритма Саймона.

Теорема 1. Представленная на Рисунке 1 схема позволяет корректно находить линейные структуры булевых отображений.

Доказательство. Рассмотрим схему выполнения алгоритма и распишем все преобразования.

1. Подготавливаем начальное состояние $\varphi_1 = |0\rangle^{\otimes n} |\delta\rangle^{\otimes n}$. При этом $\delta \neq 0$.
2. Применяя к первому регистру преобразование Адамара, получаем состояние

$$\varphi_2 = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} |x\rangle |\delta\rangle \quad (7)$$

3. Применяем к состоянию φ_2 оракул Дойча:

$$O_F(\varphi_2) = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} |x\rangle |\delta \oplus F(x)\rangle \quad (8)$$

4. Измеряем состояние второго регистра, при этом первый коллапсирует в состояние

$$\varphi_3 = \frac{1}{\sqrt{2}} (|z\rangle + |z \oplus a \oplus \delta\rangle) \quad (9)$$

5. Применяем к первому регистру преобразование Адамара:

$$H(\varphi_3) = \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \mathbb{Z}_2^n} ((-1)^{\langle y, z \rangle} + (-1)^{\langle y, z \oplus a \oplus \delta \rangle}) |y\rangle \quad (10)$$

6. Преобразуем получившееся выражение

$$\begin{aligned} \langle z, y \rangle &= \langle y, z \oplus a \oplus \delta \rangle \\ \langle z, y \rangle &= \langle y, z \rangle \oplus \langle y, a \oplus \delta \rangle \\ \langle y \oplus \delta, a \rangle &= 0 \pmod{2} \end{aligned} \quad (11)$$

Выполняя по крайней мере $\mathcal{O}(n)$ раз шаги 1-5 мы получаем систему из n линейно независимых уравнений, решая которую или находим a или доказываем, что такой линейной структуры у отображения F нет.

Теорема 2. Полученная модификация алгоритма Саймона позволяет находить линейную структуру (a, δ) для отображения F со сложностью $\mathcal{O}(n)$ обращений к оракулу $\mathcal{O}_F$.

Доказательство. Доказательство следует непосредственно из доказательства теоремы 1.

Выводы

В данной работе рассмотрена задача поиска линейных структур булевых отображений, которые активно используются при построении блочных алгоритмов шифрования. Показано, что при незначительной модификации квантового алгоритма Саймона, можно получить экспоненциальное ускорение по сложности решения задачи относительно числа обращений к оракулу, реализующему отображение F . Предложенную модификацию целесообразно использовать при проведении разностного криптоанализа блочных алгоритмов шифрования.

Литература

1. Shor P.W. Algorithms for quantum computing: discrete factoring and factoring. // Proceedings 35th annual symposium on foundation of computer science, 1994, IEEE Comput.Soc.Press: pp 124-134;
2. Grover L.K. A fast quantum mechanical algorithm for database search. // Proceedings, 28th Annual ACM Symposium on the Theory of Computing, 1996, p. 212;
3. E. Biham, A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. // Advances in Cryptology — CRYPTO '90, 1990, Springer-Verlag. pp. 2-21;
4. Chaum D., Evertse J. H. Cryptanalysis of DES with a reduced number of rounds sequences: of linear factors in block ciphers // CRYPTO'85 // Lect. Notes Comput. Sci. – 1986. – V. 218. – pp. 192-211;
5. Б. А. Погорелов, М. А. Пудовкина. Факторструктуры преобразований, Матем. вопр. криптогр., 3:3 (2012), 81-104;
6. Пудовкина М. А. Линейные структуры групп подстановок над конечным модулем // Прикладная дискретная математика. — Томск: ТГУ, 2008. – Т. 1. – С. 25-28;
7. А. А. Городилова. От криптоанализа шифра к криптографическому свойству булевой функции, ПДМ, 2016, № 3(33), С 16-44;
8. Zhou, Q., Lu, S., Zhang, Z. et al. Quantum differential cryptanalysis. // Quantum Inf Process 14, 2015, pp. 2101-2109;
9. M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia. Quantum Differential and Linear Cryptanalysis. // IACR Transactions on Symmetric Cryptology, 2016, pp.71-94;
10. Li H., Yang L. Quantum Differential Cryptanalysis to the Block Ciphers. // Applications and Techniques in Information Security. Communications in Computer and Information Science, 2015, vol 557. Springer, Berlin, Heidelberg;
11. D. R. Simon. On the power of quantum computation. // SIAM J. Comput. 26, 1997, pp. 1474-1483;
12. D. Deutsch, R. Jozsa. Rapid solutions of problems by quantum computation. // Proceedings of the Royal Society of London A. 439 (1907), 1992, pp. 553-558.

Научный руководитель: Пудовкина Марина Александровна, д.ф.-м.н., профессор кафедры ИУ-8 МГТУ им. Н. Э. Баумана, maricar.go@mail.ru.

On the usage of Simon's algorithm for finding linear structure of vectorial Boolean functions

Polyakov M.V.¹⁷⁴

Abstract. *Simon's algorithm is well known tool for solving hidden shift problem. In terms of vectorial Boolean functions such shift is also called linear structure of a function. Finding such nontrivial structure is widely known to be computationally hard problem but also useful for differential cryptanalysis. In this paper adaptation of Simon's algorithm is suggested for solving hidden shift problem for vectorial Boolean functions.*

Keywords: *quantum computations, Simon's problem, quantum cryptanalysis, differential cryptanalysis, linear structure of a Boolean function.*

¹⁷⁴ Mikhail Polyakov, post-graduate student, Bauman Moscow State Technical University, Moscow, m.polyakov@bmstu.ru

Подсистема стегоанализа цифровых изображений на основе сверточной нейронной сети

Проскурин А.А.¹⁷⁵, Яндашевская Э.А.¹⁷⁶

Аннотация. В настоящей работе представлен вариант реализации подсистемы стегоанализа цифровых изображений, циркулирующих в информационной системе. Данная подсистема расширяет функциональность существующих систем обнаружения/предотвращения вторжений с точки зрения обнаружения скрытых каналов, применяемых в компьютерных атаках. В представленном варианте предложена и реализована параметрическая модель сверточной нейронной сети для обнаружения полезной нагрузки в цифровых изображениях, выполненных рядом распознанных в реальных атаках алгоритмах стеговложений. Разработана программная реализация модульного генератора обучающей выборки (датасета), поддерживающего эти алгоритмы. Осуществлена экспериментальная оценка точности. Полученные результаты исследования рассматриваются в области информационной безопасности.

Ключевые слова: защита информации, скрытый канал передачи информации, стеганографический контейнер, система обнаружения и предотвращения компьютерных атак.

Введение

За период 2019-20 годов компании, специализирующиеся на анализе инцидентов информационной безопасности исследовали и провели технический анализ ряда специфических компьютерных атак, направленных, в первую очередь, на информационные инфраструктуры промышленных предприятий и коммерческих организаций. Особенностью этих атак является использование на одном из этапов развития вектора атаки скрытых стеганографических каналов (например, [1-3]), базирующихся на цифровых изображениях (ЦИ), размещенных на легитимных публичных хостингах.

Так в [4, 5] приведен подробный технический анализ варианта этой же атаки, связанной с распространением трояна Ursnif. Втором распространения атаки является организация запросов к публичным хостингам ЦИ, таких как imgur.com и imgbox.com (рассмотрены в [4]) или postimg.cc (рассмотрен в [5]) с целью получения стегоконтейнеров, представленных легитимными ЦИ. В качестве стегоконтейнера используется ЦИ формата PNG. Стеговложение выполняется программой с открытым исходным кодом Invoke-PSImage [6], которая, получая на вход сценарий PowerShell, кодирует его байты в пиксели PNG файла, используя модификацию метода LSB. В зависимости от варианта атаки такие ЦИ содержали, либо обфурцированный скрипт PowerShell, реализующий дальнейшее развитие вектора атаки, либо непосредственно вредоносную полезную нагрузку.

Высокий процент успешных атак, выполненных на основе представленных примеров, показывает, что наряду с такими факторами, как социальная инженерия, их реализации способствовало наличие скрытого канала передачи информации [7, 8].

Поскольку системы защиты атакуемых предприятий и организаций, основанные IDPS/DLP системах с традиционными для них контейнерным и сигнатурным видами анализа циркулирующей информации, не обнаруживают стегоконтейнеры ЦИ, относя канал их получения к легитимным каналам информационной системы, это делает задачу

¹⁷⁵ Проскурин Александр Александрович, к.т.н., доцент, Академия ФСО России, г. Орел, iakleshnya@gmail.com

¹⁷⁶ Яндашевская Элина Андреевна, сотрудник, Академия ФСО России, г. Орел, elenayanda@yandex.ru

их обнаружения актуальной.

Многоэтапная реализация существующей компьютерной атаки и противоборствующие ей функциональные возможности подсистем защиты представлены на рисунке 1.

Решением этой проблемы может быть расширение функциональности IDPS/DLP систем [9], включение в них модуля стегоанализа ЦИ с соответствующим перехватчиком, обеспечивающего решение задачи распознавания ЦИ – потенциальных стегоконтейнеров (рис. 2). При этом важной исследовательской задачей является выбор метода распознавания, обеспечивающего оптимальную точность распознавания при низких временных и ресурсных издержках. Дополнительным условием является достаточная гибкость метода, позволяющая подстраиваться под модификации алгоритмов встраивания, используемых в реальных компьютерных атаках.

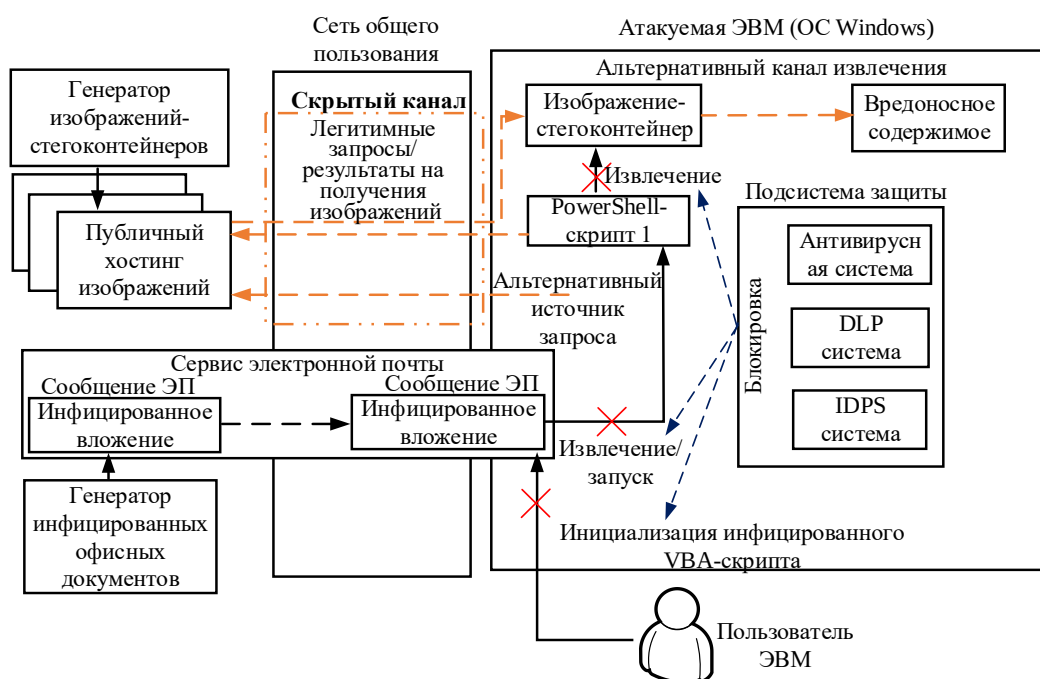


Рис. 1. Архитектура комбинированной IDPS/DLP системы с дополнительным модулем стегоанализа ЦИ

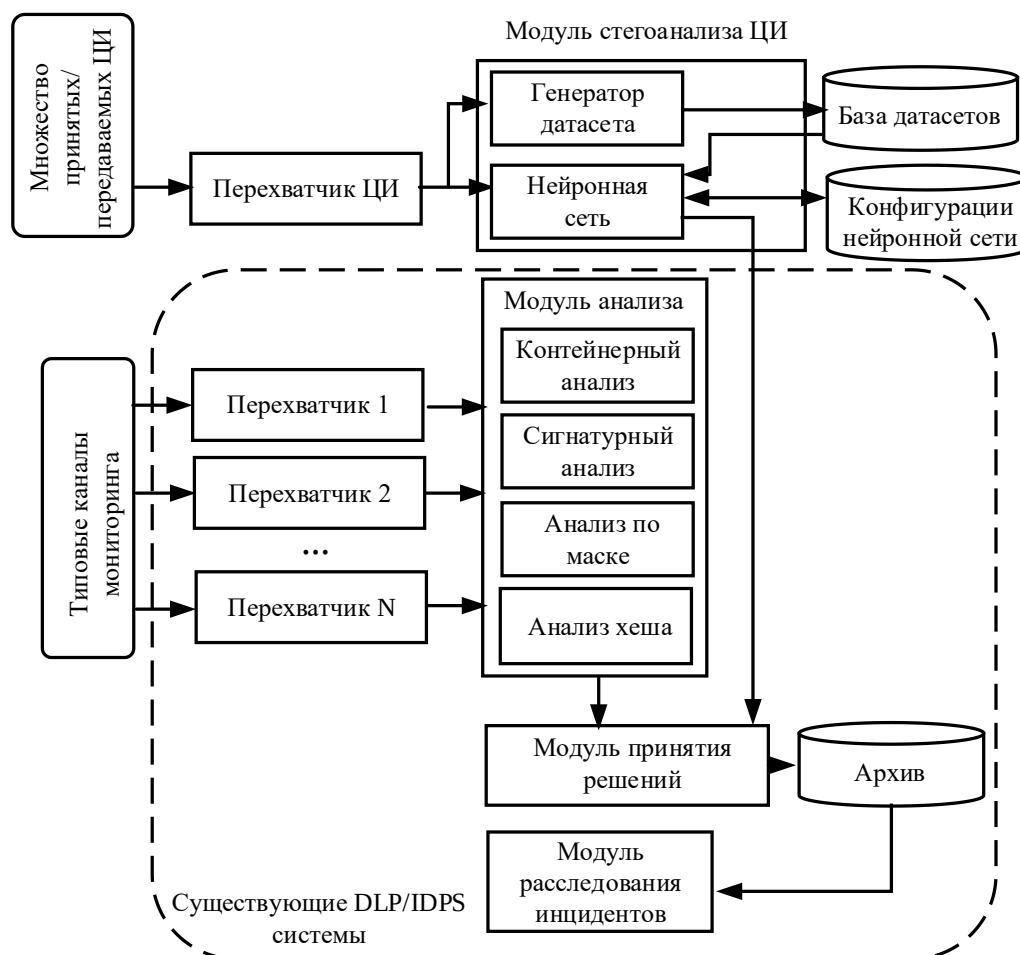


Рис. 2. Архитектура комбинированной IDPS/DLP системы с дополнительным модулем стегоанализа ЦИ

Вариант модуля стегоанализа цифровых изображений на основе сверточной нейронной сети

В исследовании в качестве основы модуля стегоанализа ЦИ предлагается использование варианта сверточной нейронной сети (СНС) [10]. Обоснование такого выбора и достоинства ее применения представлены в работе автора [11]. Структура разработанной СНС в общем случае соответствует представленной в [12] архитектуре сверточных сетей и представлена следующими типами слоев: сверточные слои; слои подвыборки (pooling); полносвязные слои.

Базовая функция сверточного слоя и слоя подвыборки уменьшение ядра - матрицы весов. Их параметрами являются: f (filters count) – количество фильтров в слое; K (kernel size) – размер (высота и ширина) ядра; s (stride) – шаг свёртки (количество пикселей, на которое перемещается матрица фильтра по входному изображению); p (padding) – дополнения нулями (количество пикселей, которые добавляются с каждого края изображения). Перемещение ядра над пикселями ЦИ выполняется перемножение и последующее суммирование его весов и значение пикселей, над которыми находится ядро. Эта функция именуется двумерная свертка. Ее результатом для последующего сверточного слоя новое ядро меньшего размера. Сверточные слои и слои подвыборки используются для предварительной обработки ЦИ. В таблице 1 представлены значения параметров сверточных слоев и слоев подвыборки разработанной СНС.

Таблица 1

Значения параметров сверточных слоев и слоев подвыборки разработанной СНС

Слой	Значение f (in/out)	Размер K	Значение s	Значение p
Сверточный слой 1	3/8	5	1	2
Сверточный слой 2	8/16	5	1	2
Сверточный слой 3	16/64	5	1	2
Слой подвыборки 1		5	4	2
Слой подвыборки 2		5	4	2

Полносвязный слой реализует вариант нелинейной функции, которая, проверяя комбинации входных данных реализуют бинарную (Cover/Stego) классификацию ЦИ. В разработанной СНС реализовано 5 полносвязных слоев, редуцирующих значения f (in/out) с 4096/2048 до 128/2, где 2 – результат решения задачи бинарной классификации.

Важной задачей при разработке СНС явилась задача выбора обучающей выборки – датасета. Так, в [13] предлагается повысить эффективность и работоспособность СНС за счет деления датасета обучения на две выборки: обучающая и валидационная, последняя из которых используется в итерационном алгоритме проверки чувствительности СНС к параметрам выборки.

Обучение СНС выполнялось на массиве из 35000 ЦИ, полученных из публичного хостинга imgur.com. На базе 15000 из них, с использованием алгоритма Invoke-PSImage, были реализованы PNG-стегоконтейнеры с различной полезной нагрузкой. Тестирование обученной СНС производилось на 2000 ЦИ, из которых 1000 были представлены вариантами Invoke-PSImage стегоконтейнеров. И в процессе обучения, и в процессе тестирования размер батча (подмножества ЦИ, подаваемого на вход СНС) был равен 64. На рисунке 4 представлены графики точности распознавания (ассигасу) и функции потерь для этапов обучения и тестирования СНС.

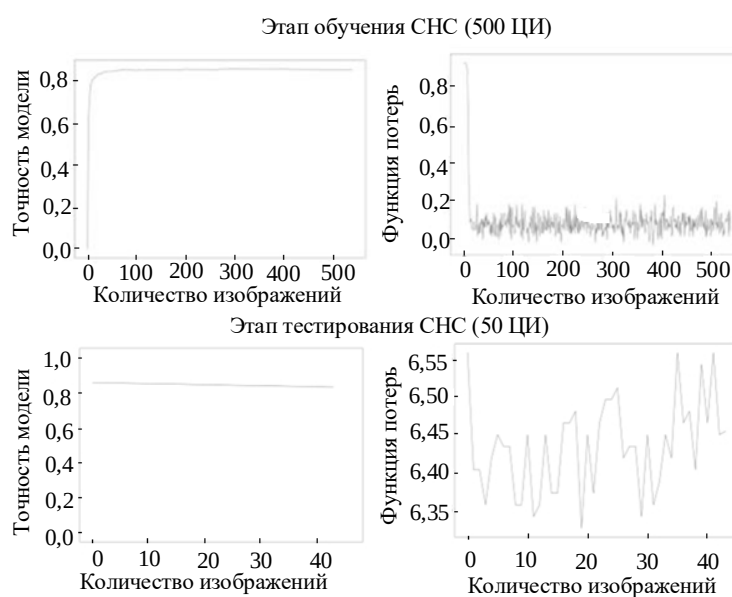


Рис. 5 Результаты экспериментальной оценки разработанной СНС

Заключение

В статье на примерах зафиксированных компьютерных атак с использованием скрытых стеганографических каналов предложен подход по расширению функциональности современных систем обнаружения и предотвращения вторжений за счет использования модуля стегоанализа цифровых изображений, циркулирующих в защищаемой информационной системе. В качестве базы такого модуля обоснован выбор аппарата сверточных нейронных сетей. Предложен вариант сверточной нейронной сети,

а также модульный генератор датасета для нее, обеспечивающий подключение распознанных в реальных атаках алгоритмов стеговложений. На основе сформированных обучающей и тестовой выборок цифровых изображений, полученных с используемого в компьютерных атаках публичного хостинга, проведен эксперимент, демонстрирующий приемлемую степень распознавания. Направление дальнейших исследований, является совершенствования предложенного стегоанализатора путем комбинирования методов статистической бинарной классификации и сверточных нейронных сетей с целью сокращения временных и ресурсных затрат, связанных с этапом обучения сети.

Литература

1. Макаренко С. И. Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии // Вопросы кибербезопасности. -2014. -№ 2(3). -С. 24-32.
2. Сивачев А.В., Прохожев Н.Н., Михайличенко О.В., Башмаков Д.А. Эффективность стеганоанализа на основе методов машинного обучения // Вопросы кибербезопасности. 2017. № 2 (20). С. 53-60.
3. Evsutin O., Shelupanov A., Kokurina A., Shumskaya O., Kozachok A. Approach to increase in efficiency of information embedding into a phase spectrum of the discrete fourier transformation due to minimization of quantity of changeable frequency coefficients. In: CEUR Workshop Proceedings. conference proceedings. 2017. P. 54-58.
4. Копейцев В. Стеганография в атаках на промышленные предприятия (обновлено) // Лаборатория Касперского. 2020. URL: <https://ics-cert.kaspersky.ru/reports/2020/06/17/steganography-in-attacks-on-industrial-enterprises/> (дата обращения: 21.01.2021).
5. Pierluigi P. Ursnif: Long Live the Steganography and AtomBombing! // Security affairs. 2019. URL: <https://securityaffairs.co/wordpress/80777/malware/ursnif-steganography-atombombing.html> (дата обращения: 21.01.2021).
6. InvokePSImage source code [Электронный ресурс]. URL: <https://github.com/peewpw/Invoke-PSImage> (дата обращения: 15.10.2020).
7. Колесников А. А., Яндашевская Э.А. Теоретико-информационный подход к моделированию распределенной стенографической системы с пассивным противником // Сборник научных статей научно-технического журнала «Системы управления и информационные технологии». Воронеж. 2020. № 3 (81). С. 19-23. (Рекомендован ВАК).
8. Яндашевская Э.А. Подход к тестированию на проникновение в информационные сервисы сети RSNNet по скрытым каналам, основанным на методах стеганографического преобразования информации // Научно-технический журнал «I-Methods». Санкт-Петербург: ООО «Институт ИНТЕХ». 2020. Т. 12, №4. С. 1-14.
9. Белова А.Л., Бородавкин Д.А. Сравнительный анализ систем обнаружения вторжений // Актуальные проблемы авиации и космонавтики. 2016. №1. С.742-744.
10. Саймон Х. Нейронные сети. Полный курс. М.: Вильямс. 2019. 1104 с.
11. Полунин А.А., Яндашевская Э.А. Использование аппарата свёрточных нейронных сетей для стегоанализа цифровых изображений // Труды ИСП РАН. 2020. №32(4). С.155–164. DOI: 10.15514/ISPRAS-2020-32(4)-11.
12. Qian Y., Dong J., Wang W., Tan T. Deep learning for steganalysis via convolutional neural networks. // IS&T/SPIE Electronic Imaging. 2015. DOI: 10.1117/12.2083479.
13. Moiseev O.V., Yandashevskaya E.A. To the question of sensitivity checking of the conventional neural network for digital images stegoanalysis to the sampling parameters at the learning stage // MIP2021'SCT: Proceedings of the XXVI-th International Open Science / Editor in Chief Dr. Sci., Prof. O.Ja. Kravets. Yelm, WA, USA: Science Book Publishing House, 2021, pp 59-63.

Subsystem for steganalysis of digital images based on a convolutional neural network

Proskurin A.A.¹⁷⁷, Yandashevskaya E.A.¹⁷⁸

Abstract. This paper presents a variant of the implementation of the subsystem for steganalysis of digital images circulating in the information system. This subsystem expands the functionality of existing intrusion detection / prevention systems in terms of detecting covert channels used in computer attacks. In the presented version, a parametric model of a convolutional neural network is proposed and implemented for detecting payload in digital images, performed by a number of steg-nesting algorithms recognized in real attacks. A software implementation of a modular generator of a training sample (dataset) that supports these algorithms has been developed. An experimental assessment of the accuracy has been carried out. The obtained research results are considered in the field of information security.

Keywords: information protection, covert information transmission channel, steganographic container, a system for detecting and preventing computer attacks.

УДК 004.056:336(045)

¹⁷⁷ Proskurin Alexander Alexandrovich, Ph.D., Associate Professor, the Academy of the Federal Guard Service of Russia, Orel, iakleshnya@gmail.com

¹⁷⁸ Yandashevskaya Elina Andreevna, employee, the Academy of the Federal Guard Service of Russia, Orel, elenayanda@yandex.ru

Оценка риска нарушения кибербезопасности в коммерческом банке (на примере атак на банкоматы “Brute force” и “Black box”)

Ревенков П.В.¹⁷⁹, Бердюгин А.А.¹⁸⁰, Макеев П.В.¹⁸¹

Аннотация. Прогресс цифровой трансформации общества и, в частности, финансово-экономических систем приводит к усложнению проблем информационной безопасности конкурирующих субъектов. Делая основной упор на научных исследованиях, можно достичь успеха в этих вопросах. Цель исследования – повышение уровня защищённости банковского обслуживания физических и юридических лиц в соответствии с рекомендациями стандартов по информационной безопасности, посредством анализа риска нарушения информационной безопасности в банковских технологиях (на примере атак “Brute force” и “Black box”). Приведён ряд стандартов для осуществления эффективного управления информационной безопасностью на предприятии. Количественно показано преимущество методов социальной инженерии над методом перебора (“Brute force”) PIN-кодов. Проанализированы временные характеристики совершения атак типа “Black box”. Предложен метод повышения эффективности реагирования и защиты банкоматов от атак типа “Black box”.

Ключевые слова: стандарты, PIN-код, кибератаки, АТМ, диспенсер, киберпреступник.

Введение

За прошедшие десятилетия условия деятельности коммерческих банков всех стран мира претерпели существенные изменения. Факторы научно-технического прогресса привели как к появлению новых финансовых инструментов и возможностей банков [1], так и к необходимости управления совершенно новыми видами рисков [2-7] в соответствии с новыми стандартами [8], о которых пойдёт речь в статье.

Серия международных стандартов ISO/IEC 27000 включает стандарты по информационной безопасности, опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC). Их набор изображён на рис. 1.

¹⁷⁹ Ревенков Павел Владимирович, доктор экономических наук, доцент, профессор Департамента информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Россия. E-mail: pavel.revenkov@mail.ru, orcid.org/0000-0002-0354-0665

¹⁸⁰ Бердюгин Александр Александрович, младший научный сотрудник Департамента информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Россия. E-mail: brdgn@bk.ru, orcid.org/0000-0003-2301-1776

¹⁸¹ Макеев Павел Владимирович, магистрант Факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Россия. E-mail: paulmakeev@gmail.com, orcid.org/0000-0003-0031-5419



Рис. 1. Структура нормативов и стандартов серии ISO/IEC 270xx¹⁸²

¹⁸² Воронин А.С. Национальная платежная система. Бизнес-энциклопедия. М.: КНОРУС: ЦИПСИР, 2013. – 424 с.

Кроме этого, комплекс документов по стандартизации Центрального банка Российской Федерации содержит единый подход к обеспечению информационной безопасности организаций банковской системы (ИББС) и рекомендации по стандартизации (РС) с учётом требований российского законодательства [9].

Решение большинства проблем и задач кибербезопасности должно иметь научную базу. При выполнении коллективной научно-исследовательской и/или опытно-конструкторской работы стандарты и нормативно-правовые акты, описанные в техническом задании (ТЗ, техзадание) к выполняемой работе, для исполнителей носят не рекомендательный, а обязательный ко внимательному прочтению характер. В противном случае может сложиться ситуация, описанная в басне И.А. Крылова «Квартет».

Атаки на банкоматы: “Brute force” и социальная инженерия

По статистике ФинЦЕРТ Банка России, основная причиной реализации кибератак в банковской сфере (согласно данным формы отчётности 0403203) – дезинформирование (97% в 2018 г. и 92% в 2017 г.). Для юридических лиц этот показатель составил 39%¹⁸³.

PIN-код банковской карты содержит 4 цифры от 0 до 9. Игнорируя реальную ситуацию, когда после трёх неправильных наборов PIN-кода банкомат блокирует или «проглатывает» карточку, а также учитывая, что перебор всех возможных комбинаций PIN-кода (“Brute force”) по технической части не сложнее приёмов социальной инженерии, определим время, необходимое для перебора.

Количество возможных комбинаций PIN-кода $N = 10^4 - 10 = 9990$ (совместное появление десяти цифр на 4 позициях за исключением номеров с четырьмя одинаковыми цифрами). На любой попытке вероятность угадывания киберпреступником PIN-кода

$P_N = \frac{1}{N}$ [10, 11] (доказательство опускается для экономии места в докладе).

Математическое ожидание количества попыток – произведение вероятности и суммы первых N членов арифметической прогрессии

$$M_N = \frac{1}{N} \cdot 1 + \frac{1}{N} \cdot 2 + \dots + \frac{1}{N} \cdot N = \frac{1}{N} \cdot (1 + 2 + \dots + N) = \frac{1}{N} \cdot \frac{(N+1) \cdot N}{2} = \frac{N+1}{2}. \quad (1)$$

Пусть продолжительность попытки подбора 5 сек. $= \frac{5}{60 \cdot 60}$ час. $= \frac{1}{720}$ час. Тогда математическое ожидание продолжительности подбора PIN-кода $\frac{9991}{2 \cdot 720} \approx 6,9$ час. Этого

времени достаточно, чтобы сотрудники банка заподозрили неладное и вызвали полицию.

Приёмы социальной инженерии ограничиваются минутами, что делает очевидным преимущество их умелого применения для киберпреступника [12, 13]. На сегодняшний день при эксплуатации новой SIM-карты перечень контактов пополняется только справочными номерами (Service Dialing Numbers – SDN) оператора мобильной связи (часть из них сразу удаляется самим абонентом). Предложение авторов состоит в том, чтобы SDN содержали номера некоторых кредитных организаций и Банка России. Это позволит:

- заинтересовать пользователя (поняв, зачем нужны номера кредитных организаций, он сам добавит нужные);
- определять входящий номер телефона (банк или жулик);
- побудить клиента самостоятельно перезвонить в банк, если ему позвонили «из службы безопасности Вашего банка».

Таким образом, организуется сотрудничество: сотовые операторы прописывают в SDN SIM-карты телефоны известных банков, банки рекламируют этих операторов на своих

¹⁸³ Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов. М.: Центральный банк Российской Федерации, 2019, 26 с. URL: https://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения 20.02.2021).

пластиковых картах, клиенты повышают свою грамотность и безопасность.

Кибератаки типа “Black box” на банкоматы

Значительной угрозой для банковской сферы являются аппаратно-программные комплексы, предназначенные для хищения денежных средств из банкоматов, которые называются “Black box” – аппаратура со специальным программным обеспечением (ПО), подключающаяся к диспенсеру (механизму выдачи денег) вместо рабочего компьютера экспертов коммерческого банка. Далее управление банкоматом переходит в руки киберпреступников, и передача данных осуществляется с помощью бесконтактных технологий (например, со смартфона) [14, 15].

Статистика, опубликованная в Отчёте о преступлениях в европейских платёжных терминалах (табл. 1) [15, 16], свидетельствует о повышении количества инцидентов логических атак на АТМ на 269% по сравнению с 2019 г. Стоит уточнить, что все зафиксированные за 2020 логические кибератаки являются атаками типа “Black box”. По результатам отчёта 22-й встречи EAST EGAF, атаки типа “Black box” занимают второе место по количеству случаев, уступая лишь «скиммингу» [17]. Также стоит упомянуть сообщения о появлениях новых способов проведения кибератаки данного типа в 2020 г. [18], что свидетельствует о востребованности методов данной атаки и интересе к ней киберпреступников.

Таблица 1.

Статистика кибератак на платёжные терминалы и банкоматы
(European payment terminal crime statistics – summary)

Terminal Related Fraud Attacks	H1 2016	H1 2017	H1 2018	H1 2019	H1 2020	% +/- 19/20
Total reported Incidents	10,820	11,934	6,760	10,723	3,631	–66%
Total reported losses	€174m	€124m	€107m	€124m	€109m	–12%
ATM Related Physical Attacks	H1 2016	H1 2017	H1 2018	H1 2019	H1 2020	% +/- 19/20
Total reported Incidents	1,604	1,696	2,046	2,376	1,829	–23%
Total reported losses	€27m	€12.2m	€15.1m	€11.4m	€12.6m	+11%
ATM Malware & Logical Attacks	H1 2016	H1 2017	H1 2018	H1 2019	H1 2020	% +/- 19/20
Total reported Incidents	28	114	61	35	129	+269%
Total reported losses	€0.41m	€1.51m	€0.25m	€0.00m	€1.00m	N/A

Source: European Association for Secure Transactions (EAST)

Учитывая перечисленные факты, можно утверждать, что атаки типа “Black box” являются актуальным и опасным вектором нападения в текущих реалиях несмотря на применяемые банками защитные меры. Рассмотрим их основные характеристики и приведём актуальные методы защиты.

Продолжительность совершения кибератаки “Black box”

Получив представление о методе совершения атаки и требуемых для этого ресурсах, проанализируем временные характеристики её совершения. Исходя из расчётов, которые пришлось опустить для экономии места в докладе, а также данных из [19, 20], была найдена

максимальная и минимальная продолжительность извлечения мошенником денежных средств из банкомата:

$$T_{\text{извл. min}} = T_{n \text{ max}} + T_{\text{подг. min}} = 420 \text{ сек.} - 23 \text{ сек.} = 217 \text{ сек.} \quad (2)$$

$$T_{\text{извл. max}} = T_{n \text{ min}} + T_{\text{подг. max}} = 240 \text{ сек.} - 210 \text{ сек.} = 30 \text{ сек.} \quad (3)$$

Раз в 20 секунд АТМ выдаёт 40 купюр, следовательно, если получать купюры максимального номинала (5000 руб.), то можно извлечь 200 000 руб. раз в 20 секунд.

Таким образом, максимальная и минимальная сумма денежных средств, которую киберпреступник успевает извлечь до приезда правоохранительных органов равна:

$$S_{\text{max}} = \frac{T_{\text{извл. min}}}{20 \text{ сек.}} \cdot 5000 \text{ руб.} = \frac{217 \text{ сек.}}{20 \text{ сек.}} \cdot 5000 \text{ руб.} = 2000000 \text{ руб.} \quad (4)$$

$$S_{\text{min}} = \frac{T_{\text{извл. max}}}{20 \text{ сек.}} \cdot 5000 \text{ руб.} = \frac{30 \text{ сек.}}{20 \text{ сек.}} \cdot 5000 \text{ руб.} = 200000 \text{ руб.} \quad (5)$$

Исходя из расчётов, киберпреступник может извлечь от 200 000 до 2 000 000 руб. На рис. 2 показана зависимость суммы хищения от времени приезда правоохранительных органов, красными линиями обозначен промежуток максимальной и минимальной суммы в случае приезда наряда в промежутке от 4 до 7 минут. Если вскрытие сервисной зоны не было замечено, то сумма потерь составит ещё больше, вплоть до полного снятия доступных в сейфе средств.

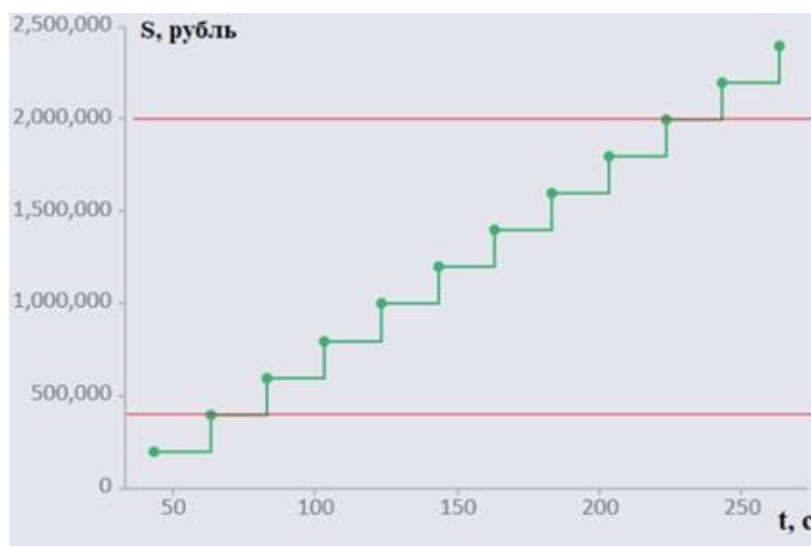


Рис. 2. Взаимосвязь ущерба и времени приезда органов обеспечения правопорядка

Таким образом, при совершении атаки типа “Black box” нанесение ущерба возможно даже при незамедлительном реагировании на факт её возникновения. Это требует наличие систем мониторинга и индикатор совершения операций, которые могут сигнализировать об атаке, но для полного предотвращения ущерба необходимо пресечь возможность злоумышленника начать использование ресивера банкомата в столь короткое время.

Повышение эффективности реагирования и защиты банкоматов от атак типа “Black box”

Существуют специальные устройства, обеспечивающие защиту от несанкционированного подключения к диспенсеру. Например, ЗУБ-Р, Cerber Lock и ATM Keeper. Они позволяют выполнять только аутентифицированные банковским ПО операции и расширить мониторинг событий безопасности банкомата. Основная проблема данного способа противодействия кибератакам – малый процент банкоматов, использующий

данные устройства. По данным компаний ООО «АНСЕР ПРО» и ООО «Artifakts» устройства используются в 15 000 АТМ, что составляет 7% от общего количества банкоматов [21]. В России до настоящего времени нет конкурентоспособного производства программно-технических средств связи и электронных компонентов [9] (не военных).

Таким образом, перечисленные способы не обеспечивают надёжную защиту от атак типа “Black box”. Нужна разработка надёжного способа увеличить время, необходимое киберпреступнику для доступа к диспенсеру. Возможным способом будет являться установка временной задержки на запуск диспенсера после его включения. Минимальная продолжительность такой задержки равняется 217 сек. При использовании надёжных средств сигнализации это позволит сократить количество случаев успешной эксплуатации банкоматов методом “Black box”.

Заключение

Рассмотренные меры направлены на повышение эффективности реагирования на инциденты информационной безопасности и, в частности, на развитие системы защиты клиентов от методов социальной инженерии и банкоматов от атак типа “Black box”. В работе проводится анализ кибератак на банкоматы типов “Brute force” и “Black box”. Научная новизна работы состоит в предложении авторами решения для ослабления приёмов социальной инженерии в результате сравнения их эффективности с эффективностью метода “Brute force”. Практическая значимость работы заключается в определении временных характеристик совершения атаки “Black box” и разработке дополнительных методов защиты банкоматов.

Литература

1. Skinner Chris. Digital Human: The Fourth Revolution of Humanity Includes Everyone. Marshall Cavendish International (Asia) Pte Ltd, 2018. – 400 p.
2. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1 (25). С. 28-38.
3. Ревенков П.В., Бердюгин А.А. Вероятностный анализ риска воздействия кибератак на системы электронного банкинга. В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019. С. 323-328.
4. Ревенков П.В., Бердюгин А.А. Расширение профиля операционного риска в банках при возрастании DDOS-угроз // Вопросы кибербезопасности. 2017. № 3. С. 16-23.
5. Ревенков П.В., Крупенко Д.С. Оценка рисков информационной безопасности в условиях применения систем мобильного банкинга // Вопросы кибербезопасности. 2019. № 2 (30). С. 21-28.
6. Berdyugin A.A., Revenkov P.V. Approaches to measuring the risk of cyberattacks in remote banking services of Russia. In: CEUR Workshop Proceedings. Selected Papers of the X Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2019). 2019. С. 6-11.
7. Probabilistic Modeling in System Engineering. / By ed. A.Kostogryzov, - London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
8. Синки Дж. Финансовый менеджмент в коммерческом банке и в индустрии финансовых услуг. М.: Альпина Бизнес Букс, 2017. – 1018 с.
9. Гущина Е.А., Макаренко Г.И., Сергин М.Ю. Обеспечение информационно-технологического суверенитета государства в условиях развития цифровой экономики // Право.by. 2018. № 6 (56). С. 59–63.
10. Зеленцов Б.П., Тутынина О.И. Теория вероятностей в познавательных и забавных задачах. М.: Книжный дом «Либроком», 2015. – 128 с.
11. Бердюгин А.А. Реинжиниринг бизнес-процессов коммерческого банка в информационном пространстве // Безопасность информационных технологий. 2021. Т. 28, №. 1, с. 62–73 DOI: 10.26583/bit.2021.1.05.

12. 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.
13. Hadnagy C. Social Engineering: The Science of Human Hacking. Wiley publ., 2018. – 320 p.
14. Россинская Е.Р., Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации // Lex russica (Русский закон). 2019. № 3 (148). С. 87–99. DOI: 10.17803/1729-5920.2019.148.3.087-099.
15. Buldas A., Gadyatskaya O., Lenin A., Mauw S., Trujillo-Rasua R. Attribute evaluation on attack trees with incomplete information: a preprint. Computers & Security, 2020. Vol. 88. – 21 p. URL: <https://arxiv.org/abs/1812.10754> (accessed on 28.02.2021).
16. Catalin Cimpanu. Diebold Nixdorf warns of a new class of ATM 'black box' attacks across Europe. Zero Day, 07.2020 URL: <https://www.zdnet.com/article/diebold-nixdorf-warns-of-a-new-class-of-atm-black-box-attacks-across-europe/> (accessed on 10.03.2021).
17. Нефёдова М. Производитель банкоматов Diebold Nixdorf обнаружил новую форму атак в странах Европы. URL: <https://xakep.ru/2020/07/17/new-jackpotting/> (дата обращения 28.02.2021).
18. Неваленный А.В., Ревенков П.В., Силин Н.Н., Фролов Д.Б. и др. Кибербезопасность в условиях электронного банкинга: практическое пособие / [Коллектив авторов, под ред. П.В. Ревенкова]. М.: Прометей; 2020. – 520 с.
19. Антонов Алексей. Как злоумышленники используют уязвимости АТМ // Расчеты и операционная работа в коммерческом банке. М.: Регламент, 2018. № 2 (144). С. 47–59. URL: <http://futurebanking.ru/reglamentbank/article/4994> (дата обращения 23.02.2021).
20. Samuel Gibbs. Jackpotting: hackers are making ATMs give away cash. Guardian News, 01.2018. URL: <https://www.theguardian.com/technology/2018/jan/29/jackpotting-hackers-atm-cash-machine-give-away> (accessed on 24.03.2021).
21. Киздермишов А.А. Анализ возможности использования свободно распространяемых сетевых сканеров // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2014. № 3 (142). С. 201–205. URL: <https://www.elibrary.ru/item.asp?id=23055763> (дата обращения 24.02.2021).

Assessment of the risk of a cybersecurity breach in a commercial bank (by the example of an attacks “Brute force” and “Black box” on ATMs)

Revenkov P.V.¹⁸⁴, Berdyugin A.A.¹⁸⁵, Makeev P.V.¹⁸⁶

Abstract. *The progress of digital transformation of society and, in particular, financial and economic systems leads to the complication of the problems of information security of competing entities. By focusing on scientific research, you can achieve success in these areas. The purpose of the study is increasing the level of security of banking services for individuals and legal entities in accordance with the recommendations of information security standards, by analyzing the risk of information security violations in electronic banking technologies (on the example of the “Brute force” and “Black box” attacks). Standards for effective management of information security in the enterprise are given. The advantage of social engineering methods over the “Brute force” method of PIN codes is shown quantitatively. The time characteristics of “Black box ” type attacks are analyzed. A method for improving the effectiveness of the response and protection of ATMs from attacks of the “Black box” type is proposed.*

Keywords: standards, PIN code, cyberattacks, ATM, dispenser, cybercriminal.

¹⁸⁴ Pavel Revenkov, Dr.Sc., Assistant Professor, Professor of the Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: pavel.revenkov@mail.ru, orcid.org/0000-0002-0354-0665

¹⁸⁵ Alexander Berdyugin, Junior researcher of the Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: brdgn@bk.ru, orcid.org/0000-0003-2301-1776

¹⁸⁶ Pavel Makeev, Master’s Degree student of the Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: paulmakeev@gmail.com, orcid.org/0000-0003-0031-5419

Стратегические проблемы применения информационно-коммуникационных технологий в военно-политической сфере

Ромашкина Н.П.¹⁸⁷

Аннотация. В статье представлены результаты анализа стратегических угроз и проблем информационной и кибербезопасности в военно-политической сфере. Поставлены проблемы применения информационно-коммуникационных технологий (ИКТ) в военно-политических целях для осуществления враждебных действий и актов агрессии, а также обеспечения информационной безопасности военных объектов как части критически важной инфраструктуры государства, выявлены угрозы, признаки их наличия и возможности осуществления. Обоснован вывод о необходимости развития механизмов международного управления в этой области, частью которых могут стать предложенные автором конкретные международные действия с участием России в ответ на актуальные глобальные вызовы международной безопасности и стратегической стабильности.

Ключевые слова: информационная безопасность, кибербезопасность, информационное оружие, кибероружие, информационная угроза, ядерное оружие, стратегическая стабильность.

Введение

Вопросы вредоносного использования информационно-коммуникационных технологий (ИКТ) в военно-политической сфере являются самыми сложными в рамках международных организаций. Впервые указание на ИКТ-угрозы применительно не только к гражданской, но и к военной области содержалось в резолюции Генеральной Ассамблеи ООН 54/49 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 1 декабря 1999 г. С тех пор никаких международных документов на уровне ООН, нормативно ограничивающих такую противоправную деятельность, принято не было. Поэтому информационные средства для создания деструктивного эффекта в военно-политической сфере постоянно совершенствуются, разрабатываются новые ИКТ-вооружения для военной борьбы, разведывательного противоборства, электронного противоборства и т.д.; для вмешательства во внутренние дела государств; для вредоносного воздействия на объекты критически важной государственной инфраструктуры, и, в частности, на объекты военно-промышленного комплекса (ВПК) [1-3].

Информационные технологии на службе у политики

Защищенность ИКТ-систем, которые стали важным фактором обеспечения суверенитета, безопасности и обороноспособности государства, имеют стратегическое значение для большинства стран мира [4-7]. При этом речь идет об угрозе ускоренного развития (т.е. гонки) информационных вооружений как для вмешательства во внутренние дела государства, так и с военными целями [8] (табл.1). ИКТ могут привести к межгосударственному военному конфликту из-за возможности несоразмерного использования методов реагирования, а также по ошибке, т.к. в настоящее время отсутствует универсальная методология идентификации нарушителей, не выработаны критерии отнесения кибератак к вооруженному нападению, не сформированы универсальные принципы расследования инцидентов, что существенно снижает уровень стратегической стабильности [7-10].

¹⁸⁷ Ромашкина Наталия Петровна, кандидат политических наук, Руководитель подразделения проблем информационной безопасности ЦМБ ИМЭМО РАН, Москва, Romachkinan@yandex.ru.

Таблица 1.

Проблема применения ИКТ в военно-политических целях для осуществления враждебных действий и актов агрессии

Угроза	Признаки наличия угрозы	Возможности осуществления угрозы
Развитие ИКТ-вооружений	Ускоренная милитаризация ИКТ-пространства.	ИКТ-средства для применения в военной области: • борьба с системами управления и контроля; • разведывательное противоборство; • электронное противоборство; • военные средства, способствующие проведению информационных операций.
	Включение ИКТ-сферы в интегрированное поле боевых действий в стратегиях некоторых стран.	
	Наличие наступательного кибероружия и кибервойск у 30 государств.	
	Наращивание наступательных и оборонительных информационных операций странами НАТО.	
	Планы создания средств кибервойны у 140 стран.	
	Сложность выявления автора ИКТ-атаки, возможность использования «ложного флага».	
Применение ИКТ во враждебных военно-политических целях, для вмешательства во внутренние дела государств	Факты вмешательства:	Альтернативные военным средства воздействия на противника: • экономические (ИКТ-воздействие на промышленные и финансовые объекты); • информационные (пропагандистское иновещание, Интернет (поисковые системы, социальные сети, сетевые «зеркала»), мобильные приложения, смс) для подготовки и проведения массовых беспорядков, антиправительственных демонстраций, политических акций, государственных переворотов.
	• Революция «Солидарности», Польша, 1980-1990;	
	• «Бархатная революция», Чехословакия, 1989;	
	• «Бульдозерная революция», Югославия, 2000;	
	• подготовка вторжения с применением ИКТ, Афганистан, 2001;	
	• «Революция роз», Грузия, 2003;	
	• вторжение с применением ИКТ, Ирак, 2003;	
	• «Оранжевая революция», Украина, 2004;	
	• «Революция тюльпанов», Киргизия, 2005;	
	• «Жасминовая революция», Тунис, 2011;	
	• «Твиттерная революция» («Революции лотоса»), Египет, 2011;	
	• гражданская война, Ливия, 2011;	
	• «Евромайдан», Украина, 2013-2014;	
	• «Революция розеток», Армения, 2015;	
	• гражданская война, Сирия, 2011 – наст. время;	
	• подготовка государственного переворота, Венесуэла, 2019.	

Киберугрозы в стратегической военной сфере

Сегодня уже десятки стран обладают программным обеспечением для нападения на объекты критически важной инфраструктуры государства (КИ), однако 83% всех площадок, используемых для их распространения, расположены всего в 10 государствах. Лидером этого рейтинга являются США, где находится четверть всех источников. Целями

могут быть органы государственной власти, банки, спутниковые, нефтегазовые системы, электро- и атомные станции, коммуникационные системы, порты, военные объекты и т.д. [11]. Таким образом, подобные вредоносные программы представляют собой стратегическое оружие, а растущая сложность оборудования ведет к росту вероятности ошибок и уязвимостей, что может быть использовано противником [12, 13].

Одной из важнейших глобальных проблем является информационная безопасность военных объектов как части КИ, и, в первую очередь, систем ядерного оружия [14, 15]. Таким образом, существует несколько типов угроз, создающих проблему обеспечения ИКТ-безопасности объектов ВПК (табл.2) [4, 7].

Таблица 2.

Проблема обеспечения информационной безопасности военных объектов как части критически важной инфраструктуры государства

Угроза	Признаки наличия угрозы	Возможности осуществления угрозы
Развитие ИКТ-средств для вредоносного воздействия на объекты ВПК	Наличие ИКТ-угроз для военной организации и инфраструктуры, в т.ч., стратегические вооружения, система предупреждения о ракетном нападении (СПРН), система командования и контроля над ядерным оружием (ЯО), ПРО, ПВО.	- Кибернападения на объекты военной или связанной с ней гражданской инфраструктуры; - физический вред ПО, элементной базе, линиям связи и сетям военного объекта; - дистанционный «логический» вред с помощью вредоносных программ, «логических бомб» и т.д.;
	Применение ударных роботизированных средств, искусственного интеллекта, автоматизированных систем принятия решений и т.д., которые могут подвергаться кибератакам.	
	Перевод войск стратегического назначения в разных странах на цифровые технологии передачи информации, что делает их более уязвимыми для ИКТ.	
Снижение уровня стратегической стабильности	Влияние ИКТ на рост вероятности:	- умышленный или непреднамеренный удаленный вред через компьютерные сети или в результате контакта с компьютером; - кибершпионаж и создание киберагентурных сетей; - киберсаботаж; - создание неуверенности командования и персонала в бесперебойной и
	• несанкционированного запуска баллистических ракет (БР), на принятие решения о применении ЯО;	
	• получения ложной информации от СПРН о запуске БР со стороны противника;	
	• повреждения или разрушения каналов коммуникаций, создания помех в системе управления вооруженными;	
	• снижения уверенности военных в работоспособности систем управления, командования и контроля ВС.	
	Влияние ИКТ-факторов на будущее процессов ядерного разоружения и нераспространения.	

	Влияние ИКТ-факторов на уровень стратегической стабильности.	эффективной работе систем.

Выводы

1. Применение информационного оружия в военно-политических целях для осуществления враждебных действий и актов агрессии; деструктивное ИКТ-воздействие на элементы КИ; вмешательство во внутренние дела государств, нарушение общественной стабильности посредством ИКТ обозначены в качестве самых опасных угроз в российских документах и требует поиска дополнительных механизмов международного управления.
2. В связи с масштабом ИКТ-угроз в военной стратегической сфере необходима работа внешнеполитических ведомств по согласованию на международном уровне перечней критической военной (ядерной) инфраструктуры, попытка воздействия на которую с применением ИКТ будет расцениваться как попытка обезоруживающего удара с соответствующими последствиями.
3. Необходима работа ООН по формированию режима контроля над ИКТ-вооружениями, который мог бы включать:
 - конкретные меры укрепления доверия и безопасности в ИКТ-сфере;
 - запрет ИКТ-атак на конкретные объекты, в том числе, в военной сфере и в особенности – ядерные;
 - ограничение и (или) отказ от наступательных ИКТ-возможностей;
 - меры контроля за распространением ИКТ-вооружений;
 - международные нормы в отношении средств и методов предотвращения и устранения киберконфликтов;
 - разработку конвенции о запрещении вредоносного использования ИКТ в сфере ЯО.

Литература

1. Molander R., Riddile A., Wilson P. Strategic information warfare: a new face of war. Library of Congress Cataloging in Publication Data, RAND (Firm), 1996. 33 p. URL: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf.
2. Проблемы информационной безопасности в международных военно-политических отношениях. Под ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН, 2016, 183 с. URL: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf.
3. Petrenko S. Cyber Security Innovation for the Digital Economy a Case Study of the Russian Federation. - River Publishers, 2018. - 492 p.
4. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. - 2019. - No. 1 (29). - С. 2-9.
5. Ромашкина Н.П. Новые технологии: вызовы международной безопасности и стабильности // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. - М.: МГТУ им. Н.Э. Баумана, 2019. - С. 329 - 334.
6. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / Отв. ред. – А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с.
7. Ромашкина Н.П., Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. № 5 (39). С. 77-86.
8. Information Security Threats during Crisis and Conflicts of the XXI Century / Eds.: N.P. Romashkina, A.V. Zagorskii. Moscow: IMEMO, 2016. URL: https://www.imemo.ru/files/File/en/publ/2016/2016_001.pdf.

9. Арбатов А.Г. Роль ядерного сдерживания в стратегической стабильности. Гарантия или угроза. Московский Центр Карнеги, URL: <https://carnegie.ru/2019/01/28/ru-pub-78209>.
10. Ромашкина Н.П. Стратегическая стабильность в современной системе международных отношений. М.: Научная книга, 2008, 288 с., URL: <http://www.avnrf.ru/index.php/drugie-publikatsii/590-strategicheskaya-stabilnost-v-sovremennoj-sisteme-mezhdunarodnykh-otnoshenij>.
11. Шнепс-Шнеппе М.А., Селезнев С.П., Намиот Д.Е., Куприяновский В.П. О кибербезопасности критической инфраструктуры государства. // International Journal of Open Information Technologies, vol. 4, no. 7, 2016. URL: <https://cyberleninka.ru/article/n/o-kiberbezopasnosti-kriticheskoy-infrastruktury-gosudarstva>.
12. Марков А. С., Шеремет И. А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник академии военных наук. - 2019. - No. 2. - С. 82-90.
13. Markov A.S., Sheremet I.A. Enhancement of Confidence in Software in the Context of International Security // CEUR Workshop Proceedings. - 2019. - Vol. 2603. - P.88-92.
14. Romashkina N.P. New Technologies: Challenges to International Security and Stability // CEUR Workshop Proceedings. Selected Papers of the X Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2019). - 2019. - Vol. 2603. - P.65-69.
15. Sherman F. Aborting Unauthorized Launches of Nuclear-Armed Ballistic Missiles through Postlaunch Destruction // Science and Global Security, 1990, Volume 2, No. 1.

Strategic Problems of Using Information and Communication Technologies in the Military-Political Sphere

Romashkina N.P.¹⁸⁸

Abstract. *The article presents the results of the analysis of strategic threats and problems of information and cyber security in the military-political sphere. The problems of using information and communication technologies (ICT) for military-political purposes for the implementation of hostile actions and acts of aggression, as well as ensuring the information security of military facilities as part of the critical national infrastructure are posed. Threats, signs of threats and the possibility of their implementation are identified. Conclusion that it is necessary to develop mechanisms of international governance in this area, part of which can be proposed by the author of specific international actions with the participation of Russia in response to current global challenges to international security and strategic stability is substantiated.*

Keywords: *information security, cyber security, information weapons, cyber weapons, information threat, nuclear weapons, strategic stability.*

УДК 004.056

¹⁸⁸Nataliya Romashkina, PhD in Political Sciences, Head of the Informational Security Problems Group of the Primakov National Research Institute of World Economy and International Relations (IMEMO) of the Russian Academy of Sciences, Moscow, Romachkinan@yandex.ru

Методы тестирования программного обеспечения для повышения безопасности продукта

Северов В.С.¹⁸⁹

Аннотация. Тестирование безопасности программного обеспечения является важным средством для поддержания в разрабатываемом продукте безопасности и надежности. В этой статье исследуются и анализируются методы тестирования безопасности программного обеспечения, а затем делаются выводы об их преимуществах и недостатках с точки зрения количества выявленных уязвимостей. При этом рассматриваются методы тестирования, которые влияют на безопасность как напрямую, за счёт непосредственного выявления уязвимостей, так и косвенно, за счёт улучшения качества продукта.

Ключевые слова: анализаторы кода, фаззинг тестирование, тестирование на проникновение, модульное тестирование, интеграционное тестирование, регрессионное тестирование.

Введение

В настоящее время умные технологии начинают применяться в совершенно разных сферах жизни, будь то серьезное производство или незначительные IoT устройства в наших домах. Всё чаще вместо привычных бумажных документов можно встретить специальные системы электронного документооборота. И все эти устройства и системы не могут существовать без специализированного программного обеспечения.

Но что будет, если у этих программных средств будут различные ошибки или даже уязвимости? В таком случае злоумышленники украсть персональные данные пользователей или нарушить алгоритмы работы программного обеспечения. Это может привести к непоправимым последствиям. Именно поэтому целью данного исследования является анализ различных методов для повышения безопасности проектов на этапе тестирования.

Основная часть

Существуют различные методы тестирования программного обеспечения. Их можно разделить на две категории. Во-первых, это методы, которые напрямую влияют на безопасность. Их применение более существенно и без них практически невозможно разработать безопасное программное обеспечение. Во-вторых, это методы, применение которых влияет лишь косвенно. Их применение в большей степени влияет на качество программного обеспечения, которое в свою очередь может повышать безопасность системы, поэтому они будут рассмотрены менее подробно [1].

Тестирование программного обеспечения осуществляется после разработки отдельного модуля или всей системы в целом. В целом, тестирование не даёт гарантий того, что разработанное программное обеспечение не будет содержать ошибок и уязвимостей, однако использование хороших методов может гарантировать существенное уменьшение количества неисправностей и, соответственно, повышения безопасности.

Тестирование можно проводить вручную, однако такое тестирование имеет ряд существенных недостатков: на него уходит много времени, и оно очень редко позволяет протестировать весь функционал. Поэтому для тестирования часто прибегают к использованию автоматизированных средств, видов которых достаточно большое количество.

¹⁸⁹ Северов Владимир Сергеевич, студент, МГТУ им. Н. Э. Баумана, Москва, vsev.s@mail.ru

Далее будут рассмотрены методы тестирования программного обеспечения, которые могут быть использованы как для ручного, так и для автоматизированного тестирования.

Методы для повышения безопасности

Анализаторы кода

Существует множество различных статических анализаторов кода для различных языков программирования и различных задач [2, 3]. Но среди всех них можно выделить ряд общих типов ошибок, влияющих на безопасность, которые они способны обнаружить.

Анализаторы могут выявить код, который имеет неопределенное поведение. Например, оно возникает, когда есть не проинициализированные переменные или присутствует так называемое состояние гонки. В результате состояния гонки порой можно получить доступ к тем ресурсам, к которым доступа быть не должно. Особенно это касается программ, запускаемых с правами администратора.

Анализаторы могут помочь найти некорректное использование различных функций. Например, при вызове функции аутентификации может быть упущена передача пароля, что может привести к некорректному разрешению доступа.

Анализаторы могут выявить использование популярных, но небезопасных функций. Например, большинство функций для работы со строками в языке Си считаются небезопасными. Их использование может привести к атакам переполнения буфера.

Анализаторы также могут обнаружить потенциальные места, где может произойти утечка памяти. Например, когда кто-то пытается освободить ресурсы после возврата результата из функции (код освобождения ресурсов просто не будет выполнен).

В связи с вышеперечисленными характеристиками можно сказать, что анализаторы кода могут сильно повысить безопасность продукта. При этом они являются наиболее используемыми в связи с простотой использования [4, 5].

Тестирование на наличие уязвимостей

Существуют различные автоматизированные средства, которые позволяют выявлять несложные уязвимости. Их периодическое использование позволит еще на ранних этапах разработки выявить большинство уязвимостей. Например, это может быть тестирование на возможность использования SQL инъекций [6].

Фаззинг тестирование

Во время проведения тестирования стоит также проводить, так называемое, фаззинг тестирование [1, 7-9]. Оно позволит определить, корректно ли разработанная система обрабатывает случайные входные данные. Таким образом, достаточно легко обнаружить отсутствие проверки входных данных. В тех местах, где проверки входных данных нет, может быть проведено множество атак, например XSS или SQL инъекции, однако обычно такое тестирование не очень эффективно.

Тестирование на проникновение

Тестирование на проникновение [10] выполняется экспертами по информационной безопасности и позволяет выявить сложные уязвимости, которые не получилось выявить при тестировании с помощью различных автоматизированных средств. Например, это

может быть эксплуатирование одних уязвимостей, чтобы найти другие. При грамотном составлении моделей угроз на этапе проектирования, а также при тестировании опытными специалистами по безопасности, может быть выявлено большинство уязвимостей.

Методы для повышения качества

Тестирование стабильности

Тестирование стабильности [1, 11] предназначено для проверки корректности работы программного обеспечения, которое находится под нагрузкой в течение определённого времени. Это может быть полезно, так как некоторые проблемы, такие как утечки памяти, сложно заметить при коротком тестировании. При создании большой нагрузки будет происходить большое количество вызовов различных функций, что может спровоцировать состояние гонки данных или многократный вызов функций, в которых есть различные ошибки. По окончании тестирования происходит анализ полученных результатов, например, ошибок авторизации. Модули, в которых возникло большое количество ошибок необходимо доработать и провести тестирование заново.

Модульное тестирование

Модульное тестирование [1, 12] предназначено для проверки работоспособности различных частей системы. Плюсом данного подхода является то, что можно полностью протестировать отдельный модуль, а также при возникновении ошибок можно с лёгкостью определить, где они произошли. Однако это приводит и к основному минусу: так как все модули тестируются отдельно, то невозможно проверить правильность работы модулей между собой. Например, можно протестировать функцию валидации и хеширования пароля.

Интеграционное тестирование

В отличие от модульного тестирования, интеграционное тестирование [1, 13] проверяет работу группы модулей, чтобы позволяет проверить не только сами модули, но и то, как они взаимодействуют. Также данный вид тестирования позволяет проверить всю систему в целом. Минусом является то, что достаточно сложно протестировать все части системы полностью. Например, можно проверить, что доступ к разным модулям осуществляется, только если модуль авторизации подтвердил пользователя.

Регрессионное тестирование

Регрессионное тестирование [14, 15] – тестирование, которое предназначено для того, чтобы при добавлении новых модулей или при исправлении старых, убедиться, что в ранее протестированных частях программы новых ошибок не возникло. Как правило, при данном виде тестирования используются модульные и интеграционные тесты, созданные на предыдущих этапах.

Выводы

В данном исследовании были рассмотрены различные методы тестирования программного обеспечения. Часть из них влияет на безопасность напрямую, а часть из них косвенно, за счёт улучшения качества продукта. Все перечисленные методы широко используются на практике [16], и наиболее популярным среди них являются применение статических анализаторов в связи с простотой использования и достаточно хорошей эффективностью.

Литература

1. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь. 2012. 192 с.
2. Рибер Г., Малмквист К., Щербakov А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1(2). С. 36-39.
3. C. Cowan. Software security for open-source systems. IEEE, 2003; DOI:10.1109/MSECP.2003.1176994.
4. Кононов Д.С. Итерационный метод поиска клонированного кода, основанный на вычислении редакционного расстояния // Вопросы кибербезопасности. 2017. № 1. С. 16-21.
5. Gu Tian-yang. Research on Software Security Testing, World Academy of Science, 2010;
6. William G.J. Halfond. A Classification of SQL Injection Attacks and Countermeasures. Georgia Institute of Technology, 2006;
7. Баранов А.П. Актуальные проблемы в сфере обеспечения информационной безопасности программного обеспечения // Вопросы кибербезопасности. 2015. № 1. С. 2-5.
8. 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
9. Sofia Bekrar. Finding Software Vulnerabilities by Smart Fuzzing. IEEE, 2011;
10. B. Arkin. Software penetration testing. IEEE, 2005;
11. Myrvin H. Ellestad. Stress Testing: Principles and Practice. Oxford University Press, 2003;
12. Ian J. Hayes. Specification directed module testing. IEEE, 1986;
13. Paul Clifton Jorgensen. Object-oriented integration testing. Communication of the ASM, 1994;
14. Akira K Onoma. Regression testing in an industrial environment. Communication of the ASM, 1998.
15. W. E. Wong. A study of effective regression testing in practice. IEEE, 1997.
16. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5. С. 2-10.

Рецензент: Цирлов В.Л., к.т.н., доцент кафедры ИБ МГТУ им.Н.Э.Баумана

Software Testing Methods to Improve Product Security

Severov V. S.¹⁹⁰

Abstract. *Software security testing is an important means for maintaining security and reliability in the product development process. In the article, software security testing methods are analyzed, and then conclusions about their advantages and disadvantages are made based on the number of vulnerabilities identified. Meanwhile, testing methods affecting security by directly identifying vulnerabilities, and indirectly, by improving the quality of the product, are considered.*

Keywords: *code analyzers, fuzzing testing, penetration testing, unit testing, integration testing, regression testing.*

УДК 004.056

¹⁹⁰ Severov Vladimir, student, Bauman Moscow State Technical University, Moscow, vsev.s@mail.ru

Обеспечение защиты сетевых ресурсов в телемедицинской системе наблюдения пациентов с деменцией

Соколова А.В.¹⁹¹

Аннотация. Рассмотрены требования к безопасности телемедицинских систем. Оценка состояния здоровья человека с деменцией выполняется на основе медицинских данных, которые регистрируются датчиками и передаются в облачную медицинскую информационную систему. На основе полученных данных лечащим врачом формируются рекомендации. Поскольку медицинские консультации оказываются на расстоянии, возникает необходимость обеспечить надёжность хранения и передачи медицинских данных пациента. Определены решения и способы защиты передаваемых данных, способствующие привести разрабатываемую телемедицинскую систему к требуемым нормам безопасности. Отмечено, что представленные методы являются необходимыми, но недостаточными и требуются дополнительные способы защиты передаваемых данных.

Ключевые слова: защита информации, мониторинг, электронная медицинская карта, медицинские информационные системы.

Введение

Улучшения в сфере здравоохранения способствуют тому, что жизнь людей становится более продолжительной и более здоровой. Наиболее популярным направлением здравоохранения на сегодняшний день является телемедицина. В рамках этого направления создаётся большое количество телемедицинских систем, способных повысить качество и скорость получения медицинской помощи посредством дистанционного взаимодействия с врачом.

Применение телемедицинских технологий при оказании медицинской помощи осуществляется с соблюдением требований, установленных законодательством Российской Федерации в области персональных данных, и соблюдением врачебной тайны [1]. Так как медицинская консультация осуществляется в удалённом формате, то есть риск несоблюдения врачебной тайны – медицинские данные пациента могут оказаться у третьих лиц. Чтобы этого избежать, телемедицинской системе необходимо принимать меры по обеспечению защиты данных как при передаче их между пациентом и врачом, так и при их хранении в системе [2].

В данной статье будут выявлены требования к телемедицинским системам по безопасности, а также и их выполнение на примере разрабатываемой телемедицинской системы, способной оценивать состояние людей с деменцией.

Архитектура телемедицинской системы

Разрабатываемая телемедицинская система представлена в виде клиент-серверного приложения. Она позволит пациенту общаться с врачом, предоставляя системе определённые результаты исследований, необходимые для постановки диагноза деменции. Предполагается, что система будет обрабатывать полученные от пациента результаты исследований и предоставлять эту информацию лечащему врачу [3]. Помимо исследований, пациент может пройти нейропсихологические тесты, являющиеся эффективным инструментом обнаружения деменции. В свою очередь, врач, используя полученные результаты исследования и тестов, сможет более точно диагностировать деменцию при её наличии и сформировать индивидуальные рекомендации по лечению и поддержке состояния пациента, исходя из полученного анамнеза. Система позволяет облегчить и

¹⁹¹ Соколова Акси́нья Влади́мировна, аспирант кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, г. Москва, aksinya.sokolova@yandex.ru

Разрабатываемую систему планируется использовать как помощник для облегчения и ускорения обработки анализов пациента врачом дистанционно.

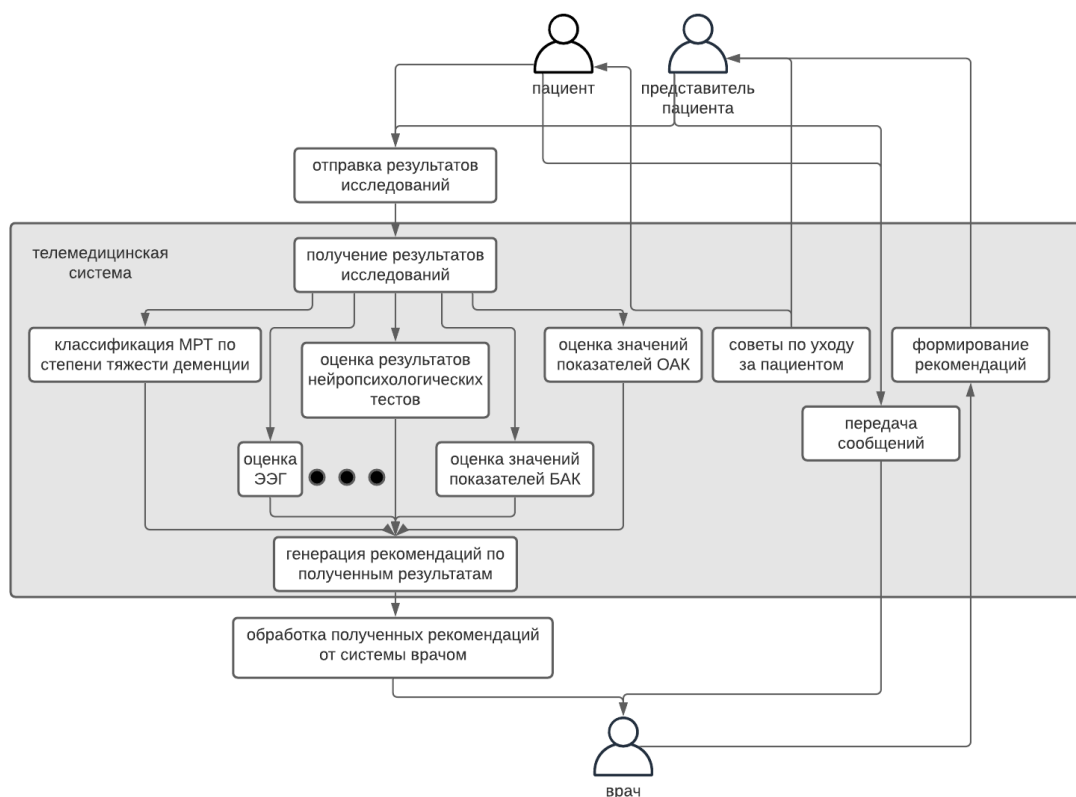


Рис. 1. Структура телемедицинской системы наблюдения пациентов с деменцией

Для соответствия телемедицинской системы всем требованиям Министерства здравоохранения стоит проводить мероприятия по обеспечению безопасности информационных систем [4]. К требованиям по безопасности информации добавляется необходимость соблюдения Федерального Закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

- предотвращение неправомерного доступа к информации, ее модифицирования, блокирования, копирования, предоставления и распространения (исключение доступа к неавторизованным пользователям),

- возможность восстановления информационной инфраструктуры, за счет создания и хранения резервных копий (телемедицинские системы должны функционировать в

специализированных внутренних сетях, с использованием системы резервного копирования на случай, если часть данных будет утеряна);

- передача информации медицинским учреждениям или организациями только в зашифрованном виде.

Ниже приведены решения, реализация которых обеспечит системе соответствие перечисленным нормам безопасности.

Меры по обеспечению безопасности системы

Основной задачей безопасности передачи данных является необходимость обеспечения защиты личного кабинета пользователей системы. Предполагается, что войти в систему может только пациент, представитель пациента, врач-консультант, сотрудники медицинского учреждения, а также администратор системы [5]. В связи с этим были реализованы пять ролей на основании функциональной модели системы, которые обладают следующими свойствами (таб. 1).

Таблица 1.

Ролевая модель системы

	добавление информации	редактирование информации пациента	просмотр информации	формирование медицинских рекомендаций пациента	для
пациент	+	+	+	-	
представитель пациента	+	-	+	-	
врач	+	-	+	+	
медицинский персонал	+	-	+	-	
администратор	+	+	+	+	

Работа с функционалом системы приходится на веб-приложение, авторизовавшись в котором пользователь открывает весь функционал, предусмотренный для его роли [6].

Так как медицинские услуги в телемедицине предоставляются на расстоянии, то есть необходимость перехода на электронный документооборот. Пациент либо его законный представитель смогут по запросу, направленному в том числе в электронной форме, получать отражающие состояние его здоровья медицинские документы, включая выписки из них, и копии медицинских документов, в форме электронных документов, подписанных усиленной квалифицированной электронной подписью врача.

Идентифицировать пользователя системы, подписавшего документ, позволяет электронная цифровая подпись (ЭЦП) - криптографическое программное обеспечение, которое обеспечивает высокую степень защиты данных.

В качестве алгоритма для электронной подписи применяется метод шифрования с открытым ключом, при котором для пользователя специальным образом выбирается пара ключей – открытый и закрытый. При этом алгоритмы выбора ключей гарантируют, что открытым ключом можно расшифровать только те документы, которые шифровались соответствующим ему закрытым ключом. Таким образом, если открытый ключ владельца ЭЦП известен и полученный от него документ удалось расшифровать, то стоит утверждать, что пользователь идентифицирован [7].

ЭЦП обеспечивает высокую степень защиты данных и позволяет исключить возможность несанкционированного доступа к системе. Следовательно, каждому пользователю системы необходимо иметь сертификат и ключ электронной подписи, чтобы иметь возможность воспользоваться телемедицинскими услугами.

Выводы

В ходе работы были рассмотрены требования к безопасности телемедицинских систем, проанализированы различные необходимые методы безопасности.

На практике было определено, что меры по организации безопасности системы обеспечили доступ к системе только авторизованным и верифицированным пользователям, а также позволили осуществить защищённый документооборот между пациентом и сотрудниками медицинского учреждения, осуществляющего консультации.

Указанные требования к безопасности были выполнены при проектировании клиент-серверной архитектуры разрабатываемой системы, внутренних сервисов и структуры баз данных, а также их нормализации, были осуществлены действия по управлению уязвимостями и ведением отчётности по всем действиям пользователя в системе.

В работе была показана организация мер безопасности системы, способной оценивать состояние людей с деменцией, но перечисленные меры будут актуальны для всех телемедицинских систем.

Литература

1. Блинов С.В., Кузьмина Н.М., Ревина С.Н., Сидорова А.В. Соблюдение врачебной тайны при оказании телемедицинских услуг // Вестник медицинского института "РЕАВИЗ": реабилитация, врач и здоровье. 2019. № 2 (38). С. 196-200.
2. Булдакова Т.И., Миков Д.А., Соколова А.В. Защита данных при дистанционном мониторинге состояния человека // Журнал «Вестник МГТУ. Серия: Приборостроение». 2020. № 4. С. 42-57.
3. Pijush Kanti Dutta Pramanik, Gaurav Pareek, Anand Nayyar. Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards // Telemedicine Technologies: big data, deep learning, robotics, mobile and remote applications for global healthcare, 2019, P. 201-225.
4. Журавлев М.С. Защита персональных данных в телемедицине // Право. Журнал Высшей школы экономики. 2016. № 3. С. 72–84
5. Булдакова Т.И., Соколова А.В., Халайджи А.К. Мониторинг состояния человека-оператора киберфизической системы // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2020. № 10. С. 20-27.
6. Булдакова Т.И., Кривошеева Д.А. Угрозы безопасности в системах дистанционного мониторинга. // Вопросы кибербезопасности. 2015. № 5(13). С. 45-50.
7. Гомалеев А.О. Перспективы применения электронной, в том числе дистанционной электронной, подписи в целях повышения эффективности предоставления государственных услуг // Научно-практический электронный журнал Аллея Науки. 2018. №2(18). С. 661-667.

Научный руководитель

Булдакова Татьяна Ивановна, доктор технических наук, профессор кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана, buldakova@bmstu.ru.

Securing Network Resources in the Telemedicine Surveillance System for Dementia Patients

Sokolova A.V.¹⁹²

Annotation. *The requirements for the safety of telemedicine systems are considered. The health status of a person with dementia is assessed based on medical data recorded by sensors and transmitted to a cloud-based medical information system. On the basis of the data obtained, the attending physician formulates recommendations. Since medical consultations are at a distance, it becomes necessary to ensure the reliability of storage and transmission of patient medical data. The solutions and methods of protecting the transmitted data, which help to bring the developed telemedicine system to the required safety standards, have been determined. It is noted that the presented methods are necessary, but insufficient, and additional methods of protecting the transmitted data are required.*

Keywords: *information security, monitoring, electronic medical record, medical information systems.*

¹⁹² Sokolova Aksinya, postgraduate student, Bauman Moscow State Technical University, Moscow, aksinya.sokolova@yandex.ru

Биометрические технологии аутентификации**Тарапанова Е.А.¹⁹³, Бойко Е.В.¹⁹⁴**

Аннотация. Статья посвящена актуальным аспектам биометрических технологий аутентификации. Авторами выполнен обзор существующих биометрических технологий аутентификации и рассмотрены области их применения. Представлена градация биометрических систем в соответствии с используемым биометрическим признаком. Проанализированы основные виды статических биометрических систем и принципы их функционирования. Также изучен принцип действия поведенческой биометрии и рассмотрены основные виды динамических биометрических систем. Проведено исследование различных категорий мультибиометрических систем, а также уровней объединения технологий и способов формирования совместного решения в них. Сделаны выводы.

Ключевые слова: биометрия, биометрические статические и динамические характеристики, идентификация, верификация, биометрический признак, дактилоскопия, двухмерное и трехмерное распознавание лиц, секвенирование ДНК, мультибиометрические системы.

Введение

На данный момент биометрические системы находят применение во многих сферах жизни общества, они являются одними из наиболее динамично развивающихся технологий. Традиционно биометрические технологии связывают с такими направлениями как защита информации и криминалистика. Однако растет также эффективность их использования:

- в качестве систем контроля доступа, систем аутентификации личности и систем электронной коммерции;
- при проведении электронных платежей и аутентификации на Web-ресурсах;
- в качестве систем учета рабочего времени сотрудников и для регистрации посетителей организации;
- в различных социальных проектах, где требуется идентификация или верификация людей и в проектах гражданской аутентификации (пересечение государственных границ, выдача различных видов виз на посещение страны, в системах голосования, борьба с коррупцией в Гвинейской Республике [1]) и т.д.

Кроме того, все шире применяются электронные средства идентификации личности, основанные на биометрических данных в современных системах, основанных на технологии блокчейн [2], которая объединяет теорию игр, криптографию и разработку программного обеспечения. Подменить блок в цепочке крайне тяжело, если не невозможно, так как одно из основных свойств криптографических хеш-функций – необратимость. [3] А для повышения безопасности транзакций и коммуникаций, что, как следствие, повышает надежность сохранения приватности пользователя и применяется биометрическая защита блокчейна.

Актуальность использования биометрических систем связана с тем, что в отличие от факторов владения (smart-карта, телефон, пропуск, паспорт, водительские права) и факторов знания (пароль, персональный идентификационный номер (PIN), код)

¹⁹³ Тарапанова Елена Александровна, кандидат философских наук, доцент кафедры «Защита информации», ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», Москва, tarapanova@bmstu.ru

¹⁹⁴ Бойко Екатерина Витальевна, выпускник кафедры «Информационная безопасность», ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», Москва, boykokate@mail.ru

биометрические характеристики (факторы признака) не могут быть забыты или потеряны, их трудно подделать (некоторые невозможно на данном этапе) и практически невозможно изменить (некоторые абсолютно невозможно).

Тема биометрической аутентификации граждан последние несколько лет находится в фокусе не только общественного, но и политического внимания. Например, в России рассматривается возможность введения всеобщей обязательной биометрической регистрации, но ее внедрение затруднено тем, что для биометрических данных должен быть установлен специальный правовой режим и регулирование. [4] Кроме того, остро встает вопрос безопасности такой базы данных: у субъектов персональных биометрических данных во всем мире вызывает беспокойство возможность адекватной защиты биометрических шаблонов. [5]

Основная часть

Выделяют два вида биометрических систем:

- Системы, функционирующие в режиме биометрической идентификации (системы контроля доступа/учета рабочего времени и т.п.). В них каждый из биометрических образцов сопоставляется со всеми имеющимися записями или выбранной частью записей в базе данных (сопоставление 1:N или «один ко многим»)
- Верификационные системы. В них предъявленный биометрический признак сравнивается с одним биометрическим признаком из базы данных (сопоставление 1:1). То есть система проверяет является ли пользователь тем, за кого себя выдает.



Рис.1. Схема процесса обработки информации в типовой биометрической системе

По принципу действия биометрические системы делятся на статические, динамические и комбинированные.



Рис.2. Схема градации биометрических систем

Рассмотрим более подробно градацию статических биометрических систем по используемому биометрическому признаку.

1) Биометрические системы, использующие дактилоскопию

Дактилоскопическая аутентификация — это процесс установления тождества человека с использованием отображений уникального папиллярного узора пальцев человека.

Существуют два вида признаков по которым происходит распознавание папиллярных линий пальца, это — по отдельным деталям (характерным точкам) и по рельефу всей поверхности пальца, а также по их комбинациям. [6]

В биометрических системах, использующих дактилоскопию, конструктивно различают следующие виды сканеров, применяемых для аутентификации по отпечатку

пальца.



Рис.3. Виды сканеров, наиболее часто применяемых в биометрических системах, использующих дактилоскопию (по конструкции)

По используемой технологии сканеры бывают следующих видов:

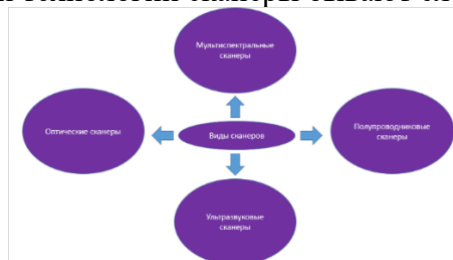


Рис.4. Виды сканеров, применяемых в биометрических системах, использующих дактилоскопию (по используемой технологии)

Рассмотрим более подробно каждый из видов дактилоскопических сканеров.

- Оптический сканер

Применение оптического сканера основывается на использовании оптических методов получения изображения. [7] Существуют следующие основные технологии реализации оптических сканеров: • FTIR-сканеры; • Электрооптические сканеры; • Оптоволоконные сканеры; • Оптические протяжные сканеры; • Роликовые сканеры; • Бесконтактные-сканеры. [8]

Самыми распространенными из них являются контактные FTIR-сканеры, в которых используется эффект «нарушения полного внутреннего отражения» (от англ. Frustrated Total Internal Reflection).

- Полупроводниковые сканеры

В полупроводниковых сканерах для получения отображения папиллярных узоров пальцев используют изменение свойств полупроводников в местах контакта гребней папиллярного узора с поверхностью сканера. В настоящее время существуют следующие технологии реализации полупроводниковых сканеров: • Емкостные сканеры; • Емкостные протяжные сканеры; • Чувствительные к давлению сканеры; • Термо-сканеры; • Протяжные термо-сканеры; • Радиочастотные сканеры; • Радиочастотные протяжные сканеры.

Емкостные сканеры — наиболее широко распространенный тип полупроводниковых дактилоскопических сканеров, в которых для получения отображения отпечатка пальца используется эффект изменения емкости рп-перехода полупроводникового прибора при соприкосновении гребня папиллярного узора с элементом полупроводниковой матрицы. [8]

- Ультразвуковые сканеры

Ультразвуковые дактилоскопические сканеры используют для создания визуального отображения папиллярных линий пальца те же принципы, что и медицинское УЗИ. Звуковые волны в данных устройствах генерируются с помощью пьезоэлектрических преобразователей, а отраженная энергия улавливается с помощью пьезоэлектрических

материалов.

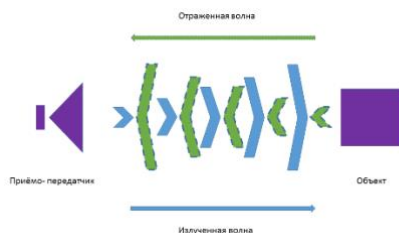


Рис.5. Принцип работы ультразвукового сенсора

- Мультиспектральные сканеры.

Сенсоры MSI обеспечивают возможность получения ряда снимков пальца при различных условиях освещения, включающих в себя разные длины волн, положение источника света и условия поляризации. [9] Это позволяет фиксировать фундаментальный «внутренний отпечаток пальца», со всеми его подкожными структурами и сосудами.

На данный момент мультиспектральное сканирование является одной из наиболее перспективных технологий, применяемых для целей биометрической аутентификации. Связано это с тем, что технология распознавания живых тканей использует передовые алгоритмы машинного обучения, способные обновляться при идентификации новых типов угроз и подделок. [10]

2) Биометрические системы, использующие аутентификацию по рисунку вен

Среди всего многообразия средств биометрической аутентификации следует отметить высокий потенциал развития систем, в основе работы которых лежат механизмы распознавания рисунка кровеносных сосудов в ладони или пальце руки пользователя. [11]

Технология биометрической аутентификации по венозному рисунку основывается на оптической визуализации вен человека для их дальнейшего распознавания. При этом венозный рисунок ладони является достаточно сложным и позволяет достичь оптимальную точность процедуры распознавания.

Существует два метода получения изображения рисунка вен ладони: метод отражения (от англ. Reflection) и метод пропускания ИК-света (от англ. Transmission).

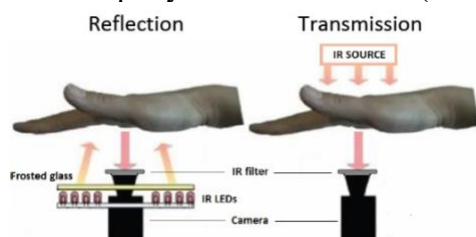


Рис.6. Сравнение метода отражения и метода пропускания ИК-света

Значительно чаще в технологиях биометрической аутентификации по рисунку вен используется метод считывания отраженного ИК-света. При реализации данного метода используется оптическая система, включающая в себя камеру без инфракрасного (ИК) фильтра, ИК светодиоды и ИК светофильтр, пропускающий только излучение, соответствующее длине волн ИК светодиодов. Для получения отображения рисунка вен пользователя поверхность его ладони освещается ИК светодиодами. Так как гемоглобин, содержащийся в крови человека, имеет свойство поглощать ИК излучение, а другие ткани – отражать, то от венозных сосудов ладони отражается излучение меньшей интенсивности, что и улавливает чувствительная камера. Соответственно, месторасположение вен на снимке выглядит как темная область. Далее специальная программа на основе полученных данных создает цифровую свертку. [12] И в последствии эта свертка используется для

сравнения с эталонной, хранящейся в базе данных, для аутентификации пользователя.

Распознавание по венам ладони — инновационный и динамично развивающийся способ, точность которого признана одной из самых высоких на данный момент. И.С. Беров, директор по цифровой идентичности ПАО «Ростелеком», одного из главных участников рынка цифровых услуг, заявил о планах на внесение в 2020 году в единую биометрическую систему (ЕБС) нового слежка — рисунка вен ладони. В настоящее время в ПАО «Ростелеком» ведутся пилотные проекты по применению биометрии в транспортной отрасли, МФЦ, нотариате и т.д.

3) Биометрические системы, использующие аутентификацию по сетчатке глаза

Сетчатка — это фоточувствительный слой, расположенный на внутренней поверхности глазного яблока и содержащий взаимосвязанные нейроны и фоторецепторы, чувствительные к воздействию световой энергии.

Сканирование сетчатки обычно происходит с использованием ИК излучения низкой интенсивности, направленного через зрачок к кровеносным сосудам задней стенки глаза. [13] В современных сканерах часто применяют лазеры мягкого действия.

Сканирование глазного дна выполняется безопасным для глаз источником ИК излучения приблизительно за минуту. За это время биометрическая система успевает подсветить сетчатку, получить отраженный от ретины сигнал и зафиксировать отраженное излучение специальной чувствительной камерой. При этом малейшее движение или неправильная фокусировка на источнике света могут привести к отказу распознавания.

Принцип действия технологии аутентификации по сетчатке глаза основывается на том, что при проецировании невоспринимаемого глазом луча ИК света в глаз пользователя кровеносные сосуды сетчатки поглощают этот свет интенсивнее, чем остальные части глаза, и во время сканирования создается определенный узор, который преобразуется в компьютерный код, сохраняющийся затем в базе данных. Далее происходит сравнение полученного образца с установленным шаблоном.

4) Биометрические системы, использующие аутентификацию по радужке глаза

Радужная оболочка — это видимая невооружённым взглядом подвижная диафрагма глаза, расположенная между зрачком и склерой. Она представляет собой тонкую эллиптическую структуру глаза, которая путём рефлекторного сужения и расширения зрачка регулирует поток проникающих внутрь глаза световых лучей. «Цвет глаз» — это как раз цвет именно радужной оболочки глаза.

Как и папиллярный и венозный рисунки, радужная оболочка является фенотипической особенностью человека.

Распознавание радужной оболочки глаза представляет собой автоматизированный метод биометрической аутентификации, который использует математические методы для распознавания уникального рисунка радужной оболочки глаз того или иного человека.

Как и любой иной метод биометрической аутентификации данный метод разделяется на несколько этапов:

1. Получение биометрических данных (чаще всего с помощью технологии использования едва уловимой ИК подсветки).

2. Предварительная обработка (фильтрация изображения, улучшение контрастности, бинаризация изображения и выделение границ).

3. Извлечение признаков из биометрических данных (выделение частотной или какой-либо другой информации о текстуре радужки из изображения и сохранение этой информации в виде специального кода IrisCode).

4. Классификация биометрических образцов (идентификация) или сравнение с образцом (верификация). [14]

5 и 6) Биометрические технологии с системой распознавания лиц (2D и 3D)

Распознавание лиц (от англ. Face Recognition) — это практическое приложение теории

распознавания образов, в задачу которого входит автоматическая локализация лица на фотографии/в видеопотоке и, в случае необходимости, аутентификация личности. На данный момент биометрические технологии с системой распознавания лиц считаются одними из наиболее перспективных среди других технологий бесконтактной аутентификации человека.

Любая система распознавания лиц состоит как минимум из двух основных блоков: камеры видеонаблюдения и программного обеспечения, выполняющего анализ изображения/видеопотока. Автоматическая аутентификация личности с помощью программного обеспечения для распознавания лиц является комплексной процедурой, для которой требуются довольно сложные методы искусственного интеллекта и машинного обучения.

Системы распознавания лиц используются в приложениях для:

- 1) визуальной экспертизы изображения лица, полученного с камеры наблюдения с разрешением, достаточным для определения экспертом таких особенностей, которыми можно пользоваться для проверки личности (шрамы, родимые пятна, родинки, татуировки и т.п.);
- 2) визуальной верификации личности человека путем сравнения с эталонными изображениями лица;
- 3) автоматической биометрической идентификации лица (поиск «один ко многим»);
- 4) автоматической биометрической верификации лица (поиск «один к одному»).

Биометрические системы двумерного (2D) распознавания лиц являются на данный момент весьма востребованными из-за того, что все основные мировые базы данных лиц – именно двухмерные. Алгоритмы двумерного распознавания лиц используют: антропометрические параметры лица, графы – модели лиц или эластичные 2D-модели лиц, а также изображения с лицами, представленные некоторым набором физических или математических признаков. К ключевым недостаткам таких систем относится легкость фальсификации предъявляемых факторов признака (путем использования муляжей, фотографий, сценического макияжа и т.д.), а также зависимость от уровня освещенности и положения головы человека.

В свою очередь биометрические системы трехмерного (3D) распознавания лиц являются более перспективными, так как трехмерные модели предоставляют качественно большее количество материала для анализа. По этой причине такие системы обладают большей точностью и меньшим количеством ошибок по сравнению с двумерными системами распознавания лиц.

Существует несколько разнообразных технологий 3D сканирования. Например, применяются лазерные сканеры с оценкой дальности от сканера до элементов поверхности объекта, а также специальные сканеры со структурированной подсветкой поверхности объекта и математической обработкой изгибов полос или сканеры, обрабатывающие фотограмметрическим методом синхронные стереопары изображений лиц.

Соответственно, 3D (трехмерные) модели лица также могут создаваться различными способами, такими как проецирование ИК-сетки («структурированного света»), слияние нескольких изображений или использование информации о полутонах в отдельном изображении.

Основными недостатками технологии 3D распознавания лиц считаются:

- Более высокая стоимость специальных камер для трехмерного сканирования по сравнению со стандартными камерами видеонаблюдения, используемыми в 2D распознавании;
 - Невозможность распознавания близнецов;
 - Отсутствие готовых трехмерных баз данных лиц.
- На данный момент ведется активный поиск решения этой проблемы. Уже существуют два основных проекта по созданию трехмерной модели лица на основе 2D изображения: 3D-реконструкции лиц на основе одного двумерного

изображения лица (на базе нейросети) и 3D-реконструкции на основе двух двумерных изображений.

7) Биометрические системы, использующие секвенирование ДНК

Наибольшее распространение получили следующие методики секвенирования ДНК:

- метод Сэнгера (метод терминации цепи);
- пироксеквенирование (секвенирование путем синтеза);
- секвенирование на основе лигирования;
- секвенирование одиночных молекул;
- нанопоровое секвенирование.

Следует отметить, что на данный момент масштабное применение технологии секвенирования ДНК для систем контроля удаленного доступа, а также для многих других нецелесообразно из-за длительной процедуры аутентификации и ее высокой стоимости. Однако, существуют отдельные направления, для которых данная технология предоставляет уникальные возможности.

Интересно также изучить раздел динамической (поведенческой) биометрии. В поведенческой биометрии используется оценка индивидуальных психофизиологических (или эмоциональных) характеристик человека. [15]

К основным достоинствам динамических биометрических систем можно отнести: • отсутствие необходимости в дополнительных действиях пользователя (можно реализовать дополнительную аутентификацию на основе привычных пользователю рутинных действий); • простота внедрения и реализации; • возможность скрытного внедрения данного типа аутентификации (например, пользователь может и не подозревать, что проходит дополнительную проверку клавиатурного почерка).

Принцип действия поведенческих биометрических систем рассматривается на блок-схеме ниже:

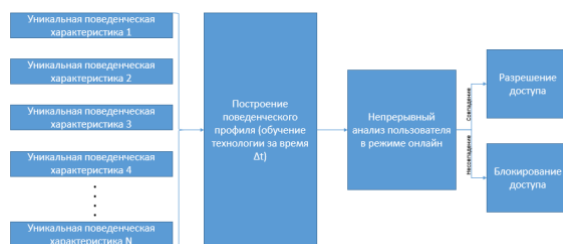


Рис.7. Принцип действия типовой технологии поведенческой биометрии

По используемому биометрическому признаку различают следующие основные динамические биометрические системы:

1) Биометрические системы, анализирующие динамику подписи. В качестве уникальных поведенческих характеристик в таких системах могут рассматриваться: угол наклона ручки, скорость движения ручки и акселерации, время написания, сила, с которой пишущий держит ручку, то, сколько раз ручка отрывалась от бумаги, а также иные;

2) Биометрические системы, анализирующие работу на клавиатуре (динамику/ритм нажатия клавиш, параметры движения курсора мыши, силу прикосновения к сенсорному экрану, частоту возникновения ошибок при вводе, угол наклона экрана, глубокие связи между набором разных символов и задержки при вводе этих символов и т.д.). Анализ может производиться как по набору свободного текста, так и по ключевой фразе. На сегодняшний день современные алгоритмы, разработанные компанией Smart Security, могут обрабатывать более 150 измеримых поведенческих характеристик.

3) Биометрические системы, анализирующие голос. Аутентификация по голосу может осуществляться либо текстонезависимым, либо текстозависимым методом. При этом во многих системах анализ производится не только по особенностям голоса, зависящим от

физиологических особенностей гортани, но и по эмоциональным характеристикам речи;

4) Биометрические системы, анализирующие походку. Технология распознавания походки является относительно редкой, и до недавнего времени она существовала только в экспериментальных воплощениях. Однако, недавно в университете Осака было разработано программное обеспечение, работающее с последовательностью кадров, импортированных из системы видеонаблюдения. Данное ПО осуществляет анализ походки по определенным характерным движениям ног, рук и туловища пользователя.

5) Биометрические системы, анализирующие мимику (FACS), и другие.

В настоящий момент компанией Neurobotics создан программный комплекс высокоточного определения эмоций на базе нейронных сетей EmoDetect. В реализованной поведенческой системе используется система кодирования лицевых движений (FACS), алгоритмы индивидуальной общей корректировки (IGCA) на основе нейтрального эмоционального состояния (включая нейронную сеть, обученную на имеющихся базах), а также алгоритмы индивидуальной частной корректировки на основе конкретного ложного эмоционального состояния (IPCA). Сейчас разработчиками проводится пилотное тестирование для оценки эффективности работы программного комплекса. [16]

Следует понимать, что поведенческая биометрия является относительно новой ветвью биометрии, поэтому на сегодняшний день она активно развивается, но при этом остается актуальным вопрос оценки надежности ее методов.

Помимо статических и динамических биометрических систем в настоящее время становятся все более распространенными мультибиометрические технологии распознавания. Они применяются для улучшения качества автоматического распознавания личности и технических характеристик системы, а также для снижения уровня риска. Основное достоинство мультибиометрических технологий заключается в том, что они обрабатывают большее количество информации о субъекте, проходящем аутентификацию. [17]

Различают следующие категории мультибиометрических систем:

1) Мультихарактеристиковая (использует данные от нескольких типов биометрических характеристик);

2) Мультиэкземплярная (использует несколько разных биометрических экземпляров для одного единственного типа биометрической характеристики, например, рисунки папиллярных линий нескольких пальцев);

3) Мультидатчиковая (использует несколько различных датчиков для сбора биометрических образцов одного биометрического экземпляра, например, пару датчиков для получения кадров в разных диапазонах длин волн);

4) Мультиалгоритмическая (использует несколько различных алгоритмов для обработки одного биометрического образца);

5) Мультипредъявление (использует несколько различных предъявлений биометрических образцов одного экземпляра биометрической характеристики).

Все представленные выше категории мультибиометрических систем способствуют снижению вероятности фальсификации биометрических признаков, поэтому мультибиометрические решения открывают широкие перспективы для дальнейших научных исследований.

При создании мультибиометрической технологии добавление нового модуля может выполняться на любом из этапов обработки. Выделяют следующие основные уровни объединения:

1) Уровень образцов;

2) Уровень признаков;

3) Уровень степеней схожести;

4) Уровень принятия решения.

При осуществлении объединений на уровне образцов или уровне извлечения признаков формируется объединенный шаблон, содержащий большее количество признаков. Однако, данные типы объединений также требуют больших финансовых и технологических затрат. Поэтому на практике наиболее часто реализуется объединение технологий на уровне принятия решения. [18]

Существуют два наиболее простых способа формирования совместного решения:

1) Правило конъюнкции (логическое "И" / "&");

2) Правило дизъюнкции (логическое "ИЛИ" / "||"). [19]

Для того, чтобы вероятность ошибки ложного доступа для мультибиометрической системы была ниже, чем вероятности ошибок второго рода для исходных технологий следует руководствоваться правилом конъюнкции. При применении данного правила ошибка ложного доступа (т.е. ошибка второго рода) может возникнуть только в том случае, если решением обеих технологий будет предоставление ложного доступа. Таким образом, объединенная вероятность ошибки ложного доступа без учета корреляции является произведением вероятностей ошибок отдельных технологий. Однако, при создании мультибиометрической технологии стоит учитывать взаимосвязь ошибок классификаторов. Для вычисления корреляции ρ_{nc} на уровне принятия решения используют формулу:

$$\rho_{nc} = \frac{n \times N_c^f}{N + n \times N_c^f - N_c^f - N_c^t} \quad (1)$$

где n – общее число тестируемых классификаторов;

N – общее число входных данных;

N_c^f – число входных данных, ошибочно классифицируемых всеми классификаторами при использовании порога C ;

N_c^t – число входных данных, правильно классифицируемых всеми классификаторами при использовании порога C .

Следует учитывать, что в соответствии с соотношением вероятностей ошибок первого и второго рода, вероятность ложного недопуска при использовании правила конъюнкции, оказывается выше, чем для каждой технологии по отдельности.

Для достоверной оценки ошибок первого и второго рода мультибиометрической системы целесообразно выполнение полноценных испытаний.

Испытания биометрических технологий целесообразно проводить по следующим ГОСТ:

- ГОСТ Р ИСО/МЭК 19795-1–2007
- ГОСТ Р ИСО/МЭК 19795-2–2008
- ГОСТ Р ИСО/МЭК ТО 19795-3–2009
- ГОСТ Р ИСО/МЭК 19795-4–2011
- ГОСТ Р ИСО/МЭК 19795-6–2015 [20]

Выводы

В рамках проведенного научного исследования нами были рассмотрены основные виды биометрических систем и принципы их функционирования. На основании вышеизложенного можно сделать следующие выводы:

• Биометрические системы на данный момент являются одной из наиболее динамично развивающихся технологий. Связано это с тем, что в отличие от факторов владения и факторов знания биометрические характеристики не могут быть забыты или потеряны, их трудно фальсифицировать (некоторые невозможно на данном этапе) и практически

невозможно изменить (некоторые абсолютно невозможно);

- Современные биометрические системы решают два класса задач: задачи верификации и задачи идентификации;

- По используемому биометрическому признаку на данный момент выделяют 7 основных видов статических биометрических систем. Это системы, использующие дактилоскопию, двухмерное (2D) распознавание лиц, трехмерное (3D) распознавание лиц, секвенирование ДНК, а также аутентификацию по рисунку вен, по сетчатке глаза и по радужке глаза. Наиболее надежными зарекомендовали себя биометрические системы, использующие мультиспектральную дактилоскопию, секвенирование ДНК, аутентификацию по рисунку вен и по сетчатке глаза. Однако, их применение целесообразно лишь при повышенных требованиях к безопасности и к точности результата;

- По используемому биометрическому признаку среди динамических биометрических систем наиболее распространены системы, анализирующие динамику подписи, работу на клавиатуре, голос, походку и мимику. Поведенческая биометрия является относительно новой, перспективной ветвью биометрии, поэтому на сегодняшний день актуален вопрос оценки надежности ее методов;

- Помимо статических и динамических биометрических систем в настоящее время набирают популярность мультибиометрические технологии распознавания. Они применяются для улучшения качества автоматического распознавания личности и технических характеристик системы, а также для снижения уровня риска. Основное достоинство мультибиометрических технологий заключается в том, что они обрабатывают большее количество информации о субъекте, проходящем аутентификацию. Все категории мультибиометрических систем способствуют снижению вероятности фальсификации биометрических признаков, поэтому мультибиометрические решения открывают широкие перспективы для дальнейших научных исследований.

Выполненный в статье обзор, основывающийся на глубоком изучении научных работ по рассматриваемой проблематике, позволяет систематизировать основные достижения в сфере биометрических систем к настоящему времени, помогает сориентироваться в существующих технологиях и наметить дальнейшие пути их развития.

Литература

[1] Трунцевский Ю.В. Е-антикоррупция или е-коррупция: влияние глобальной цифровизации // Международное публичное и частное право. 2019. № 4. С. 42 – 48.

[2] Кузнецов Ю.В. Кriptoактивы как документарные ценные бумаги // Закон. 2018. № 9. С. 96 – 105.

[3] Тарапанова Е. А., Иванников П. В. Правовое регулирование криптовалют и их реализация на базе отечественных стандартов информационной безопасности // Наукоемкие технологии. 2018. Т. 19. № 11. С. 58 - 64.

[4] Рассолов И.М., Чубукова С.Г., Микурова И.В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex russica. 2019. № 1. С. 108 – 118.

[5] Платонова Н.И. Современные правовые подходы к пониманию биометрических данных // Информационное право. 2018. № 1. С. 22 – 26.

[6] Маркелов К.С. Идентификация и верификация личности – комплексная биометрическая информационная технология // International Journal of Open Information Technologies. 2015. № 5. С. 12 – 18.

[7] SecurityRussia. Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации [Электронный ресурс] // URL: <https://securityrussia.com/blog/biometriya.html> // (Дата обращения 03.11.2019)

[8] Национальная библиотека им. Н.Э.Баумана. Распознавание отпечатков пальцев [Электронный ресурс] // URL: https://ru.bmstu.wiki/index.php?mobileaction=toggle_view_mobile&title=Распознавание_отпечатков_пальцев# // (Дата обращения 18.10.2019)

- [9] Гинце А.А. Мультиспектральная технология в дактилоскопических сенсорах [Электронный ресурс] URL: http://secuteck.ru/articles2/sys_ogr_dost/multispektralnaya-tehnologiya-v-daktiloskopicheskikh-sensorah // (Дата обращения 18.10.2019)
- [10] Горшков А. Эволюция мысли: новые биометрические разработки [Электронный ресурс] // URL: http://secuteck.ru/articles2/sys_ogr_dost/evolyutsiya-mysli-novye-biometricheskie-razrabotki/ // (Дата обращения 07.11.2019)
- [11] Безик О.В., Басараб М. А. Разработка и анализ алгоритма биометрической аутентификации по рисунку кровеносных сосудов пользователя // Молодой ученый. 2016. № 8. С. 116-119 [Электронный ресурс] // URL <https://moluch.ru/archive/112/28527/> // (Дата обращения: 01.04.2020)
- [12] Баранов С.О., Абрамов Д.Б. Технология биометрической аутентификации пользователя по венозному рисунку кистей // Вестник СибАДИ. 2017. № 2(54). С.134-139
- [13] Ворона В.А., Костенко В.О. Биометрические технологии идентификации в системах контроля и управления доступом [Электронный ресурс] // URL: <https://cyberleninka.ru/article/n/biometricheskie-tehnologii-identifikatsii-v-sistemah-kontrolya-i-upravleniya-dostupom/pdf> // (Дата обращения: 27.04.2020)
- [14] Назарова Т.Ю., Лавров Д.Н. Компьютерное моделирование идентификации личности по радужной оболочке глаза на основе опенсв // Математические структуры и моделирование. 2018. № 3(47). С. 68–81
- [15] Анисимов Р., Мамаев В. Поведенческая биометрия заменит пароли [Электронный ресурс] // URL: http://secuteck.ru/articles2/sys_ogr_dost/povedencheskaya-biometriya-zamenit-paroli/ // (Дата обращения 09.03.2019)
- [16] Neurobotics EmoDetect [Электронный ресурс] // URL: <https://neurobotics.ru/en/catalog/psychophysiology/emotion-detection-software-emodetect/> // (Дата обращения 04.03.2019)
- [17] Coderlessons. Мультимодальные биометрические системы [Электронный ресурс] // URL: <https://coderlessons.com/tutorials/akademicheskii/uchites-biometrii/multimodalnye-biometricheskie-sistemy> // (Дата обращения: 17.04.2020)
- [18] Сесин Е.М., Белов В.М. Системы идентификации личности, основанные на интеграции нескольких биометрических характеристик человека [Электронный ресурс] // URL: <https://cyberleninka.ru/article/n/sistemy-identifikatsii-lichnosti-osnovannye-na-integratsii-neskolkih-biometricheskikh-harakteristik-cheloveka> // (Дата обращения: 21.04.2020)
- [19] Кручинина Е., Николаев Д. Особенности мультибиометрических технологий [Электронный ресурс] // URL: http://secuteck.ru/articles2/sys_ogr_dost/osobennosti-multibiometricheskikh-tehnologiy // (Дата обращения: 21.04.2020)
- [20] Мамаев В. Журнал «Технологии Защиты». Биометрические СКУД [Электронный ресурс] // URL: <http://www.techportal.ru/251949> // (Дата обращения: 27.04.2020)

Biometric authentication technologies

Tarapanova E.A.¹⁹⁵, Boyko E.V.¹⁹⁶

Abstract. *This article is dedicated to the actual aspects of biometric authentication technologies. The authors reviewed the existing biometric authentication technologies and considered their application fields. The classification of biometric systems according to the biometric features used in them is given in the text below. There was also made the analysis of main static biometric systems and their operation principles. Either it was scrutinized the operation principle of the behavioral biometry and were investigated the main dynamic biometric systems. The authors carried out a research of different categories of multi-biometrics systems, and technology fusion levels and ways of forming a joint decision in them as well. In summery are given the conclusions on the topic.*

Keywords: *biometry, physiological and behavioral characteristics of biometric data, identification, verification, biometric feature, dactyloscopy, two-dimensional and three-dimensional face recognition, DNA sequencing, multi-biometrics systems.*

¹⁹⁵ Helena Tarapanova, Ph.D. in Philosophy, Associate Professor of Information Security, Bauman Moscow State Technical University, Moscow, tarapanova@bmstu.ru

¹⁹⁶ Katerina Boyko, graduate of the department Information Security, Bauman Moscow State Technical University, Moscow, boykokate@mail.ru

Обзор компьютерных атак на биометрические системы

Татаренков В.С.¹⁹⁷

Аннотация. В данной статье описано общее устройство биометрических систем аутентификации. Приведена классификация атак на биометрические системы аутентификации по преследуемым злоумышленниками целям. Освещены примеры атак с учетом современных трендов в киберпреступности. Приведено описание основных методов защиты биометрических систем аутентификации, которые необходимо использовать при построении и разработке современных биометрических систем аутентификации для обеспечения их должной безопасности.

Ключевые слова: биометрические системы, аутентификация, информационная безопасность.

Введение

Биометрические системы аутентификации за последние годы получили широкое распространение в своем применении [1-7]. В качестве примеров такого роста популярности использования биометрических систем можно привести: создание проекта ЕБС¹⁹⁸ для обеспечения предоставления клиентам банков финансовых услуг, доступ к которым будет осуществляться после прохождения биометрической аутентификации по лицу и голосу¹⁹⁹; введение властями Москвы проекта, позволяющего оплачивать проезд в московском метрополитене при помощи функции распознавания лица²⁰⁰; появление возможности оплачивать покупки при помощи систем распознавания лица в крупных сетях супермаркетов Москвы²⁰¹ и т.д.

Так как биометрические системы аутентификации используются в качестве СКУД²⁰² для организации доступа к критически важной инфраструктуре (защищенные помещения, серверные и т.д.) или к сервисам, позволяющим выполнять критически важные действия (банковские услуги, АСУ ТП²⁰³ на опасных предприятиях и производствах), то при их построении необходимо учитывать текущие тенденции в сфере обеспечения безопасности биометрических систем аутентификации.

В данной статье рассматриваются основные угрозы и атаки на системы биометрической аутентификации пользователя, которые были выявлены на сегодняшний день в процессе эксплуатации подобного рода систем, а также методы защиты от данных атак.

1. Общее устройство биометрических систем аутентификации и возможные направления атак

На современном рынке биометрических систем идентификации и аутентификации представлено большое разнообразие систем, основное различие между которыми заключается в использовании разных биометрических данных, которые подлежат проверке при прохождении процесса идентификации и аутентификации. На основе данного критерия

¹⁹⁷ Татаренков В.С., студент 1 курса аспирантуры, Финансовый университет при Правительстве РФ, Москва

¹⁹⁸Здесь и далее: ЕБС - единая биометрическая система

¹⁹⁹ <https://bio.rt.ru/>

²⁰⁰ https://www.rbc.ru/technology_and_media/02/09/2020

²⁰¹ <https://www.rbc.ru/finances/10/03/2021>

²⁰²Здесь и далее: СКУД - система контроля и управления доступом

²⁰³Здесь и далее: АСУ ТП - автоматизированная система управления технологическим процессом

можно выделить системы, использующие в своей основе распознавание: лица, голоса, отпечатка пальца, радужной оболочки глаза, венозной карты ладони и т.д. Несмотря на такое разнообразие систем, их общее устройство и архитектуру построения можно представить в качестве следующей схемы, см. рис. 1.



Рисунок 1 - Обобщенная схема устройства биометрических систем аутентификации

Обобщенная схема устройства биометрических систем аутентификации отражает следующий принцип работы данных систем, а именно: на вход модуля ввода, который выступает в качестве устройства-датчика, считывающего биометрические данные (сканер отпечатков пальцев, видеокамера и т.д.), принимаются биометрические данные пользователя, проходящего процесс идентификации и аутентификации. Далее эти биометрические данные передаются в модуль выделения характеристик, где происходит их первичная обработка и подготовка к тому виду, который необходим для правильного функционирования модуля сравнения. Затем, подготовленные данные передаются в модуль сравнения, который связан с базой данных пользователей. В данном модуле происходит основная работа функционирующего в системе алгоритма распознавания, в качестве которого могут выступать различные алгоритмы (eigenfaces алгоритм, DTW²⁰⁴ алгоритм и т.д.) или нейронные сети (сверточные нейронные сети и т.д.). После выполнения алгоритмом распознавания и сравнения информации, полученной от пользователя, и информации, полученной из базы данных, принимается решение о формировании положительного или отрицательного результата прохождения пользователем процесса аутентификации, которое в дальнейшем передается на устройство или приложение для выполнения дальнейших действий по предоставлению/отказу доступа, индикации/информирования о результате прохождения процесса аутентификации и т.д.

На данной схеме цифрами обозначены места, где злоумышленники могут произвести атаку. Количество данных мест непосредственно зависит от реализации самой системы, так как некоторые модули могут быть объединены в одно устройство без использования физических каналов связи между ними. На обобщенной схеме устройства биометрических систем аутентификации выделяется 9 мест для проведения возможных атак: 1 - модуль ввода; 2 - модуль выделения характеристик; 3 - модуль сравнения; 4 - приложение; 5 - база данных; 6,7,8,9 - каналы связи между модулями [7].

2. Основные современные атаки на биометрические системы

Перед описанием основных атак на биометрические системы приведем классификацию данных атак по преследуемым злоумышленниками целям.

²⁰⁴Здесь и далее: DTW - dynamic time wrapping

Спуфинг атаки (Spoofing attacks)

Основной целью данного типа атак является выдача себя злоумышленником за пользователя, у которого имеется легальный доступ к системе. Подобного рода атаки в основном производятся с использованием искусственно созданных (синтетических) копий или же фальсификатов биометрических данных атакуемого пользователя [8].

Биометрическая обфускация (Biometric obfuscation)

Подобные типы атак направлены на маскировку или фальсификацию предоставляемых системе биометрических данных с целью сделать невозможным корректное распознавание человека, проходящего процесс аутентификации. Данный тип атак преимущественно используется преступниками, которые находятся в розыске, для предотвращения своего обнаружения системой распознавания. Для реализации данного типа атак применяется два основных подхода: физическое изменение собственных биометрических данных и использование методов, которые относятся к спуфинг атакам.

Отказ в обслуживании (Denial of Service)

Цель данного типа атаки — это ухудшить качество работы системы или же остановить ее работу полностью. Система, подвергшаяся успешному нападению при помощи данного типа атак, не позволяет легитимным пользователям использовать ее в обычном штатном режиме. К данному типу атак прибегают в случаях, когда необходимо вывести систему из строя, шантажировать владельца атакуемой системы, а также в качестве ведения нечестной конкурентной борьбы. Простая методология выполнения данного типа атаки — это отправка большого объема "мусорных" данных с большой степенью зашумленности на вход системы, что существенно замедлит работу системы, которая будет полностью или частично занята обработкой данной "пустой" информации.

Предварительный сговор или принуждение

При осуществлении атаки на биометрическую систему по предварительному сговору или по принуждению, легитимный пользователь облегчает доступ к системе злоумышленникам путем своего прохождения процесса аутентификации и дальнейшей передачи возможности доступа злоумышленникам. Особенностью данного типа атак является то, что легитимный пользователь сам участвует в процессе аутентификации, следовательно, распознать атаку подобного типа очень сложно, так как все предоставленные системе биометрические данные верны и были зафиксированы и взяты от самого пользователя без применения различного рода фальсификатов, синтетических копий и т.д.

На протяжении всего времени своего существования и эксплуатации биометрические системы подвергались различным атакам со стороны злоумышленников. Опишем далее основные атаки и современные тенденции их развития.

Самой известной и преданной широкой огласке общественности является атака "ложной биометрией" (точка 1 на рисунке 1) с применением фальсификатов, изготовленных при помощи полученных сведений о биометрических данных легитимных пользователей на различных физических носителях [9]. Распространенности данного типа атак способствовало то, что при проведении такой атаки нет необходимости знать архитектуру и устройство реализации системы, а также иметь какой-либо физический доступ к ее узлам, за исключением штатного доступа к модулю ввода биометрических данных. В качестве примеров фальсификатов для проведения подобной атаки можно привести следующие:

фотографии, видео, запись голоса, объемная маска-накладка и т.д. С течением времени и развитием биометрических систем, фальсификаты также претерпевали изменения в сторону улучшения качества подделки, усложнения в производстве и увеличении времени для подготовки к проведению атаки. На текущий момент примерами современных фальсификатов, которые представляют опасность для биометрических систем и сохраняют актуальную угрозу прохождения их аутентификации, являются: изготовленные на тонкой проводящей тепло и ток тела силиконовой основе отпечатки пальцев²⁰⁵, объемные маски-накладки, "оживленные" с помощью современных технологий искусственного интеллекта фотографии атакуемых пользователей и т.д. Также данному типу атак посвящен стандарт ISO/IEC 30107-1 [4, 10, 11].

Следующими типами атак для рассмотрения являются вмешательство в процесс выделения характеристик из полученных биометрических данных (точка 2 на рисунке 1) и атака на алгоритм сравнения (точка 3 на рисунке 1). Схожесть данных типов атак заключается в том, что в обоих случаях атаке подвергаются функционирующие в модулях алгоритмы. Вмешательство в процесс выделения характеристик нацелено на то, чтобы алгоритм выделения характеристик сгенерировал на выходе желаемые признаки, которые в дальнейшем будут переданы системой в модуль сравнения, или же на то, чтобы помещать алгоритму правильно функционировать. Вмешательство в процесс сравнения нацелено на то, чтобы алгоритм сравнения произвел ту операцию, которая необходима злоумышленнику, а именно, выдачу злоумышленником себя за другого человека и т.д. На текущий момент существуют следующие современные атаки подобного типа: атаки с применением алгоритма Hill climbing attacks, атаки с применением алгоритма Fast Gradient Sign Method [12], атаки на основе состязательных атак (Adversarial attacks)²⁰⁶. Данные атаки способны обмануть функционирующие алгоритмы выделения признаков и сравнения с помощью набора синтетически сгенерированных данных. При генерации данного набора данных учитываются глубинные особенности функционирования нейронных сетей, которые часто применяются в биометрических системах аутентификации пользователей, и формируются так называемые DeepFake-шаблоны данных, способные обмануть систему²⁰⁷.

Следующий необходимый для рассмотрения тип атак - это атаки, направленные на базу данных пользователей биометрической системы (точка 5 на рисунке 1). К данному типу атак относятся: изменение биометрических данных пользователей в самой базе данных (нарушение их целостности), регистрация (добавление) нелегального пользователя. При проведении данного типа атак злоумышленникам необходимо учитывать архитектуру базы данных, учитывать, является ли она централизованной или распределенной, а также, используются ли в ней какие-либо технологии резервного копирования или зеркалирования.

Следующим типом атак, которые необходимо учитывать при построении биометрических систем, являются атаки на каналы связи между модулями (точки 6, 7, 8, 9 на рисунке 1), направленные на внедрение ложных пакетов данных, а также на изменение или повторное использование легитимных пакетов данных, курсирующих в биометрической системе. Особенно стоит обратить внимание на атаку в точке 8 на рисунке 1, так, если злоумышленник имеет возможность изменить окончательный результат процесса аутентификации, то это делает бесполезным существование самой системы аутентификации в целом. Ярким примером такого рода атак являются BlackBox атаки,

²⁰⁵ <https://www.kaspersky.ru/blog/sas2020-fingerprint-cloning/28101/>

²⁰⁶ <https://habr.com/ru/company/dsec/blog/437092/>

²⁰⁷ ²⁰⁷ <https://plusworld.ru/daily/tehnologii/ot-biometricheskih-mifov-k-biometricheskoj-realnosti/>

направленные на взлом и обход систем аутентификации в банкоматах. По статистике от одной такой успешной атаки ущерб может составить от 2 до 5 млн. рублей²⁰⁸.

Также опасность для биометрических систем аутентификации представляют атаки, направленные на повторное использование оставшихся данных и информации после процесса аутентификации (оставшиеся временные файлы, частично оставшиеся фрагменты данных от использовавшихся файлов и т.д.). Для выполнения данных атак требуется наличие физического доступа к оборудованию, функционирующему в составе системы биометрической аутентификации пользователя. Основной целью злоумышленника становятся оставшиеся временные файлы или фрагменты удаленных основных файлов, которые ранее использовались в процессе аутентификации пользователя. Сбор и анализ подобного рода файлов может позволить злоумышленнику в дальнейшем выполнять атаки на биометрические системы аутентификации.

3. Основные методы защиты биометрических систем аутентификации

При построении и разработке биометрической системы аутентификации необходимо учитывать текущие тенденции в области информационной безопасности, используемые для обеспечения высокого уровня защищенности биометрических систем. Рассмотрим следующие из них:

Многофакторная аутентификация. В данном случае процесс аутентификации происходит с предъявлением пользователем нескольких факторов аутентификации помимо основного фактора свойства (биометрии), среди которых также фактор знания (ПИН-код) и фактор владения (токен).

Аутентификация на основе объединения нескольких биометрических данных. Данный метод защиты биометрических систем подразумевает, что при прохождении аутентификации, пользователь предоставляет несколько типов биометрических данных. Примером такой системы может служить биометрическая система аутентификации по лицу и голосу.

Аутентификация на основе запроса случайных данных биометрии. Основная идея данного механизма аутентификации состоит в том, что у пользователя запрашиваются биометрические данные в случайном порядке, например: запрошенные в случайном порядке отпечатки пальцев при аутентификации по отпечаткам пальцев, произношение случайной фразы при аутентификации по голосу и т.д. Повышение безопасности связано с тем, что злоумышленнику необходимо иметь возможность правильно воспроизвести все возможные данные, которые могут быть запрошены у пользователя.

Аутентификация с использованием механизма обнаружения "жизни" образца (Life Detection). Данный механизм используется для предотвращения спуфинг атак с использованием синтетических, искусственно созданных копий биометрических данных атакуемого пользователя²⁰⁹. Примерами такого механизма являются: датчики температуры, датчики обнаружения капилляров для проверки отпечатков пальцев, датчики определения количества выделяемого воздуха во время произношения пароля, что позволяет определить живого человека от микрофона, и т.д.

Анализ защищенности внутренних алгоритмов системы. Данный метод заключается в том, чтобы проанализировать устойчивость алгоритмов, построенных на основе

²⁰⁸ <https://www.banki.ru/news/lenta/?id=10424133>

²⁰⁹ <https://habr.com/ru/company/trendmicro/blog/469533/>

технологий Deep Learning, которые будут функционировать в будущей биометрической системе аутентификации, к атакам с применением технологий DeepFake.

Обеспечение безопасного хранения данных. Данный метод защиты биометрических систем заключается в том, что при организации хранения эталонных шаблонов биометрических данных зарегистрированных пользователей необходимо обеспечивать их безопасность, а также необходимо иметь в виду, что при функционировании модулей системы, хранится определенная временная информация для выполнения процесса аутентификации, которую потом необходимо удалять.

Использование криптографии и шифрования при передаче пакетов данных. Шифрование пакетов данных, циркулирующих в системе по каналам связей, и использование имито-вставок позволяют защитить систему от атак, связанных с их чтением, анализом и записью, а также предотвратить возможность злоумышленнику осуществить атаку "человек посередине" (man in the middle).

Использование стандартов. Для построения защищенной биометрической системы необходимо следовать указаниям, описанным в стандартах. Примерами стандартов в области информационной безопасности, затрагивающих тематику биометрических систем являются: ГОСТ Р ИСО/МЭК 19794-13, ГОСТ Р ИСО/МЭК 19795, ГОСТ Р 52633.0-2006, ГОСТ Р ИСО/МЭК 30107 в трех частях, ГОСТ Р ИСО/МЭК 19794-8-2009 [3, 13, 14]. А также необходимо соблюдение законодательства, регулирующего отношения в области использования персональных данных пользователей: Конституция РФ, Гражданский кодекс РФ, ФЗ №152 «О персональных данных», приказ ФСБ РФ №771 от 16 декабря 2016 г., приказ ФСТЭК №31 от 14 марта 2014 г., приказ ФСТЭК №21 от 18 февраля 2013 г. и т.д.

Обучение и осведомление персонала. Персонал, который будет работать с биометрической системой, необходимо обучать для снижения вероятности совершения им ошибки, которая может повлечь нанесение серьезного ущерба безопасности.

Обеспечение физической безопасности модулей биометрической системы. Данный метод необходим для предотвращения получения физического доступа злоумышленником к узлам биометрической системы.

Выводы

Биометрические системы аутентификации все больше находят свое применение в жизни человека, в том числе и в повседневной. Подобного рода системы испытывают на себе всевозможные атаки со стороны злоумышленников на протяжении всего времени своего существования, что подтверждается регулярно публикуемыми результатами статистики. Также необходимо учитывать тот факт, что большинство биометрических данных, в первую очередь таких, как лицо и голос, может быть легко скомпрометировано; в свою очередь, пользователь, подвергшийся атаке и чьи биометрические данные были раскрыты, не имеет возможности изменить эти данные также просто, как стандартный пароль. Поэтому решение проблемы безопасности биометрических систем аутентификации является важной и приоритетной задачей для разработчиков подобного рода систем.

На сегодняшний день специалистами в сфере информационной безопасности разработаны методы защиты биометрических систем, которые, при их использовании и соблюдении, позволяют создать серьезно защищенную биометрическую систему. Для разработки защищенной биометрической системы аутентификации необходимо

комплексно подходить к вопросу ее защиты, любая халатность при проектировании системы может повлечь в будущем серьезную угрозу безопасности и ущерб.

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. Грижебовская А.Г., Михалев А.В. Биометрический метод идентификации человека по сосудистому рисунку пальца // Вопросы кибербезопасности. 2019. №5(33). С. 51-56.
3. Крутохвостов Д.С., Хиценко В.Е. Парольная и непрерывная аутентификация по клавиатурному почерку средствами математической статистики // Вопросы кибербезопасности. 2017. № 5 (24). С. 91-99.
4. Ложников П.С., Сулавко А.Е., Бурая Е.В., Писаренко В.Ю. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица // Вопросы кибербезопасности. 2017. № 3 (21). С. 24-34.
5. Математические основы информационной безопасности/Басараб М.А., Булатов В.В., Булдакова, Т.И., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г., Медведев Н.В., Троицкий И.И., Чичварин Н.В. и др.: Под ред. Матвеева В.А. -М.: НИИ РИЛ МГТУ им.Н.Э.Баумана, 2013. -244 с.6
6. Соков Б.Б. Создание прототипа системы биометрической аутентификации по геометрии лица с помощью методов машинного обучения. В сборнике: Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 175-178.
7. Serratos F. Security in biometric systems [Электронный ресурс] URL: <https://arxiv.org/ftp/arxiv/papers/2011/2011.05679.pdf> (дата обращения: 17.03.2021).
8. Калиновский И.А., Лаврентьева Г.М. Обнаружение спуфинг-атак на систему лицевой биометрии [Электронный ресурс] URL: <https://www.graphicon.ru/html/2018/papers/204-207.pdf> (дата обращения: 20.03.2021).
9. Николаев Д., Кручинина Е. Нападение и защита от атак в биометрии [Электронный ресурс] URL: http://lib.secuteck.ru/articles2/sys_ogr_dost/napadenie-i-zaschita-ot-atak-v-biometrii (дата обращения: 20.03.2021).
10. Федотенко М. Технология защиты от угрозы подмены биометрического сканера [Электронный ресурс] URL: <https://ib-bank.ru/bisjournal/post/819> (дата обращения: 21.03.2021).
11. Фаворская М.Н., Киба А.С. Атаки на системы биометрической идентификации и методы их выявления. В сборнике: Решетневские чтения. Материалы XXIV Международной научно-практической конференции, посвященной памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева: в 2 частях. 2020. С. 481-483.
12. Маршалко Г. Атаки на биометрические системы [Электронный ресурс] URL: <http://www.itsec.ru/articles/ataka-na-biometricheskie-sistemy> (дата обращения: 21.03.2021).
13. Николаев Д. Единые биометрические стандарты [Электронный ресурс] URL: <https://www.secuteck.ru/articles/edinye-biometricheskie-standarty> (дата обращения: 22.03.2021).
14. Герасименко В.Г., Кирсанов Ю.Г., Язов Ю.К. Особая роль национального стандарта РФ ГОСТ Р 52633-2006 в системе международных биометрических стандартов // Вопросы защиты информации. 2008. № 2 (81). С. 21-25.

Security of biometric authentication systems: basic attacks and protection against them

Tatarenkov V.S.²¹⁰

Abstract. *This article describes the general structure of biometric authentication systems. The classification of attacks on bio-metric authentication systems according to the purposes pursued by the cybercriminals is given. Examples of attacks taking into account modern trends in cybercrime are highlighted. The description of the main methods of protection of biometric authentication systems, which must be used in the construction and development of modern biometric authentication systems to ensure their proper security, is given.*

Keywords: *biometric systems, authentication, information security.*

²¹⁰ Tatarenkov V.S., 1-st year graduate student, Financial University under the Government of the Russian Federation, Moscow, vt96@mail.ru

Сравнительный анализ методик атрибуции кибератак Чеверкалов В.А.²¹¹

Аннотация. В последнее время для мирового сообщества задача правильного выявления ответственных за кибератаки или вредоносные кампании приобрела первостепенное значение. В рамках данной статьи представлено краткое описание существующих методик кибератрибуции, а также их сравнительный анализ, в результате которого была выявлена необходимость разработки новой методики атрибуции кибератак, поскольку существующие методики атрибуции не всегда дают однозначный результат и не совсем учитывают достоверность выявляемых артефактов (следов), что является первоочередным при наличии проблемы ложных флагов в киберпространстве.

Ключевые слова: кибербезопасность, информационная безопасность, атрибуция, кибератаки, киберпространство, хакерские группировки.

Введение

На сегодняшний день в связи с глобальной цифровизацией перед мировым сообществом остро стоит проблема кибератак, сложность и технологичность которых стремительно растет. Кроме того, кибератаки все чаще направлены на объекты критической инфраструктуры и преследуют цели кибершпионажа или саботажа, что создает угрозу национальной безопасности, подрывает государственный суверенитет и приводит к существенному экономическому, политическому, военному, технологическому ущербу [1]. Ввиду этого резко возросла актуальность правильного определения исполнителей кибератак в киберпространстве с целью привлечения их к ответственности.

Суть атрибуции

Пока не существует общепризнанного определения понятия атрибуции, также оно отсутствует в методических документах, стандартах и глоссариях регуляторов, сообществ и служб по защите информации [1]. Тем не менее, эксперты компании «Лаборатория Касперского» трактуют атрибуцию как совокупность организационно-технических мер, способствующих установлению исполнителей, стоящих за кибератакой или вредоносной кампанией. Атрибуция предполагает исследование следов киберпреступления и следственные действия правоохранительных органов на основании вывода аналитиков.

Методики атрибуции кибератак

Атрибуцию проводят компании, занимающиеся кибербезопасностью и спецслужбы, поэтому далее будут рассмотрены их методики атрибуции кибератак [4].

Специалисты из таких компаний как Group-IB, Лаборатория Касперского, FireEye, CrowdStrike проводят атрибуцию на основе методики, включающей следующие стадии: [2, 4]:

- 1) *Анализ вредоносного программного кода.* Позволяет выявить IP – адреса серверов атакующих, время компиляции и компоновки образца, пути к файлам отладки, ранее использованные участки кода с прошлых атак, а также язык в ОС, раскладка клавиатуры, язык комментариев в коде, на основе чего можно предположить страну атакующих. Еще анализируется функционал образца вредоносного ПО и оценивается его сложность.
- 2) *Анализ эксплойтов и уязвимостей.* Позволяет находить корреляцию между

²¹¹ Чеверкалов Владимир Александрович, студент, Финансовый университет при Правительстве РФ, Москва, v.cheverkalov@gmail.com

вредоносными атаками, особенно если в них были использованы уязвимости нулевого дня.

- 3) *Анализ инфраструктуры злоумышленников.* Выявляются использованные домены, субдомены, их страна регистрации, в ряде случаев вследствие дружеских отношений компаний по кибербезопасности с хостингами, в результате чего они могут прослушивать трафик определенных серверов, как это было с атрибуцией APT1, проведенной компанией FireEye, когда аналитикам разрешили записывать RDP – соединения на нескольких серверах [4].
- 4) *Анализ тактик, техник и процедур (ТТП), использованных в атаке в соответствии с матрицей MITRE ATT&CK.* MITRE ATT&CK – общедоступная обновляемая база данных, содержащая структурированную информацию о ТТП, используемых хакерскими группировками. Соответственно, по перечню ТТП можно определить вероятного исполнителя.
- 5) *Анализ временных меток.* По времени наибольшей активности хакерской группировки, компиляции и компоновки вредоносного ПО аналитики могут предположить, в каких часовых поясах находятся злоумышленники.
- 6) *Анализ целей группировки и геополитической и экономической ситуации.* Позволяет определить мотивацию атакующих на основании перечня вопросов: какой объект был атакован, в каком регионе он находится, какие политические конфликты там существуют, для кого украденная информация представляет экономический интерес.
- 7) *Разведка на основе общедоступных источников (OSINT).* Поиск и анализ информации на различных форумах, в том числе и хакерской тематики и в даркнете, а также в социальных сетях.
- 8) *Использование honeypot-систем.* Такие ложные системы могут быть атакованы злоумышленниками, в результате чего будут оставлены различные следы, к примеру, IP – адреса их серверов и т. д.
- 9) *Обратная трассировка IP – адресов.* Функционал ОС и маршрутизаторов, позволяющий воссоздать обратный маршрут до серверов атакующих и выявить промежуточные узлы, что позволяет приблизительно определить географическую принадлежность адреса.

Основная активность в сфере публичной атрибуции исходит от компаний по кибербезопасности. Тем не менее, заявления об авторстве со стороны правительства и спецслужб, в частности, считаются более авторитетными. Спецслужбы же используют следующую методику, во многом схожую с методами компаний по кибербезопасности [4]:

- 1) *Радиоэлектронная разведка,* позволяющая спецслужбам осуществлять перехват информации между определенными лицами и перехватывать интернет-трафик путем анализа и контроля точек обмена трафиком.
- 2) *Агентурная разведка).* Работа разведывательных агентств с информаторами и их вербовка в целях получения информации о проведенной атаке.
- 3) *Реализация наступательных кибер-операций.* В целях сбора нужной информации разведывательные службы могут взламывать информационные системы и персональные компьютеры. Так, в том же АНБ США существует специальное подразделение Tailored Access Operations (TAO), целью которого как раз является взлом компьютеров по всему миру, внедрение бэкдоров в аппаратное и программное обеспечение [4].
- 4) *Запросы к провайдерам.* В большинстве юрисдикций спецслужбы могут запрашивать информацию от Интернет-провайдеров, социальных сетей и почтовых сервисов, в результате чего можно получить IP – адреса, с которых было

подключение, почтовую переписку и контактные данные.

- 5) *Анализ общедоступных источников (OSINT).*
- 6) *Анализ вредоносного программного кода.*
- 7) *Анализ уязвимостей и эксплойтов.*
- 8) *Анализ инфраструктуры группы.*
- 9) *Анализ временных меток.*
- 10) *Анализ целей группировки и геополитической и экономической ситуации.*
- 11) *Анализ ТТП, использованных в атаке в соответствии с матрицей MITRE ATT&CK.*

Анализируя данные методики, можно выделить следующие утверждения:

– эффективней анализировать вредоносный код и временные метки способны компании по кибербезопасности, ведь их бизнес-модель предполагает разработку антивирусов и предоставление услуг по Threat Intelligence, вследствие чего у них накапливается огромная база вредоносного программного кода и индикаторов компрометации, что позволяет им точнее устанавливать часовые пояса злоумышленников и выявлять корреляцию между кибератаками.

– большая часть индикаторов, выявляемых при использовании данных методик, довольно легко изменяема и учитывая возможность ложного флага, это достаточно серьезная проблема, ведь злоумышленники могут подделать комментарии в программном коде, удалить информацию об отладке, изменить время компиляции и т. д. Также вредоносный код и эксплойты одной группировки могут быть украдены другой, а инфраструктура может быть общей для нескольких группировок, что затрудняет проведение атрибуции.

– в то же время методы агентурной и радиоэлектронной разведки тоже не защищены от обмана, однако в ряде случаев они могут дать неопровержимые доказательства для атрибуции, которые также можно получить в результате осуществления ответной кибероперации. Но все эти доказательства не подходят для публичной атрибуции по понятным причинам.

Выводы

В настоящее время атрибуция кибератак проводится как компаниями по кибербезопасности, так и силами спецслужб и в ходе анализа их методик атрибуции было выявлено, что они не всегда гарантируют результат с высокой степенью уверенности, а также не учитывают степень достоверности выявляемых следов. Данная проблема решается разработкой новой методики атрибуции кибератак.

Литература

1. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. С. 98. DOI: 10.20542/978-5-9535-0581-9.
2. Лукацкий, А. В. Определение источника кибератак / А. В. Лукацкий // Индекс безопасности. – 2015. – Т. 21. – № 2(113). – С. 73-86
3. Международная информационная безопасность: теория и практика / Крутских А.В., Бирюков А.В., Бойко С.М., Волкова С.Г., Зиновьева Е.С., Зинченко А.В., Матюхин Д.В., Смирнов А.И. Учебник для вузов: в 3-х томах / Под общ. ред. А.В. Крутских. – М.: МГИМО, 2021. - Том 1 (2-е изд., доп.) – 384 с
4. Timo Steffens. Attribution of Advanced Persistent Threats: how to identify the actors behind cyber-espionage. 2021, 206 p

5. Lin H. Attribution of malicious cyber incidents: From soup to nuts, Economics, Hoover Working Group on National Security, Technology, and Law, 2016, Aegis Series Paper No 1607, 56 p.
6. Wheeler D.A., Larsen G.N., Techniques for Cyber Attack Attribution. IDA Paper, P-3792, 2003, 84 p
7. Skopik, F., Pahi, T. Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity* 3, 2020, 8 p
8. Simone Vernacchia. A Practical Method of Identifying Cyberattacks. 2018, 17 p
9. Li Qiang, Yang Ze-Ming, Liu Bao-Xu, Jiang Zheng-Wei. A Reasoning Method of Cyber-Attack Attribution Based on Threat Intelligence, *International Scholarly and Scientific Research & Innovation* 10(5), 2016, 56 p
10. Rid T., Buchanan B. Attributing Cyber Attacks, *The Journal of Strategic Studies*, 2015, 34 p

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

Comparative analysis of cyberattack attribution methods

Cheverkalov V.A.²¹²

Abstract. *Recently, for the global community, the task of correctly identifying those responsible for cyber attacks or malicious campaigns has become of paramount importance. Within the framework of this article, a brief description of the existing methods of cyber attribution is presented, as well as their comparative analysis, as a result of which the need to develop a new method of attribution of cyberattacks was identified, since the existing methods of attribution do not always give an unambiguous result and do not quite take into account the reliability of the artifacts (traces) identified, which is a priority when there is a problem with false flags in cyberspace.*

Keywords: *cybersecurity, information security, attribution, cyberattacks, cyberspace, hacker groups.*

²¹² Vladimir Cheverkalov, student of Financial University under the Government of the Russian Federation, Moscow, v.cheverkalov@gmail.com

Об одной модификации известной апробированной системы распознавания лиц

Чемоданов Н.С.²¹³, Гордеев Э.Н.²¹⁴

***Аннотация.** Данные тезисы отражают три аспекта исследовательской работы, направленной на анализ и имплементацию системы распознавания лиц. Первый аспект касается анализа и сравнения известных апробированных систем с упором на учет их основного заявленного авторами базового свойства. На втором этапе выбиралось это свойство и конкретная система, его использующая. В результате проведенного анализа были выявлены «гибридные» возможности модификации исходной системы, допускающие параметризацию, что в дальнейшем позволило подобрать такие значения параметров этой модификации, которые позволили улучшить заявленные авторами характеристики. Основная проблема – это стратегия численных экспериментов в условиях ограниченных возможностей.*

***Ключевые слова:** распознавание лиц, нейронная сеть, машинное обучение.*

Введение. Выбор решения для модификации

Базовая система распознавания лиц обычно состоит из нескольких этапов. Первый шаг – определить, какие области изображения содержат лицо через компонент обнаружения или отслеживания. Расположение лица обнаруживается с помощью отделения лицевых признаков от фоновых. Затем информация о лице извлекается и преобразуется в форму, требуемую алгоритмом распознавания, а потом лицо сравнивается с изображениями из базы данных. В обычных CNN (англ. Convolutional Neural Network), например, в VGG16 и LeNet-5 [1, 2], для многоклассовой классификации изображений в качестве классификатора используют классификатор softmax. При использовании softmax для распознавания лиц сеть придется переобучать каждый раз, когда в базу данных добавляется новый класс, так как количество выходных значений сети меняется с изменением количества классов. Поэтому использование нейронных сетей с классификатором softmax нежелательно. Помимо CNN с классификаторами softmax, существуют еще SNN (англ. Siamese Neural Network) [3]. При решении задач распознавания лиц данные нейронные сети в общем случае состоят из двух веток CNN, при этом CNN в ветвях имеют общие весовые коэффициенты, то есть можно сказать, что используется одна CNN, которая называется ядром SNN.

Характеристики и особенности выбранного для модификации решения

В качестве апробированного решения была взята архитектура FaceNet NN2 [4] с некоторыми изменениями:

- размер входного изображения принят равным $96 \times 96 \times 3$, вместо $224 \times 224 \times 3$;
- размер ядра и шаг в conv1, соответственно, равен 3 и 2;
- во всех inception блоках нет свертки с фильтрами 5×5 .

При этом архитектура ядровой CNN в FaceNet NN2 является подобной GoogLeNet [5]. То есть в ней используется Inception блоки (рис.1).

²¹³ Чемоданов Никита Сергеевич, студент, МГТУ им. Н.Э.Баумана, Москва, chemodanov_nikita@mail.ru

²¹⁴ Гордеев Эдуард Николаевич, д.ф.-м.н., профессор, МГТУ им. Н.Э.Баумана, Москва, gordeeven@bmstu.ru

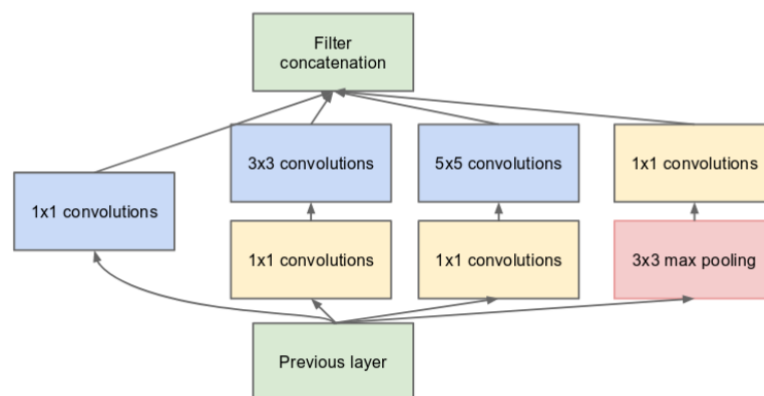


Рис.1. Архитектура Inception блока

Настройка обучающего и тестового наборов

Авторы [4] проверяли свою модель на наборе данных LFW [6]. LFW состоит из 13233 изображений 5749 людей.

Авторы [4] использовали стандартный протокол unrestricted, labeled outside data и подход «View 2», то есть помимо изображений из набора данных LFW для обучения используются другие изображения. Всего используется 100-200 миллионов изображений лиц для 8 миллионов человек. При этом ими была получена $98,87\% \pm 0,15$ точность классификации, используя модель NN1 (с размером входного изображения 220×220), однако модель NN3 с размером входного изображения 160×160 достигает почти тех же результатов.

В отличие от авторов для обучения и тестирования апробированной нейронной сети использовалась база данных вырезанных изображений лиц LFW cropped [7].

Апробированная нейронная сеть была обучена на обучающем наборе из «View 1» [6].

Обучающий набор состоит из 9525 изображений 4038 человек. Этот набор был аугментирован с помощью случайных зеркальных отображений по горизонтали, а также изменения яркости в диапазоне $[0,25; 1,5]$. В результате аугментации обучающий набор был расширен до 19050 изображений 4038 человек.

Для проверки эффективности нейронной сети был использован подход «View 2». То есть была реализована перекрестная проверка с разбиением на 10 частей (англ. 10-fold cross-validation).

Модификация апробированной сети

Для модификации нейронной сети FaceNet NN2 предлагается использовать механизм внимания (англ. Attention Mechanism) CBAM (англ. Convolutional Block Attention Module) [9]. В отличие от SE блока (англ. Squeeze-And-Excitation) [10] CBAM состоит из двух блоков SAM (англ. Spatial Attention Module) и CAM (англ. Channel Attention Module). Кроме того согласно, авторам [9] точность при использовании SE блоков хуже, чем при использовании CBAM.

Пространственное внимание (англ. Spatial Attention) представляет механизм внимания (маску внимания) на картах признаков. Пространственный слой, связан с каждой картой признаков (англ. feature map), он усиливает признаки объекта, который необходимо классифицировать.

Внимание канала (англ. Channel Attention) представляет механизм внимания (маску внимания) вдоль канала карт признаков. Внимание канала добавляет веса каждому каналу и таким образом учитывает важность конкретного канала (карты признаков).

Пусть $F \in \mathbb{R}^{C \times H \times W}$ является выходом предыдущего слоя, тогда CBAM последовательно выводит 1D CAM $M_c \in \mathbb{R}^{C \times 1 \times 1}$ и 2D SAM $M_s \in \mathbb{R}^{1 \times H \times W}$. Общий процесс внимания выглядит следующим образом:

$$\mathbf{F}' = \mathbf{M}_c(\mathbf{F}) \times \mathbf{F}, \mathbf{F}'' = \mathbf{M}_s(\mathbf{F}') \times \mathbf{F}' \quad (1)$$

где: $\times$ – это поэлементное умножение; $\mathbf{F}'$ – выход САМ; $\mathbf{F}''$ – итоговый усовершенствованный выход СВАМ.

Внимание канала $\mathbf{M}_c \in \mathbb{R}^{C \times 1 \times 1}$ вычисляется следующим образом:

$$\mathbf{M}_c(\mathbf{F}) = \sigma(\text{MLP}(\text{AvgPool}(\mathbf{F})) + \text{MLP}(\text{MaxPool}(\mathbf{F}))) = \sigma(\mathbf{W}_1(\mathbf{W}_0(\mathbf{F}_{\text{avg}}^c)) + \mathbf{W}_1(\mathbf{W}_0(\mathbf{F}_{\text{max}}^c))) \quad (2)$$

где: σ – сигмоида; $\mathbf{F}_{\text{avg}}^c$ – выход среднего пулинга; $\mathbf{F}_{\text{max}}^c$ – выход максимального пулинга; $\mathbf{W}_0 \in \mathbb{R}^{C/r \times C}$ весовые коэффициенты первого слоя MLP; $\mathbf{W}_1 \in \mathbb{R}^{C \times C/r}$ весовые коэффициенты второго слоя MLP.

Пространственное внимание $\mathbf{M}_s \in \mathbb{R}^{H \times W}$ вычисляется следующим образом:

$$\mathbf{M}_s(\mathbf{F}) = \sigma(f^{7 \times 7}([\text{AvgPool}(\mathbf{F}); \text{MaxPool}(\mathbf{F})])) = \sigma(f^{7 \times 7}([\mathbf{F}_{\text{avg}}^s; \mathbf{F}_{\text{max}}^s])) \quad (3)$$

где: σ – сигмоида; $\mathbf{F}_{\text{avg}}^s$ – выход среднего пулинга, $\mathbf{F}_{\text{avg}}^s \in \mathbb{R}^{1 \times H \times W}$; $\mathbf{F}_{\text{max}}^s$ – выход максимального пулинга, $\mathbf{F}_{\text{max}}^s \in \mathbb{R}^{1 \times H \times W}$; $f^{7 \times 7}$ – операция свертки с размером фильтра 7×7 ; $[\cdot; \cdot]$ – операция конкатенации.

Реализация модификации

Особенности модифицированной архитектуры реализованной FaceNet NN2.

1.Используется СВАМ блок со сверточным слоем внутри САМ с размером ядра 7×7 и шагом 1, а также размером скрытого слоя MLP в блоке САМ равный размеру входного слоя, поделенному на 4.

2.Также внутри САМ после сверточного слоя с размером ядра 3×3 используется СВАМ «cbam4 (7×7 , 1; 16)».

Результаты выполнения

Модифицированная нейронная сеть была обучена в течении 500 эпох (рис. 2). После 493 эпохи была получена точность классификации $89,50\% \pm 0,52$. При этом реализованная апробированная нейронная сеть имеет точность $86,22\% \pm 1,26$, то есть модифицированная нейронная сеть имеет на 3,28% выше точность.

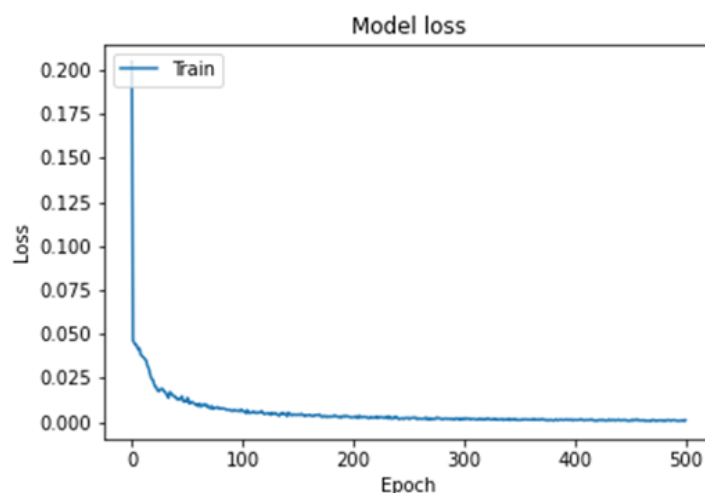


Рис.2. Значения функции потерь на каждой эпохе обучения

Вывод

В данной работе обучена апробированная нейронная сеть FaceNet NN2, была получена точность классификации $86,22\% \pm 1,26$, хотя оригинальная FaceNet имеет точность $98,87\% \pm 0,15$. Данное отличие точности объясняется тем, что:

- во-первых, оригинальная нейронная сеть была обучена на наборе данных в 5000-10000 больше, чем реализуемая.
- во-вторых, размер изображения, подаваемый на вход в реализуемой FaceNet NN2, равен

96×96, а размер изображения, подаваемый на вход оригинальной FaceNet NN2, равен 220×220 для NN1 и 160×160 для NN3.

- в-третьих, реализуемая нейронная сеть не имеет 5х5 сверток в inception блоках.

Кроме того, FaceNet NN2 модифицирован путем добавления в него блоков СВМ. Получена точность 89,50%±0,52, это лучше реализованной системы распознавания лиц на 3,28%.

Литература

- 1.Simonyan K., Zisserman A. Very deep convolutional networks for large-scale image recognition //arXiv preprint arXiv:1409.1556. – 2014.
- 2.LeCun Y., et al. Gradient-based learning applied to document recognition //Proceedings of the IEEE . – 1998. –Т.86 –№.11. – С. 2278-2324.
- 3.Taigman Y., et al. Deepface: Closing the gap to human-level performance in face verification //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2014. – С. 1701-1708.
- 4.Schroff F. Facenet: A unified embedding for face recognition and clustering //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2015. – С. 815-823.
- 5.Szegedy C., et al. Going deeper with convolutions //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2015. – С. 1-9.
- 6.Labeled faces in the wild: A database for studying face recognition in unconstrained environments. Режим доступа: <http://vis-www.cs.umass.edu/lfw/#information> (дата обращения 02.10.2020)
- 7.LFWcrop Face Dataset. Режим доступа: <https://conradsanderson.id.au/lfwcrop/> (дата обращения 10.10.2020)
- 8.Barry-Straume J. An evaluation of training size impact on validation accuracy for optimized convolutional neural networks // SMU Data Science Review. – 2018. – Т. 1. – №. 4. – С. 12.
- 9.Woo S. Cbam: Convolutional block attention module // Proceedings of the European conference on computer vision (ECCV). – 2018. – С. 3-19
10. Hu J., Shen L., Sun G. Squeeze-and-excitation networks //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2018. – С. 7132-7141.

About one modification of the well-known proven facial recognition system

Chemodanov N.S.²¹⁵, Gordeev E.N.²¹⁶

Abstract. *These theses reflect three aspects of the research work aimed at analyzing and implementing the facial recognition system. The first aspect concerns the analysis and comparison of known tested systems with an emphasis on taking into account their main basic property declared by the authors. At the second stage, this property and the specific system that uses it were selected. As a result of the analysis, "hybrid" possibilities of modification of the original system that allow parameterization were identified, which later allowed us to select such values of the parameters of this modification that allowed us to improve the characteristics claimed by the authors. The main problem is the strategy of numerical experiments in conditions of limited possibilities.*

Keywords: *facial recognition, neural network, machine learning.*

²¹⁵ Chemodanov N.S., student, Bauman Moscow State Technical University, Moscow, chemodanov_nikita@mail.ru

²¹⁶ Gordeev Eduard, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, gordeeven@bmstu.ru

Система безопасности объектов с использованием трехмерной визуализации Шайтура С.В.²¹⁷, Минитаева А.М.²¹⁸, Сумзина Л.В.²¹⁹, Максимов А.В.²²⁰

Аннотация. В статье проведены исследования по проектированию систем безопасности объектов с использованием трехмерных средств визуализации и геоинформационных систем. Эта технология основана на интеграции систем видеонаблюдения, распознавания образов и картографической платформы для точного определения местоположения события на карте или плане. Такие системы используются для быстрого выявления чрезвычайных ситуаций и быстрого принятия решений о реагировании. Технология предлагается для охраны муниципальных объектов, таких как больницы, школы, детские сады, учебные заведения и т.д. Внедрение технологии позволит существенно обезопасить эти объекты от проникновения на них и проведения террористических операций.

Ключевые слова: трехмерное моделирование, система безопасности, геоинформационные технологии, геоинформационные системы, система видеонаблюдения, технические средства, контрольно-пропускные пункты.

Введение

По мере развития общества появляются новые вызовы безопасности муниципальных объектов. Повышается техническая оснащенность потенциальных нарушителей, совершенствуются методы проведения противоправных действий [1]. Самыми незащищенными при этом являются муниципальные объекты, такие как больницы, поликлиники, образовательные заведения, детские сады и т.д.

Обычные системы управления контролем доступа на объект выводят информацию с камер на контрольно-пропускной пункт и предоставляют анализировать текущую ситуацию диспетчеру без обработки и выделения опасных объектов [2,3]. Создание интеллектуальной системы контроля доступа на объект на основе создания трехмерной геоинформационной системы позволяет подойти к охране объекта на качественно другом уровне. Такие системы позволяют не только контролировать текущую ситуацию, но и прогнозировать возможные отклонения от стандартной ситуации, оценивать степень чрезвычайности ситуации и предлагать оптимальное решение для предотвращения опасной ситуации. Интеллектуальные системы контроля доступа позволяют вынести пункт принятия решения по доступу на удаленный объект, таким образом, обезопасив сотрудников вневедомственной охраны.

1. Материалы и методы

В статье исследуются возможности применения пространственного геоинформационного анализа [4, 5] к вопросу создания системы безопасности объекта [6]. Геоинформационный анализ данных основывается на математических и статистических методах, методах искусственного интеллекта (распознавание образов, нейросетевые методы) [7, 8, 9], картографическом и пространственном анализе [10, 11, 12].

²¹⁷ Шайтура Сергей Владимирович, кандидат технических наук, доцент, Российский университет транспорта, Москва, swshaytura@gmail.com

²¹⁸ Минитаева Алина Мажитоана, кандидат технических наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, aminitaeva@mail.ru

²¹⁹ Сумзина Лариса Владимировна, кандидат технических наук, доцент, Российский государственный университет туризма и сервиса byttech1@yandex.ru

²²⁰ Максимов А.В., кандидат технических наук, доцент, Российский государственный университет туризма и сервиса, maksimovav52@yandex.ru

2. Система моделирования и визуализации пространственных данных в трехмерном виде

Система моделирования и визуализации пространственных данных в трехмерном виде предназначена для визуализации территорий и объектов в пространстве, комплексного анализа территории и отображения геоинформационных ресурсов [13, 14, 15, 16]. Программа дает пользователям возможность свободного перемещения в трехмерном пространстве, обеспечивает визуальное представление городов, поселений, рельефа местности, критически важных объектов в трехмерном виде, моделирования возможных природно-техногенных ситуаций. Программа позволяет загружать векторные слои и космические снимки, данные дистанционного зондирования Земли, трехмерные модели с возможностью редактирования расположения моделей на местности.

3. Создание системы безопасности

Для организации пропускного режима на объекте оборудуется контрольно-пропускной пункт (КПП) [1]. Оборудование пункта пропуска должно обеспечивать необходимую пропускную способность и возможность тщательной проверки пропусков, документов от проходящих лиц, досмотра всех видов транспорта, перевозимых грузов и отвечать следующим требованиям. КПП должен быть оборудован необходимыми системами связи и сигнализации для вызова резерва охраны. В качестве контроля доступа можно использовать различные турникеты. На объекте так же устанавливаются видеокамеры. На основе программ трехмерного моделирования создается трехмерная модель объекта. Текущая ситуация определяется методом сравнения данных, поступающих с видеокамеры, с моделью объекта.

Выводы

Интеграция данных из разнородных источников и широкие возможности для комплексного анализа (в том числе в режиме реального времени), визуализация и публикация информации позволяют лицам, принимающим решения, действовать в рамках модели картографической системы. При этом могут использоваться системы распознавания образов с целью быстрого реагирования в чрезвычайных ситуациях.

Система объединяет потоки данных из различных источников (включая видео), доступ к ним предоставляется различным сервисам на картографическом портале и через мобильные устройства.

Литература

1. Алаухов С.Ф, Коцеруба В.Я. Вопросы создания систем физической защиты для крупных промышленных объектов // Системы безопасности, 2011
2. Тельный А. В., Черников Р. С. Алгоритм обработки тревожных извещений объектовых средств охранной сигнализации для снижения уровня ложных срабатываний // Системы управления, связи и безопасности. 2019. № 4. С. 140-162. DOI: 10.24411/2410-9916-2019-10405.
3. Титов А.Ю. Обзор подходов к применению технологий искусственного интеллекта в информационной безопасности данных / В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019.343-351
4. Протасова А.А., Шайтура С.В. Анализ методов защиты баз данных // Славянский форум. - 2017. - № 1 (15). - с. 290 - 298.
5. Шайтура С.В. Интеллектуальный анализ геоданных // Перспективы науки и образования. - 2015. - № 6 (18). - с. 24-30.
6. Голкина Г.Е., Шайтура С.В. Безопасность бухгалтерских информационных систем – Учебное пособие - Бургас, 2016

7. Гаврилова В.В., Шайтура С.В. Естественный и искусственный интеллект // Славянский форум. - 2014. - № 2 (6) - с. 24-27.
8. Шайтура С.В. Интеллектуальные системы и технологии - Учебное пособие / Бургас, 2016
9. Shaitura S.V., Ordov K.V., Lesnichaya I.G., Romanova Yu. D., Khachaturova S.S. Services and mechanisms of competitive intelligence on the internet // [Espacios](#).- 2018.- Т. 39.- № 45.- С. 24.
10. Shaitura S.V., Feoktistova F.M., Minitaeva A.M., Olenov L.A., Chulkov V.O., Kozhaev Y.P. Spatial geomarketing powered by big data //Revista Turismo Estudos & Práticas. 2020. № S5. С. 13.
11. Shaitura S.V., Kozhaev Yu.P., Ordov K.V., Vintova T.A., Minitaeva A.M., Feoktistova V.M. Geoinformation services in a spatial economy // International Journal of Civil Engineering and Technology. 2018. Т. 9. № 2. С. 829-841.
12. Tsvetkov V.Ya., Shaytura S.V., Sultaeva N. L. Digital Enterprise Management in Cyberspace. - Proceedings of the 2nd International Scientific and Practical Conference “Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth” (MTDE 2020), Yekaterinburg, Russia, pp. 361 – 365 <https://doi.org/10.2991/aebmr.k.200502.059>
13. Шайтура С.В., Минитаева А.М., Розенберг И.Н., Кожаев Ю.П. Трехмерное моделирование и создание панорам - Монография - Бургас, 2019.
14. Шайтура С.В., Сумзина Л.В., Розенберг И.Н., Винтова Т.А. Моделирование и визуализация трехмерных пространственных объектов - Монография - Бургас, 2018.
15. Иваныш А.В., Ядрышников Ф.М., Жирнова К. А., Штрахов И.С., Митрофанов Е.М. Построение трехмерной измерительной модели с использованием мобильной системы контрольных точек // Славянский форум, № 1 (31), 2021, с. 305-312
16. Shaitura S.V., Minitaeva A.M., Feoktistova V.M., Ordov K.V. Blockchains in spatial data security - В сборнике: CEUR Workshop Proceedings. Selected Papers of the X Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2019). - 2019. - С. 70-74.

Facility security system using three-dimensional visualization

Shaytura S.V.²²¹, Minitaeva A.M.²²², Sumzina L.V.²²³, Maksimov A.V.²²⁴

Abstract. *In the article, the system design of security systems for objects, the use of three-dimensional visualization tools and geographic information systems. This technology is based on the integration of video surveillance systems, image recognition and a mapping platform to accurately determine the location of events on a map or plan. Such systems are used for quick response and quick decision making about response. Protection of municipal facilities such as hospitals, schools, kindergartens, educational institutions, etc. is offered. Implementation of methods to secure your funds from penetration through them.*

Keywords: *three-dimensional modeling, security system, geoinformation technologies, geoinformation systems, video surveillance system, technical means, checkpoints.*

²²¹ Sergey Shaytura, Ph.D., Associate Professor, Russian University of Transport (MIIT), Moscow, swshaytura@gmail.com

²²² Alina Minitaeva, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, aminitaeva@mail.ru

²²³ Larisa Sumzina, Ph.D., Associate Professor, Russian State University of Tourism and Service, Moscow, byttech1@yandex.ru

²²⁴ Alexandr Maksimov, Ph.D., Associate Professor, Russian State University of Tourism and Service, Moscow, maksimovav52@yandex.ru

Масштабирование размеров команд и управления правами доступа в групповых исследованиях по сетевому моделированию с использованием технологии биометрической идентификации

Шевадронов А.С.²²⁵, Киселев В.В.²²⁶, Бабиченко О.А.²²⁷

***Аннотация.** Предложен алгоритм аутентификации исследователей на стенде с использованием биометрической информации, подробно рассмотрены шаги этого алгоритма. Данный алгоритм применим для решения проблем в области предоставления доступа в среде с пропускным режимом доступа к помещениям и развитой сетевой инфраструктурой. Сформулированы требования для создания такой системы. Рассмотрено применение такого алгоритма к существующему стенду полунатурного математического моделирования.*

***Ключевые слова:** аутентификация, кооперативные исследования в больших группах, биометрическая идентификация, сетевое полунатурное моделирование, локальные вычислительные сети.*

Введение

В рамках исследовательских работ на стенде полунатурного моделирования МСКБО [1-3] (многофункциональный стенд комплекс бортового оборудования) расположенного в ИНОЦ АВИАНИКА в главном учебном корпусе МГТУ им. Н.Э. Баумана, была выявлена проблематика необходимости автоматизированного предоставления доступа к программной инфраструктуре стенда математического моделирования [4]. Это возникает вследствие наличия нескольких команд разработчиков программного обеспечения для моделирования полета летательных аппаратов. Также, следует отметить использование стендом новой программной архитектуры [5] которая представлена на рисунке 1, расширением которой является данная подсистема биометрической идентификации.

²²⁵ Шевадронов Александр Сергеевич, аспирант ИУ-6, МГТУ им Н.Э. Баумана, Москва, shevadronov@student.bmstu.ru

²²⁶ Киселев Владимир Владимирович, аспирант ИУ-8ИБ, МГТУ им Н.Э. Баумана, Москва, kvv20ua042@student.bmstu.ru

²²⁷ Бабиченко Ольга Андреевна, студент ИУ-1, МГТУ им. Н.Э. Баумана, Москва, babichenko_olga@mail.ru

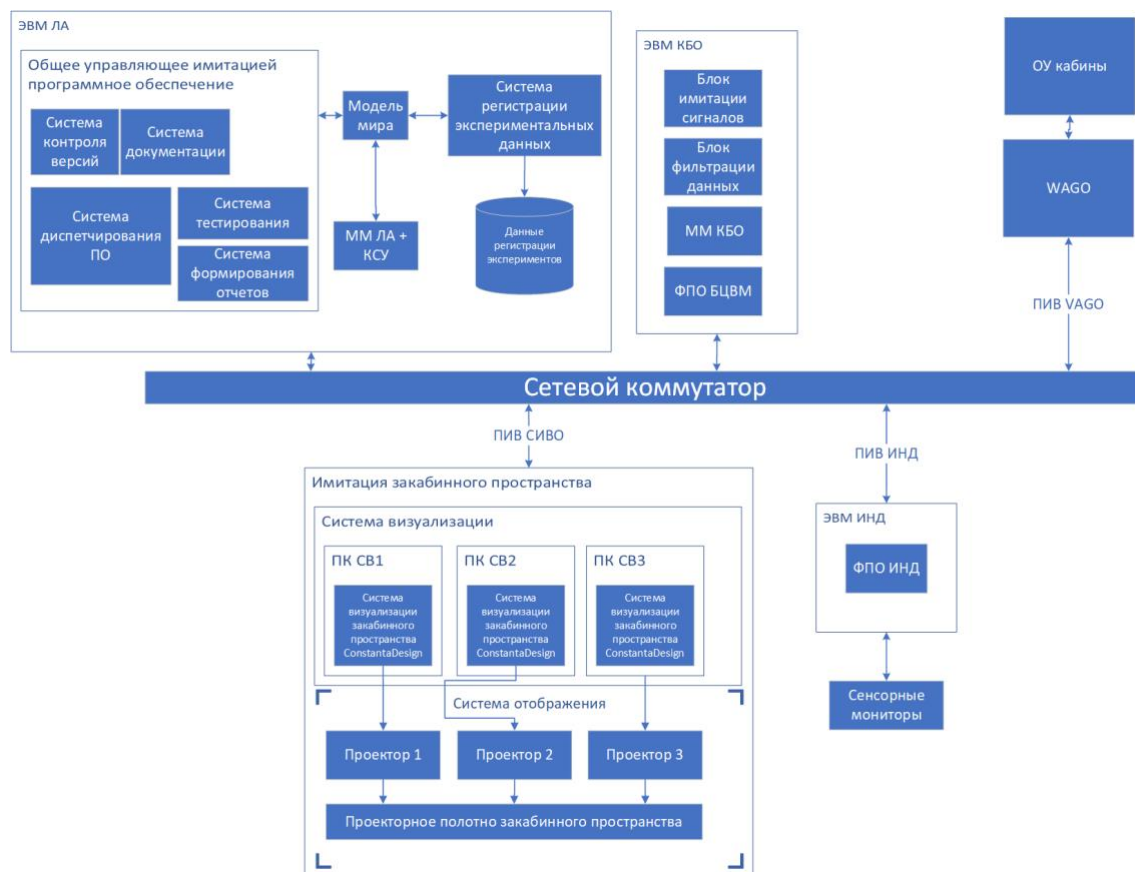


Рис.1. Схема станда МСКБО после программной модернизации

Предлагается система для автоматизированного предоставления доступа посредством идентификации лиц по запросу в виде формального документа из доверенного источника. Алгоритм данного решения представления на рисунке 2.

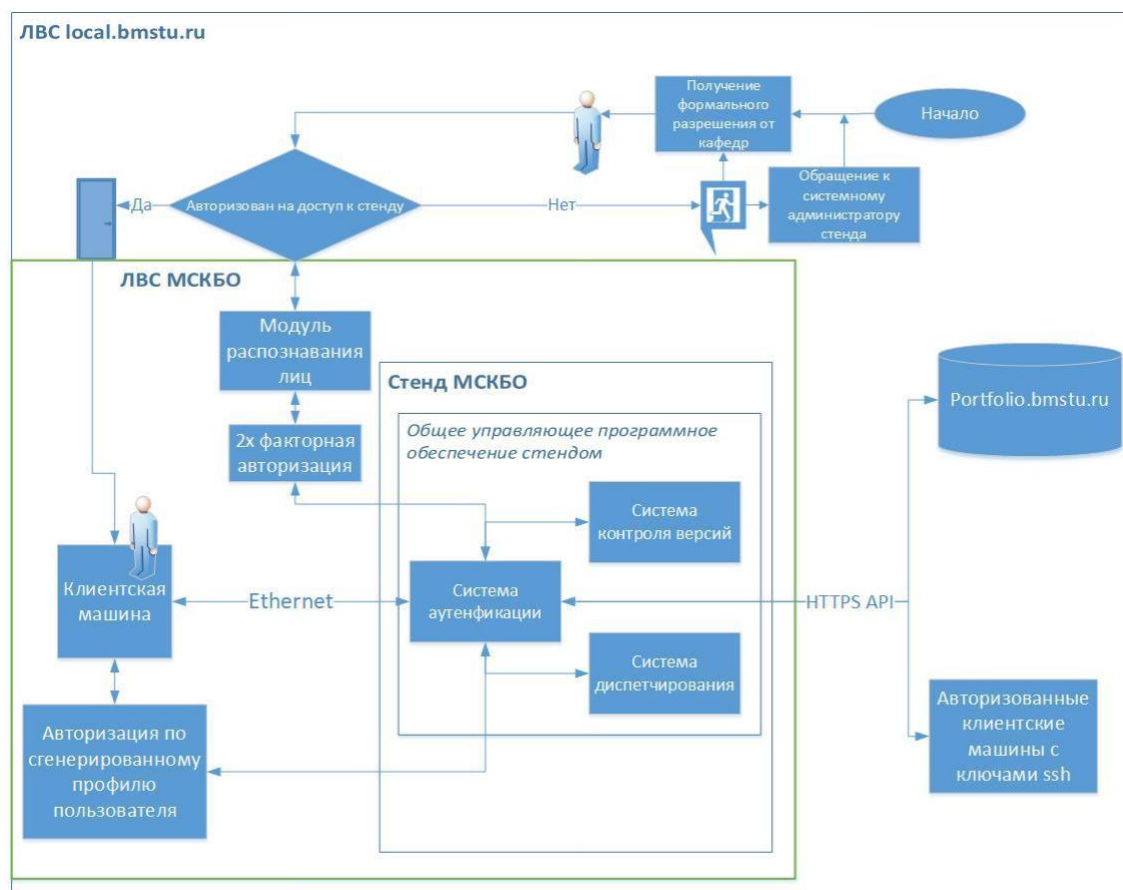


Рис 2. Алгоритм предоставления доступа к стенду МСКБО
Рассмотрим задачу подробно.

Постановка задачи

Требуется создать процедуру идентификации новых пользователей стенда, при которой выдача необходимых прав доступа, документов и физический доступ к стенду полностью автоматизирован. Это необходимо для оптимизации трудозатрат высококвалифицированных исследователей и программистов. Эти трудозатраты могут быть использованы для новых исследований, что делает максимально целесообразным разработку такой автоматизированной системы. [6] Следует отметить необходимость в высоком уровне безопасности такой системы, поэтому проект такой подсистемы для стенда был вынесен на обсуждение. Соответственно, требованием является безопасность доступа, но порог требований существенно ниже, поскольку мы находимся в доверенной среде, в которой все посещающие главное здание имеют пропуска или проходят по спискам, в которых указаны их паспортные данные, при том, что люди, которые проходят по спискам не находятся значительное время на территории и вероятность проникновения существенно снижена. Поэтому, в качестве доверенного источника информации о благонадежности вновь присоединяющихся исследователей является передача информация о их желании вести работу на стенде от вышестоящих организаторов, таких как кафедры и НУК факультетов. Поэтому, получив формально подтвержденную информацию в виде заявки на использование стенда, мы делаем данный документ первичным источником данных, в которой указывается ФИО работающих на стенде людей и их проекты.

Данная заявка направляется с доверенной электронной почты, такой как почты заведующих кафедр, почты научных руководителей исследователей и других уполномоченных лиц. В данной заявке может быть фото, телефонный номер, электронная почта всех желающих работать на стенде и ФИО. С помощью портфолио проверяются

данные обучающегося МГТУ: ФИО, фотография, учебная группа и дата рождения. На основе публичных данных собирается обучающая выборка. Одним из преимуществ геометрии лица как биометрического идентификатора является бесконтактный способ получения сведений для распознавания пользователей. [7]

Статическая (физиологическая характеристика) - фотография лица используется для идентификации пользователя. На основе различных черт лица с помощью нейронной сети формируется уникальный цифровой шаблон. [8]

В режиме идентификации пользователь предъявляет фото в составе анкеты. В этом случае фотография лица сравнивается с базой данных ранее записанных шаблонов. В качестве алгоритма распознавания лиц используется сверточная нейронная сеть. [9] Чтобы снизить риск ложноотрицательного срабатывания системы применяется 2-х факторная авторизация на основе временных одноразовых паролей. Данный способ используется только для предоставления доступа к стенду тем, у кого в заявке часть данных может быть некорректна. Фотоидентификация используется чтобы убрать необходимость вводить и запоминать одноразовые пароли. При высокой степени совпадения, система автоматически предоставляет доступ. Если степень доверия недостаточна, то принимается решение о предоставлении физического доступа пользователя к инфраструктуре стенда с помощью системного администратора.

После этого, высылается подтверждение авторизации по электронной почте. Если пользователь хочет работать удаленно в рамках вычислительной сети МГТУ им. Н.Э.Баумана, то ему нужно выдавать ключ авторизации по SSH, используя один из алгоритмов шифрования RSA или ED25519.

Алгоритм аутентификации

Распишем алгоритм по шагам:

1.а Использование документа, получаемого по внутренней электронной почте установленного формата, возможно подписанного ЭЦП;

1.б Использование автоматизированной системы обмена данными с кафедрами (и другие специализированные решения);

2. Брать данные: из анкеты, из доверенных источников, таких как база портфолио МГТУ, систем электронного учета МГТУ, баз данных факультетов и кафедр;

3. Выслать подтверждение авторизации по электронной почте с кодами доступа для входа на стенд и авторизации в локальной вычислительной сети;

4. Осуществлять верификацию по фото для получения физического доступа к инфраструктуре стенда;

5. Получение ключей электронного доступа после ввода кодов и инструктажа на доверенной машине в локальной сети вычислительного комплекса;

6. Возможность работы со стендом после испытательного срока из локальной вычислительной сети МГТУ им. Н.Э. Баумана для проведения высоко автоматизированных экспериментов по тестовым сценариям без необходимости присутствия на стенде.

Предлагаемые технические решения для прототипа

Предлагается использовать следующее программное обеспечение с открытым исходным кодом

- ☐ Система контроля версий – Gitlab;
- ☐ Система диспетчирования программного обеспечения (ПО) – Jenkins [10];
- ☐ Система аутентификации – вновь разрабатываемая система;
- ☐ Система распознавания лиц – на основе сверточных нейронных сетей FaceNet;
- ☐ ПО математического моделирования - существующее ПО с модернизацией для учета необходимости совместной работы, таких как контроль версий, контейнеризация [11] и прочие необходимые элементы современной программной инфраструктуры.

Выводы

Предложен алгоритм аутентификации исследователей на стенде полунатурного моделирования МСКБО с использованием биометрической информации, подробно рассмотрены шаги этого алгоритма. Данный алгоритм применим для решения проблем в области предоставления доступа в среде с пропускным режимом доступа к помещениям и развитой сетевой инфраструктурой. Сформулированы требования для создания такой системы. Рассмотрено применение такого алгоритма к существующему стенду полунатурного математического моделирования. Данный алгоритм может служить для аналогичных стендов моделирования одним из возможных эффективных решений проблемы автоматизированного предоставления доступа.

Литература

1. Бабиченко А.В., Сухомлинов А.Б., Земляной Е.С., Воробьев А.А., Тектов М.В., Кожин В.Р., Елесин И.А., Задорнова Т.И., Шевадронов А.С. Моделирование системы интеллектуальной поддержки экипажа // Авиакосмическое приборостроение. – 2018. № 12. – С. 35-43.
2. Бабиченко А.В., Земляной Е.С., Воробьев А.А., Елесин И.А., Задорнова Т.И., Шевадронов А.С. Разработка макета бортовой системы интеллектуальной поддержки летательного аппарата// Авиакосмическое приборостроение. – 2019. № 2. – С. 26-33.
3. Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. 2016. № 6 (111). С. 85-96.
4. Федосов Е.А. Основные направления формирования научно-технического задела в области бортового оборудования перспективных ВС // Материалы докладов 4-й Международной конференции «Перспективные направления развития бортового оборудования гражданских воздушных судов», г. Жуковский Московской обл., Дом ученых ФГУП «ЦАГИ», 2017. С. 6-14.
5. Шевадронов А.С., Бабиченко А.В., Пролетарский А.В. Метод создания математических моделей авиационных систем для архитектур с использованием виртуализации //Математические методы в технике и технологиях-ММТТ-34. – 2021.
6. Горбунов В.Л., Жданова И.В., Тэт Наинг Вин. Автоматизированная система управления контролем и доступом // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2018. № 6. С. 37–47. DOI: 10.18698/0236-3933-2018-6-37-47
7. Абдурахманов А. Ш., Масюк В. М., Лачихин А. В. Подход к построению системы распознавания лиц в видеопотоке //Вопросы радиоэлектроники. – 2017. – №. 6. – С. 39-45.
8. Щеголева Н. Л., Петрова В. А. Проблемы оценки биометрических систем //Известия СПбГЭТУ ЛЭТИ. – 2017. – Т. 10. – С. 32-37.
9. Басараб М., Коннова Н. Интеллектуальные технологии на основе искусственных нейронных сетей. – 2017.
10. Юшкевич А. С. Разработка модели испытательного стенда для установки и настройки системы аудита безопасности Linux сервера //Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – 2019. –Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019. 409 с. – илл. Т. 3.
11. Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. № 1 (14). С. 24-30.

Научный руководитель: Пролетарский Андрей Викторович, доктор технических наук, профессор, декан факультета ИУ МГТУ им. Н.Э. Баумана, rav@bmstu.ru.

Научные консультанты: Бабиченко Андрей Викторович, доктор технических наук, директор учебно-научного центра АО «РПКБ», директор ИНОЦ «АВИОНИКА», ababichenko@rpkb.ru; Коннова Наталья Сергеевна, доцент кафедры «Информационная безопасность», nkonnova@bmstu.ru.

Scaling of team sizes and access rights management in collaboration research of network modeling using biometric identification technology

A. Shevadronov²²⁸, V. Kiselev²²⁹, O. Babichenko²³⁰

Abstract. *An algorithm for authenticating researchers at modeling benches using biometric information such as facial recognition is proposed, and the steps of this algorithm are considered in detail. This algorithm is applicable for solving problems in the field of providing access in an environment with a pass-through mode of access to premises and a developed network infrastructure. The requirements for creating such a system are formulated. The application of such an algorithm to the existing method of semi-natural mathematical modeling is considered.*

Keywords: *authentication, cooperative research in large groups, biometric identification, network semi-natural modeling, local area networks.*

²²⁸ Alexander Shevadronov, PhD student IC-6, Bauman MSTU, Moscow, shevadronov@student.bmstu.ru

²²⁹ Vladimir Kiselev, PhD student IC-8(IS), Bauman MSTU, Moscow, kvv20ua042@student.bmstu.ru

²³⁰ Olga Babichenko, student IC-1, Bauman MSTU, Moscow, babichenko_olga@mail.ru

Исследование аномалий в поведении пользователей Шаршеева Ж.²³¹

Аннотация. В статье рассмотрены алгоритмы и решения для выявления аномалий в поведении пользователей и предложены модели на основе искусственной нейронной сети с целью выявления нарушителя. Приведены особенности обучения данных систем и применения их на практике. Выявлены результативные алгоритмы в построении моделей.

Ключевые слова: искусственная нейронная сеть, аномальное поведение субъектов.

Введение

Целью данной работы является вычислить наилучший результат при анализе поведения пользователей для выявления нарушителя среди реальных исходных данных, опираясь на аппарат технологий искусственных нейронных сетей.

Анализируя действия пользователей, создается базовый уровень для определения нормального поведения пользователей и обнаружения закономерности, которые указывает на поведения нарушителя (рис.1).



Рис. 1. Пять уровней анализа поведения пользователей

Уровень 1 Сбор данных

Первым этапом мониторинга поведения пользователя является сбор данных о системе, объектах и событиях, которые необходимо проанализировать.

Фиксируется уникальный набор данных в соответствии с охватываемыми прецедентами.

Выделим следующую информацию об активности пользователей:

- Время логов
- Запросы на доступ к конфиденциальным активам
- Посещенные сайты
- Запущенные приложения
- Подключенные USB-устройства
- Динамика нажатия клавиш

Уровень 2 Обнаружение угроз

²³¹ Шаршеева Жибек, Финансовый университет при Правительстве РФ, Москва, jsharsheeva.rc@gmail.com

После того, как собрали информацию для определения нормального поведения пользователей, это дает возможность обнаружить поведение нарушителя. Анализ данных позволяет обнаруживать подозрительные действия и устанавливать шаблоны для различных категорий пользователей.

Уровень 3 Создание профиля поведения

Профиль пользователя содержит набор действий, типичных для определенного пользователя, на основе мониторинга данных, собранных в течение базового периода. Если такое поведение изменилось, решение сравнивает его с типичным поведением других пользователей в группе одноранговых узлов и известными шаблонами внутренних угроз, а затем предупреждает о наличии каких-либо нарушений.

Такая функциональность полезна для ожидания инцидента.

Используя профили поведения, можно обнаружить:

- злоумышленная деятельность
- скомпрометированные аккаунты
- потенциальные злоумышленники
- злоупотребление привилегиями
- злоупотребление доступом

Уровень 4 Выявление раннего предупреждения

Уровни 4 и 5 представляют наиболее мощные типы анализа поведения пользователей. При использовании машинного обучения и анализа, они составляют прогноз о нарушениях информационной безопасности на основе собранных данных. Основное различие между этими уровнями заключается в том, что решение раскрывает потенциального нарушителя. Системы уровня 4 и 5 полезны для обнаружения:

- мошенничество
- эксфильтрация данных
- кража интеллектуальной собственности
- шпионаж
- злоупотребление привилегиями

На уровне 4 решение обнаруживает аномалии в поведении пользователя, которые указывают на злонамеренные намерения. Раннее предупреждение означает, что инцидент обнаружен до потери данных - обычно, когда злоумышленник только планирует вредоносные действия. Работая с решением этого уровня, вы должны быть осторожны в интерпретации результатов анализа. Не исключено, что профилирование пользователя и анализ машинного обучения могут давать ложные срабатывания.

В этих случаях организациям дополнительно стоит полагаться на свои собственные правила, а не только на статистический анализ и профилирование.

Уровень 5 Предвидение угроз

На последнем уровне решение способно создать оценку риска по пользователям задолго до того, как они совершат атаку. Прогноз угрозы обычно основан на:

- профиль поведения пользователя
- модели атак
- прогнозирующие модели для различных типов атак
- оценка эффективности

В работе выполнен обзор методов машинного обучения для выявления аномалий. Среди методов обучения, используемых для выявления аномалий в поведении потенциального нарушителя, рассмотрены следующие алгоритмы:

А - алгоритм кластеризации;

В - критерий Колмогорова-Смирнова;

С - метод опорных векторов с одним классом.

Исследуемые алгоритмы относятся к числу недетерминированных, поэтому проводилось несколько экспериментов для получения более справедливой оценки. В табл. 1 представлены средние результаты.

Таблица 1.

Эффективность алгоритмов			
	A	B	C
True positive	0.42	0.61	0.73
True negative	0.54	0.64	0.85
Accuracy	0.56	0.67	0.84

Ассурасу(точность) показывает соотношение правильно классифицированных примеров и их общего количества.

true positive (tp) - количество верно выявленных аномалий;

true negative (tn) - количество состояний, неверно оцененных искусственной нейронной сетью как нормальные;

Из табл. 1 видно, что лучшие результаты показал метод опорных векторов с одним классом.

Рассматриваемые элементы — это журналы событий для действий, таких как вход и выход на сервер и создание / доступ к процессу сервера. Для моделирования пользовательских журналов событий время входа в систему, время выхода из системы, исходный IP-адрес, целевой IP-адрес, идентификатор пользователя и идентификатор процесса, к которому осуществляется доступ / запуск, идентифицируются как измерения. Факты, хранящиеся в таблице фактов, представляют собой логические показатели, такие как время, потраченное на измерение, которое измеряет разницу между временем входа и выхода из системы, и количество записей (рис. 2).

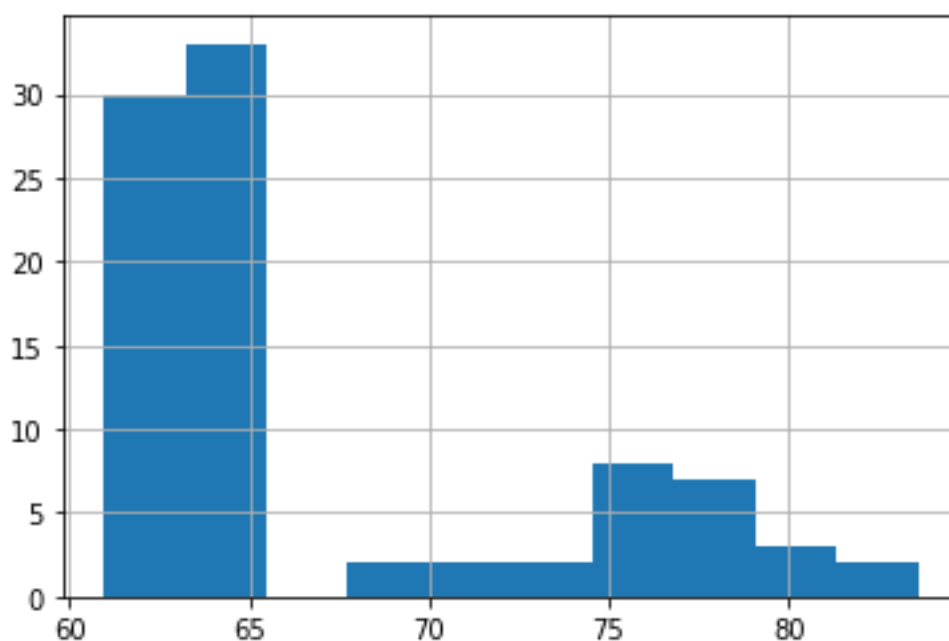


Рис. 2

Рис. 2 показывает некоторые аномалии для каждого Дня и Пользователя, но они разделены на разные кластеры в зависимости от расстояния и кластеров, указанных пользователем.

Реализация процесса

В этом разделе представлены результаты и оценка производительности алгоритмов с использованием анонимного набора данных журнала реальных событий с точки зрения статистической эффективности. Набор данных анонимного журнала событий состоял из 8675 элементов. Временной интервал событий входа в систему, выхода из системы и запуска / доступа к серверным процессам различными пользователями в организации рассматривался за 3 месяца. Пользователи, рассматриваемые для анализа, называются Пользователь1, Пользователь2, Пользователь3 и т.д. Исторические данные считаются данными за первые 75 дней, а остальные 15 используются в качестве текущих данных. Для запуска и анализа этих данных использовался Python.

На этом этапе создаем нейросети, которые будут оценивать потенциальных нарушителей. Вначале создадим двухслойную нейронную сеть прямого распространения (Рис. 6), в которую внесем 4 нейрона в скрытом слое и 1 нейрон в выходном слое. Введённые параметры будут содержать 1000 примеров по 8 значениям.

В итоге получена ИНС, которая обучилась на 1000 тренировочных данных, способная найти процентную составляющую потенциальных нарушителей среди пользователей.

На следующем этапе эксперимента предложено использовать ансамбль нейронных сетей, которая состоит из двух моделей искусственных нейронных сетей, а именно самоорганизующуюся сеть с конкуренцией (слой Кохонена) и многослойный персептрон. Как известно, фундаментальной задачей при построении ансамблей является генерация разнообразия ансамбля [2].

$$Y_{ensemble} = \frac{1}{T} \sum_{i=1}^T y_i(x_i),$$

где $Y_{ensemble}$ – выходной сигнал ансамбля моделей,

T – количество моделей НС в ансамбле,

$y_i(x_i)$ – выходной сигнал i -ой модели НС, полученный при предъявлении на вход модели сигнала x_i (входное).

Далее протестируем нейросетевой ансамбль.

1. В первой модели введем 6 нейронов, размер входного вектора составит 6, а скорость обучения – 0,25;

2. Во второй модели введем 6 слоев размер входного вектора составит 6 и скорость обучения – 0,5.

В ходе эксперимента использовалась тестовая выборка, которая содержала 1180 аномалий в поведении пользователей. За аномалию принято состояние, где результат искусственной нейронной сети не ниже 0,5.

Значение, которое лежит между 0 и 1, является статистической проверкой гипотезы о том, что поведение текущего дня аналогично нормальному поведению: значение ближе к 1 означает, что данные нормальные, а ближе к 0 означает, что данные указывают на аномальное поведение. Любой статистический тест требует порогового значения для принятия решения о результатах теста. Для обнаружения аномалии в качестве порога устанавливалось значение, равное 0,5: значение ниже, которое указывает на аномальное поведение.

Заключение

В работе были представлены алгоритмы выявления аномалий в поведении пользователей и модели сети на основе искусственной нейронной сети с целью выявления нарушителя.

В будущем анализ необходимо продолжить с использованием разнообразных наборов данных, имеющих большее количество атрибутов и записей. Технологии больших данных могут быть использованы для расширения работы.

Несмотря на то, что решение может быть полезным инструментом, его результаты должны быть тщательно проверены перед выполнением каких-либо действий. Ложноположительные результаты весьма возможны на этом уровне. Чтобы уменьшить их количество, следует:

- постоянно обеспечивать алгоритм новыми данными мониторинга. Чем больше корпоративных систем будет интегрировано в этот процесс, тем лучше будут результаты.
- обеспечить программное обеспечение с автоматической и ручной обратной связью. Алгоритм всегда должен сравнивать свои прогнозы с реальными действиями пользователя
- проводить долгосрочные и краткосрочные базовые показатели. Такое обучение научит алгоритм прогнозировать нарушения с использованием как недавних, так и прошлых контекстов.

Литература

1. Глобальное исследование утечек конфиденциальной информации в 2015 году / Аналитический центр InfoWatch 2016. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015.pdf?rel=1 (Дата обращения: 21.11.2019).
2. Гончаров М. Ансамбли моделей. [Электрон.ресурс]. Режим доступа: <http://www.businessdataanalytics.ru/download/ModelEnsembles.pdf> (дата обращения: 20.11.2019).
3. Ефременко Н. Онтологии в DLP-системах третьего поколения // «Information Security/ Информационная безопасность». – 2009. – № 4. – С.32-33.
4. Метод повышения эффективности DLP-системы при семантическом анализе и категоризации информации / Кумунжиев К.В., Зверев И.Н. URL: <https://www.science-education.ru/pdf/2014/5/302.pdf> (Дата обращения: 21.11.2019).
5. Микрюков А.А., Бабаш А.В., Сизов В.А. Классификация событий в системах обеспечения информационной безопасности на основе нейросетевых технологий. Открытое образование. 2019;23(1):57-63. <https://doi.org/10.21686/1818-4243-2019-1-57-63> (Дата обращения: 21.11.2019).
6. Черняк Л. Семантический анализ на службе // Открытые системы. – 2010. – №10.
7. Comparing the best data loss prevention products Cyber Security Threats In 2017 That You Can't Just Ignore [Электронный ресурс]. URL: <http://searchsecurity.techtarget.com/feature/Comparing-the-best-data-lossprevention-products> (Дата обращения: 21.11.2019)
8. Cyber Security Threats in 2017 That You Can't Just Ignore [Электронный ресурс]. URL: <https://purplegriffon.com/blog/10-cyber-security-threats-in-2017> (Дата обращения: 21.11.2019).
9. Halenar Igor, Juhasova Bohuslava, Juhas Martin, Nesticky Martin. Application of Neural Networks in Computer Security. Procedia Engineering 69 (2014) 1209 – 1215.
10. Information Security Breaches Survey [Электронный ресурс]. URL: <https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf> (Дата обращения: 21.11.2019).
11. The biggest cyber security threat is inside your organisation [Электронный ресурс]. URL: <https://www.itgovernance.co.uk/blog/the-biggest-cyber-security-threat-is-inside-your-organisation/> (Дата обращения: 21.11.2019).
12. The Method For Increasing The Effectiveness Of Dlp-system With Semantic Analysis And Categorization Of Information [Электронный ресурс] URL: <https://www.science-education.ru/en/article/view?id=14741> (Дата обращения: 21.11.2019).

Научный руководитель: Марков А.С., доктор технических наук, профессор кафедры МГТУ им. Н.Э.Баумана

Exploring anomalies in user behavior

Sharsheeva J.²³²

Abstract. *The article considers algorithms and solutions to detect anomalies in user behavior and proposes models based on artificial neural network to detect an intruder. The peculiarities of training these systems and their application in practice are presented. It has been revealed the effective algorithms for model building.*

Keywords: *Artificial Neural Network, Abnormal Behavior.*

²³² Zhibek Sharsheyeva, Financial University under the Government of the Russian Federation, Moscow, jsharsheeva.rc@gmail.com

Методы построения малоресурсных систем защиты для 8-битных микроконтроллеров

Штанов Е.Ю.²³³, Поляков М.В.²³⁴

Аннотация. Рассматриваются методы построения малоресурсной системы защиты на 8-битных микроконтроллерах, которая базируется на криптосистемах ГОСТ Р 34.12-2015 «Магма» и Диффи-Хеллман на эллиптических кривых (ECDH). Для каждой из них приведены методы оптимизации, позволяющие ускорить работу системы и уменьшить затраты памяти. Их использование привело к ускорению шифрования данных в 11 раз и ускорению генерации ключа более чем 1.8 раза по сравнению с базовой конфигурацией. Результаты работы применимы к любой 8-битной платформе.

Ключевые слова: ГОСТ Р 34.12 – 2015 «Магма», ECDH, микроконтроллеры, блочные шифры, информационная безопасность, низкоресурсная криптография.

Введение

Развитие технологического прогресса привело к удешевлению электронных компонентов, и, как следствие, к повышению их доступности. На данный момент микроконтроллеры проникли во многие электронные устройства, объединив их в, так называемые, Интернет вещей (IoT), умные дома и т.д. Через данные устройства каждый день передается огромное количество информации, среди которых есть и конфиденциальные данные [1]. Ограниченность ресурсов таких устройств не позволяет применить классические методы защиты информации [2]. Необходимо использовать методы малоресурсной криптографии для максимальной экономии ресурсов устройства [3]. Для этого разрабатываемая система была разделена на две части – для шифрования передаваемых данных необходимо использовать симметричный алгоритм шифрования, поскольку их достоинством является скорость работы и нетребовательность к ресурсам [4, 5], по сравнению с ассиметричными алгоритмами. Основной же недостаток – проблема передачи ключа. Вторая часть системы направлена на решение данной задачи. Для преодоления данного недостатка необходимо использовать протокол согласования ключей ECDH. В качестве лабораторного стенда было использовано устройство, основанное на МК STM8L151C8T6.

Оптимизация ГОСТ Р 34.12-2015 «Магма»

Первая часть данной работы содержит в себя различные методы оптимизации симметричного алгоритма ГОСТ Р 34.12-2015 «Магма» [5, 6] при реализации на 8-битных микроконтроллерах [7].

Было создано четыре реализации алгоритма: 1) базовая, в которой алгоритм не был никак улучшен – именно с ней будут сравниваться остальные реализации; 2) ориентированная на скорость зашифрования/расшифрования; 3) ориентированная на сокращение используемой оперативной и энергонезависимой памяти устройства; 4) оптимальная, которая включила в себя лучшие решения из предыдущих реализаций.

Для создания реализации, ориентированной на скорость работы, были использованы следующие техники:

²³³ Штанов Евгений Юрьевич, Магистр НИЯУ МИФИ, Москва, evg.shtanov@gmail.com

²³⁴ Поляков Михаил Вадимович, Аспирант МГТУ им. Н. Э. Баумана, Москва, m.polyakov@bmstu.ru

1. Согласно алгоритму шифрования, результат сложения блока данных с ключом делится на восемь четырехбитных векторов. Ввиду особенностей архитектуры используемой платформы, было оптимально оперировать не восьмью четырехбитными векторами, а взять четыре восьмибитных вектора. Количество векторов, а, следовательно, пропусков через узел замены уменьшится в два раза. Для реализации подобного также необходимо изменить узел замены. Оригинальные узлы замены представляют собой двумерный массив размерностью 8 на 16, что суммарно дает 128 байт. Преобразование узла для уменьшения векторов приведет к расширению последнего до двумерного массива размерностью 4 на 256 и общим размером 1024 байта.

2. В процессе работы процедур зашифрования и выработки раундовых ключей активно используются циклы и ветвления, что ведет к частому использованию инструкции `call/jump`, что увеличивает накладные расходы. Для достижения максимальных показателей по скорости работы шифра предлагается произвести полную развертку циклов в коде.

3. После прохождения через S-блоки информационный вектор, представленный как 32-битное слово, циклически сдвигается на 11 разрядов влево. Для 8-битных микроконтроллеров циклический сдвиг 32-битного слова требует использования 4 регистров, а также аккумулятора для хранения переноса из одного 8-битного слова в другое. Логичным выглядит объединение всех четырех 8-битных регистров в 32-битное слово с учетом циклического сдвига.

Для создания реализации, ориентированной на экономию памяти, были использованы следующие техники:

1. При компиляции исходной версии алгоритма было замечено, что наибольшее количество памяти отводится для хранения байт-кода процедур. Кроме того, выделение операций зашифрования и выработки раундовых ключей в отдельные функции может привести, к их адресной удаленности, а также при оптимизации компилятора каждая процедура преобразуется отдельно, что не дает достичь максимальных показателей. Для уменьшения затрат памяти в данной реализации предлагается объединить функцию шифрования с функцией генерации ключей.

2. Также для данного алгоритма доступно уменьшение S блока с четырех векторов до одного.

Для создания оптимальной реализации, сбалансированной по скорости работы и объему занимаемой памяти, были использованы следующие техники:

1. При внимательном рассмотрении основной процедуры зашифрования/расшифрования алгоритма «Магма», видно, что в последнем раунде не происходит обмена половин информационного блока. Для экономии ресурсов на операции вызова предлагается изменить схему одного раунда алгоритма «Магма» (рис 1). Новая процедура будет содержать 2 раунда зашифрования и вызываться 16 раз.

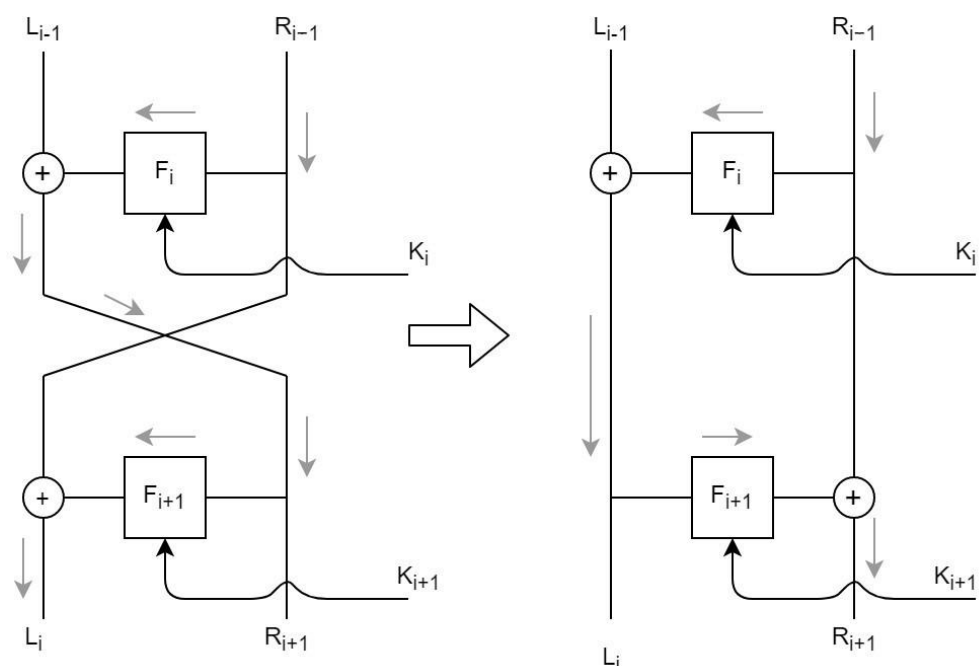


Рис.1. Изменение схемы шифрования

2. В данную реализацию мы также включили техники: применение композиции S-блоков под длину машинного слова, изменение алгоритма компоновки выходного вектора после пропуска через узел замены.

Оптимизация Диффи-Хелман на эллиптических кривых (ECDH)

Вторая часть работы посвящена техникам оптимизации протокола выработки общего ключа шифрования на основе эллиптических кривых. Для этого были созданы реализации в аффинных координатах и расширенных координатах Якоби. Показано, что применение специальных алгоритмов для арифметических операций, таких как «Быстрое вычисление модуля» (Fast Reduction Modulo P256) [8] для операции деления по модулю, улучшенный расширенный алгоритм Евклида [9] для поиска обратного элемента в поле F_p , алгоритм Монтгомери [10] для модульной арифметики [11], который базируется на двух переработанных операциях сложения XYCZ-ADD ($5M + 3S + 11A$) и XYCZ-ADDC ($5M + 3S + 16A$) и одной операции удвоения точек ($2M + 4S + 10A$) позволяет достичь существенного улучшения производительности. Тестирование проводилось на кривых $y^2 = x^3 + ax + b$ в сокращенной форме Вейерштрасса. Для эллиптических кривых такого вида возможно построить изоморфизм до расширенных координат Якоби.

Выводы

Применение вышеописанных методов для оптимизации алгоритма «Магма» позволяет ускорить процедуру зашифрования/расшифрования, а также уменьшить объем занимаемой памяти. В таблице 1 показаны результаты замеров работы «прямой» реализации без каких оптимизаций компилятора. В таблице 2 же представлены результаты работы оптимальной по скорости работы и затратам памяти реализации алгоритма с активированными флагами компилятора (максимальная оптимизация по скорости

Реализация “base” без оптимизации

Параметры	Без оптимизации		
	Функция шифр	Выработка ключей	
	Епс	Епс	Dec
Такты	110050	6457	6874
Время (с)	0.0177	0.0005	0.0005
Память	<pre> 1 694 bytes of readonly code memory 312 bytes of readonly data memory 583 bytes of readwrite data memory (+ 9 absolute) Размер: 1,95 КБ (2 006 байт) На диске: 4,00 КБ (4 096 байт) </pre>		

Таблица 3.

Реализация “optimal” с оптимизацией

Параметры	Без оптимизации		
	Функция шифр	Выработка ключей	
	Епс	Епс	Dec
Такты	10209	2208	2276
Время (с)	0.0016	0.0003	0.0003
Память	<pre> 1 466 bytes of readonly code memory 2 232 bytes of readonly data memory 583 bytes of readwrite data memory (+ 9 absolute) Расположение: D:\Main\Work\All\Магистратура\2 семестр\NIR\ Размер: 3,61 КБ (3 698 байт) На диске: 4,00 КБ (4 096 байт) </pre>		

Наглядно видно, что оптимальная реализация работает в 11 раз быстрее по сравнению с прямой реализацией алгоритма, при этом объем занимаемой постоянной памяти устройства составил всего 2 Кб (1/32 часть памяти микроконтроллера)

Время генерации секрета в координатах Якоби со всеми возможными улучшениями, занимает 15 секунд, время генерации ключа – 14. Это в 1.8 раза лучше, чем вычисления в аффинных координатах. Объем памяти, необходимый для данного алгоритма, равен 8.3 Кб. Результаты сравнения скорости работы в аффинах координатах и расширенных координатах Якоби приведены в Таблице 3.

Таблица 4.

Результаты замеров

МК	Время генерации ключа (с)	Время генерации секрета (с)	Объем занимаемой памяти (байт)	Объем прошивки (байт)
Аффинные координаты	26	26	6 160	6 615
Координаты Якоби	14	15	8 545	8 970

Литература

1. Poschmann A., Ling S., Wang H. 256 Bit Standardized Crypto for 650 GE GOST Revisited, In CHES 2010, Lecture Notes in Computer Science v. 6225, pp. 219-233, 2010.
2. S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, “Midori: A Block Cipher for Low Energy,” in Proceedings, Part II, of the 21st International Conference on Advances in Cryptology --- ASIACRYPT 2015 - Volume 9
3. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. №1(9). С. 26–43.
4. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. 2015. №2(10). С. 2–10.
5. Комарова А.В., Менщиков А.А., Коробейников А.Г. Анализ и сравнение алгоритмов цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 // Вопросы кибербезопасности. 2017. №1(19). С 51-55.
6. Dinur I., Dunkelman O., Shamir A. Improved Attacks on Full GOST. Report 2011/558, available via <http://eprint.iacr.org/>, 2011.
7. Poschmann A. Lightweight Cryptography - Cryptographic Engineering for a Pervasive World. Ph.D. Thesis, Ruhr University Bochum, 2009.
8. J. A. Solinas, “Generalized Mersenne Numbers,” Technical Report, Center for Applied Cryptographic Research. University of Waterloo, 1999.
9. Sheueling Chang Shantz. From Euclid’s GCD to Montgomery Multiplication to the Great Divide -2001- 13с.
10. P. L. Montgomery, “Modular Multiplication without Trial Division,” Mathematics of Computation, vol. 44, pp. 519—521, 1985.
11. Matthieu Rivain. Fast and Regular Algorithms for Scalar Multiplication over Elliptic Curves. -2011- 25 с.

Научный руководитель: Пудовкина Марина Александровна, доктор физико-математических наук, профессор, кафедры иу-8 МГТУ им. Н.Э. Баумана, maricap.go@mail.ru.

Methods for building low-resource protection systems for 8-bit microcontrollers

Shtanov E.²³⁵, Polyakov M.²³⁶

Abstract. *In this article we present some optimization techniques for implementation of low-resource cryptographic protection system on 8-bit microcontrollers. Our main goal was to achieve best results for GOST R 34.12-2015 “Magma” and Elliptic Curve Diffie-Hellman key exchange algorithm. Most of presented optimizations aimed on reduce memory usage and encryption speed up. We showed that by means of these techniques one can achieve 11 times faster overall performance and 1.8 faster ECDH key generation in comparison with “straight” implementation.*

Keywords: *GOST R 34.12-2015 “Magma”, ECDH, microcontrollers, block cipher, information security, lightweight cryptography.*

²³⁵ Evgeny Shtanov, master, National Research Nuclear University MEPhI, Moscow, evg.shtanov@gmail.com

²³⁶ Mikhail Polyakov, post-graduate student, Bauman Moscow State Technical University, Moscow, m.polyakov@bmstu.ru

Роль базовых систем ввода-вывода (UEFI BIOS) при оценке сценариев реализации угроз безопасности информации информационных систем
Язов Ю.К.²³⁷, Гефнер И.С.²³⁸

***Аннотация.** В статье отмечается актуальность вопросов защиты от угроз несанкционированных воздействий на базовые системы ввода-вывода с учетом их структурно-функциональных характеристик. Определены факторы, от которых зависит содержание сценариев реализации таких угроз, раскрыто содержание техник воздействия и возможные последствия.*

***Ключевые слова:** базовая система ввода/вывода, техника реализации угрозы безопасности информации, сценарий реализации угрозы безопасности информации, уязвимость.*

Введение

Высокие темпы развития информационных технологий, методов и программно-аппаратных средств обработки данных создают предпосылки для реализации целенаправленных угроз безопасности информации, при этом процесс реализации каждой угрозы состоит из нескольких этапов [1]. В частности, прежде чем реализовать целенаправленное несанкционированное или деструктивное воздействие злоумышленникам приходится выполнить подготовительные действия, включающие сбор сведений об атакуемой системе, получение доступа к системе, внедрение и управление вредоносным кодом, несанкционированные воздействия на информационную систему [2].

В целях противодействия целенаправленным угрозам безопасности информации специалистами по защите информации предложен сценарный подход [3], суть которого состоит в определении этапов реализации угроз безопасности информации (тактических задач) и технических задач (способов реализации тактических задач), решаемых нарушителем на каждом этапе. При этом каждый сценарий включает укрупненно три основных этапа, которые образуют жизненный цикл процесса реализации угрозы. Так, жизненный цикл компьютерной атаки включает в себя этапы:

- управления процессом реализации угрозы;
- доставки вредоносных программ, данных, кода и иных конструкций;
- реализации несанкционированного воздействия.

В качестве самостоятельных объектов воздействия угроз безопасности информации, как правило рассматривают компоненты систем, где хранится защищаемая информация (сервера, системы хранения базами данных), и компоненты систем, воздействие на которые нарушить функционирование системы (системы управления производством, web-сайты и др.) (рис.1).

Кроме того, при применении для оценки угроз сценарного подхода необходимо учитывать «вспомогательные» объекты воздействия угроз безопасности информации, за счет которых реализуются технические задачи.

Одним из таких вспомогательных объектов является базовая система ввода-вывода (UEFI BIOS) (далее – БСВВ). За счет того, что БСВВ функционирует на уровне аппаратной платформы и используется операционной системой для организации взаимодействия с

²³⁷ Язов Юрий Константинович, главный научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России», доктор технических наук, профессор, г. Воронеж.

²³⁸ Гефнер Ирина Сергеевна, начальник отдела Федеральной службы по техническому и экспортному контролю., г. Москва, igefner@yandex.ru

устройствами, через одну БСВВ можно проникнуть к любому элементу системы или информационно-телекоммуникационной сети (рис. 1).

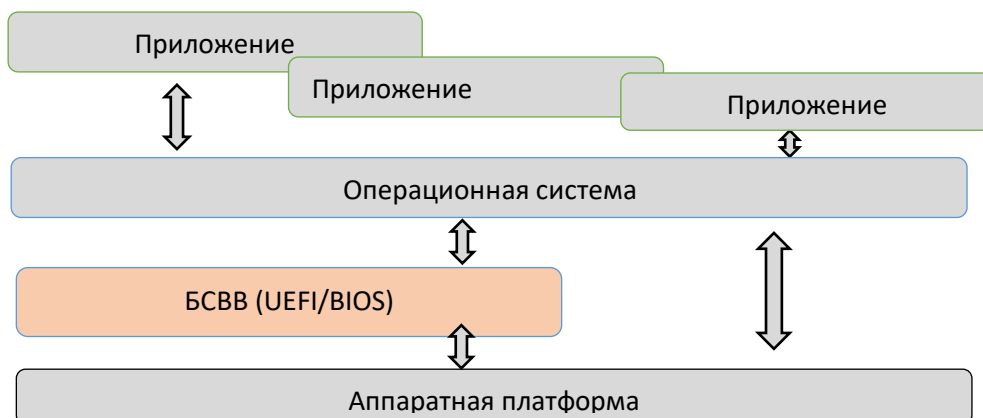


Рис.1. Расположение БСВВ в среде вычислительной техники

В результате за счет воздействия на БСВВ нарушителем может быть получен несанкционированный доступ к защищаемой информации, содержащихся в системе [4]. Учитывая изложенное, пресечение возможности сценариев реализации угроз безопасности информации за счет воздействия на БСВВ является актуальной задачей.

В открытых материалах содержится множество статей, где целевым объектом воздействия является БСВВ [5-8]. В данной статье предлагается рассмотреть БСВВ как «вспомогательный» объект воздействий при определении сценариев реализации угроз безопасности информации. При этом, как правило содержание сценария реализация угроз зависит от следующих факторов:

- архитектуры и особенностей функционирования системы;
- вида нарушителей безопасности информации;
- наличия подключений к сетям связи общего пользования;
- режимов обработки информации в системе и в ее отдельных сегментах.
- содержания возможных несанкционированных действий и вероятных последствий от реализации угроз.

На основании анализа принципов функционирования БСВВ [9-12], в качестве архитектурных и функциональных особенностей БСВВ, которые могут быть использованы для реализации технических задач являются:

- возможность модификации БСВВ на этапе создания и эксплуатации систем;
- доступность интерфейсов по настройке и управлению параметрами БСВВ;
- возможность сетевой загрузки;
- новый способ разметки жесткого диска (GPT);
- сервисы, которые функционируют время работы операционной (boot services и runtime services);
- применение криптографических алгоритмов;
- модульную архитектуру, позволяющую создавать пользовательские приложения в UEFI.

взаимодействие напрямую с аппаратными компонентами средства вычислительной техники (чипсетов, процессором и другими аппаратными компонентами средства вычислительной техники).

Учитывая модульность архитектуры БСВВ и открытость стандартов его построения, в сценариях реализации угроз безопасности могут быть задействованы следующие технические задачи на БСВВ:

- внедрение вредоносного кода на этапе создания и эксплуатации БСВВ;

внедрение вредоносного кода во время обновления БСВВ;
 изменение исполняемого кода сервисов БСВВ с последующим повышением уровня привилегий процессов и пользователей, обеспечением доступа к файлам операционной системы;

несанкционированная модификация БСВВ, осуществляемая посредством получения доступа к функциям микросхемы, где хранится БСВВ;

загрузка модифицированной прошивки БСВВ;

восстановление уязвимой версии БСВВ;

несанкционированное изменение настроек БСВВ и конфигурации устройства;

подмена ключей криптографических алгоритмов, являющих корневым элементом при проверке подлинности инициализируемых компонент устройства, угроза подмены аутентификационной информации, хранящейся в БСВВ;

получение несанкционированного доступа к привилегированному режиму процессора, из которого ему доступна на чтение и запись вся физическая память, через систему SMM.

Проанализировав возможные технические задачи на БСВВ, можно сделать вывод о возможности применения того или иной технической задачи сценария реализации угроз на этапах управление процессом реализации угрозы, доставки вредоносного кода, реализации несанкционированного воздействия (рис.2).

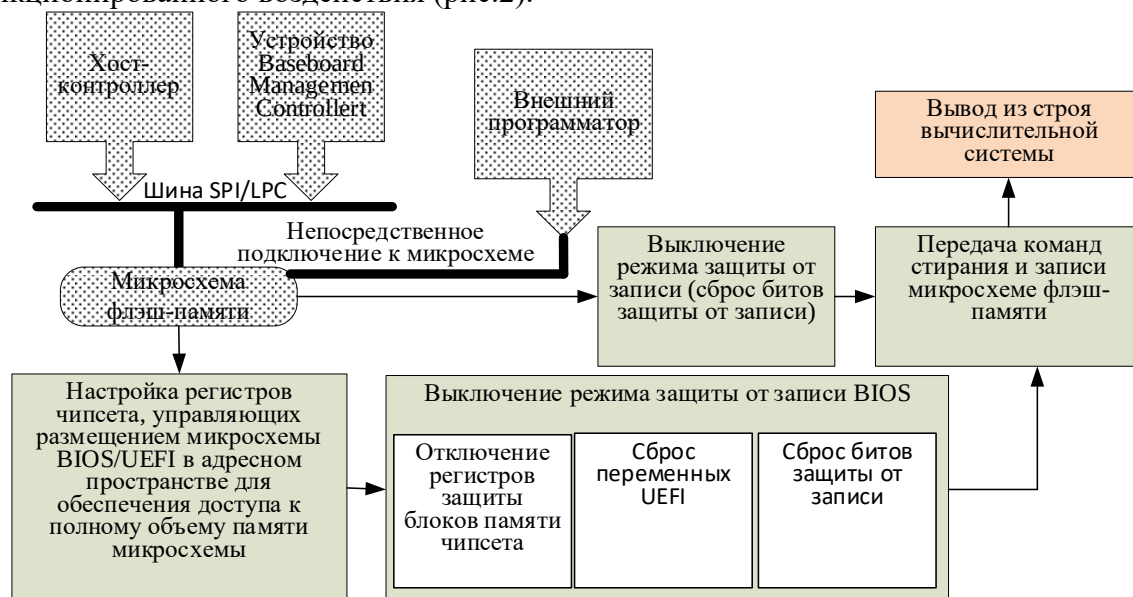


Рис.2. Пример технической задачи на БСВВ, приводящей к выводу из строя системы

Безусловно реализация рассматриваемых технических задач требует от нарушителя высокого уровня компетенции, разработки средств эксплуатации уязвимостей, однако успешная реализация техники на БСВВ, позволяет нарушителю получить максимальный уровень привилегий на микропрограммном уровне.

По результатам эксплуатации БСВВ возможны следующие последствия:

вывод из строя системы;

подмена (модификация) загрузчика операционной системы;

доступ к файловой системе;

перехват управления.

Таким образом, эксплуатация нарушителями технических задач на БСВВ создает серьезную угрозу безопасности информации, обрабатываемой в информационной системе, а область исследования техник воздействия при разнообразных сценариях реализации угроз

безопасности информации обуславливает необходимость постоянного внимания к ним, в том числе накопления сведений и поддержания их в актуальном состоянии. Принятие мер защиты информации, затрудняющих нарушителю воздействие на БСВВ, позволит минимизировать количество сценариев реализации угроз безопасности информации и существенно снизит возможности получения нарушителем максимальных прав доступа в систему.

Литература

1. Тершуков Д.А. Анализ современных угроз информационной безопасности. НБИ технологии, 2018, т.12, № 3. С. 6 -11.
2. Хлектова Д.Р., Попов К.Г. Общий цикл развития таргетированной атаки. Международный научный журнал «Символ науки» №7/2016. Режим доступа: <https://cyberleninka.ru/article/n/obschiy-tsikl-razvitiya-targetirovannoy-ataki/viewer>.
3. Климентьев К. Компьютерные вирусы и антивирусы. Взгляд программиста. – М.: ДМК Пресс, 2013. 656 с.
4. Зайцев О.В. Технология rootkit - современная угроза из прошлого // Защита информации. Инсайд. 2008. № 5 (23). С. 50-55.
5. Иванников П. В., Алтухов Н. О. Современные типы атак на BIOS. Молодежный научно-технический вестник, № 06, июнь, 2015. Режим доступа: <http://sntbul.bmstu.ru>.
6. Климентьев К. Компьютерные вирусы и антивирусы. Взгляд программиста. – М.: ДМК Пресс, 2013. 656 с.
7. Барабанов А.В., Гришин М.И., Кубарев А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых в вредоносных компьютерных программах // Вопросы кибербезопасности. 2014. № 4 (7). С. 41-48.
8. Марков А.С., Пугачев И.Б. Программный метод обеспечения безопасности загрузки операционной среды // Известия Института инженерной физики. 2009. Т. 1. № 11. С. 7-9.
9. Модестов А.А., Беляева Е.А. Комплексная оценка функциональных возможностей аппаратно-программных модулей доверенной загрузки // Вестник Российского нового университета. 2013. № 4. С. 105-107.
10. Авезова Я. Э., Фадин А. А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах//Вопросы кибербезопасности. -2016. -№ 1 (14). -С. 24-30.
11. Гефнер И.С. Особенности компьютерных атак на микропрограммном уровне. В сборнике: Безопасные информационные технологии. Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 118-121.
12. 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; номер заявки: 2010143450/08, опубл. 20.01.2011, Бюл. № 2. 2 с.

The role of UEFI BIOS in evaluation of scenarios for implementing information systems security threats

Yazov Yu.²³⁹, Gefner I.²⁴⁰

Abstract. Threats and attacks are considered at the level of the basic I / O system (UEFI / BIOS). account the structural and functional characteristics vulnerabilities of UEFI / BIOS. the article describes factors of scenarios for implementing information systems security threats.

Keywords: basic input / output system (UEFI / BIOS), attack, attack implementation objects, of scenarios for implementing information systems security threats, adversarial tactics, techniques.

²³⁹ Yazov Yuri, Dr.Sc., Professor, Federal Autonomous Institution "GNII PTZI FSTEC of Russia", Voronezh

²⁴⁰ Gefner Irina, Head of the Department of the Federal Service for Technical and Export Control, Moscow, igefer@yandex.ru

Моделирование значимых объектов критической информационной инфраструктуры в интересах исследования защищенности применяемых в них информационных технологий

Язов Ю.К.²⁴¹, Соловьев С.В.²⁴²

***Аннотация.** В докладе обоснована необходимость моделирования значимых объектов критической информационной инфраструктуры. Сделаны выводы о необходимости развития методов моделирования процессов реализации угроз и исследования путей построения эффективных систем защиты от них. Показана важность не только методического, но и информационного обеспечения исследований защищенности значимых объектов.*

***Ключевые слова:** критически важные объекты, концептуальное моделирование.*

Введение

Необходимость моделирования значимых объектов критической информационной инфраструктуры (ЗО КИИ) [1-11] в интересах исследования защищенности применяемых в них информационных технологий обусловлена следующими обстоятельствами:

во-первых, проводить такие исследования на функционирующих объектах, как правило, недопустимо из-за реальной возможности нарушения их функционирования;

во-вторых, разработка моделей позволяет целенаправленно исследовать процессы реализации конкретных угроз нарушения функционирования ЗО КИИ с варьированием условий такой реализации и параметров моделируемых процессов;

в-третьих, в ходе исследований на моделях может быть собрана состоятельная статистика для процессов реализации угроз для конкретных классов и типов ЗО КИИ, что весьма важно для анализа их защищенности, но сложно сделать для реальных объектов и связано со значительными временными затратами;

в-четвертых, в ходе исследований на моделях могут быть выявлены новые угрозы безопасности информации и способы их реализации, новые уязвимости системного и прикладного программного обеспечения ЗО КИИ, что на функционирующих объектах сделать практически невозможно;

в-пятых, на моделях могут обосновываться требования к параметрам настройки программных и программно-аппаратных средств ЗО КИИ, состав и характеристики средств защиты информации, подлежащих применению на значимых объектах критической инфраструктуры, и требования к ним и др.

Моделирование может осуществляться на специально разрабатываемых программно-аппаратных макетах, как правило, отдельных сегментов значимого объекта или с использованием различных имитационных и аналитических моделей исследуемых процессов. При этом учитываются разнообразные перспективные технологии, которые уже применяются или применение которых ожидается на ЗО КИИ (табл. 1).

²⁴¹ Язов Юрий Константинович, главный научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России», доктор технических наук, профессор, г. Воронеж.

²⁴² Соловьев С.В., кандидат технических наук, доцент

Таблица 1.

Примеры перспективных технологий, применение которых планируется на значимых объектах критической информационной инфраструктуры

Наименование перспективной технологии	Примеры объектов, на которых планируется применение перспективных технологий
Промышленная виртуализация	Амурский газохимический комплекс, цех производства этилена, планируются к внедрению (химическая промышленность, ТЭК)
Промышленный интернет вещей (IIoT)	Система eSOMS (electronic Shift Operations Management System – электронная система управления сменой по эксплуатации), Смоленская и Нововоронежская АЭС»(Энергетика)
Цифровые двойники	Цифровой двойник установки гидроочистки каталитического крекинга на Московском НПЗ. (Нефтеперерабатывающая промышленность)
Технологии «умных сетей» (Smart Grid, «цифровая подстанция»)	Система автоматизированной защиты и управления электрической подстанцией нового поколения (АСЗУ iSAS) на цифровой подстанции «Южная», г. Череповец (Энергетика)
Технологии больших данных (Big Data)	Автоматизированная система слежения и контроля процессов - АС СКП «Технология» для ПАО «Северсталь» (Металлургическая промышленность)
Технология распределенных баз данных	Система оплаты заправки воздушных судов Smart fuel
Технологии робототехники и сенсорики	ЗО КИИ практически во всех отраслях промышленности

Вместе с тем, разработка и применение программно-аппаратных макетов для проведения указанных исследований является весьма затратным и долговременным. Это обуславливает целесообразность их применение, в основном, в случаях, когда другими путями исследовать защищенность ЗО КИИ с заданным уровнем достоверности получаемых результатов не представляется возможным.

Для проведения исследований защищенности ЗО КИИ от угроз безопасности информации сегодня частично развернут и активно расширяется комплекс программных и программно-аппаратных средств, включающий в себя подсистемы:

мониторинга, сбора и анализа данных об угрозах безопасности информации, сведения о которых опубликованы в различных издательствах и в сети Internet, об уязвимостях системного и прикладного программного обеспечения функционирования ЗО КИИ и о предлагаемых в публикациях мерах защиты от разнообразных угроз, в том числе применительно к новым информационным технологиям и др.;

анализа средств реализации компьютерных атак и эксплуатации уязвимостей;

прогнозирования появления новых угроз безопасности информации на основе ретроспективного анализа трендов появления инцидентов безопасности для различных классов ЗО КИИ, результатов исследований уязвимостей программного обеспечения и др.;

моделирования процессов функционирования фрагментов ЗО КИИ и процессов реализации угроз безопасности информации, приводящей к нарушению функционирования ЗО КИИ или утечки критически важной информации о них;

административную подсистему, предназначенную для ведения банка данных угроз безопасности ФСТЭК России (БДУ), подготовки рекомендаций по парированию выявленных угроз или устранению уязвимостей, организации оповещения заинтересованных инстанций о результатах исследований защищенности ЗО КИИ.

Сведения, полученные в ходе исследования защищенности ЗО КИИ, помещаются в определенном формате в БДУ ФСТЭК России и используются в интересах совершенствования или проектирования систем защиты ЗО КИИ, в том числе в случае применения новых информационных технологий.

Сложившееся сегодня представление о требуемых исходных данных, порядке и ожидаемых результатах моделирования значимых объектов критической информационной инфраструктуры в интересах исследования их защищенности, наработанный определенный опыт ведения БДУ ФСТЭК России показали необходимость интенсивного развития как соответствующего методического, так и информационного обеспечения ведения БДУ (рис. 1).

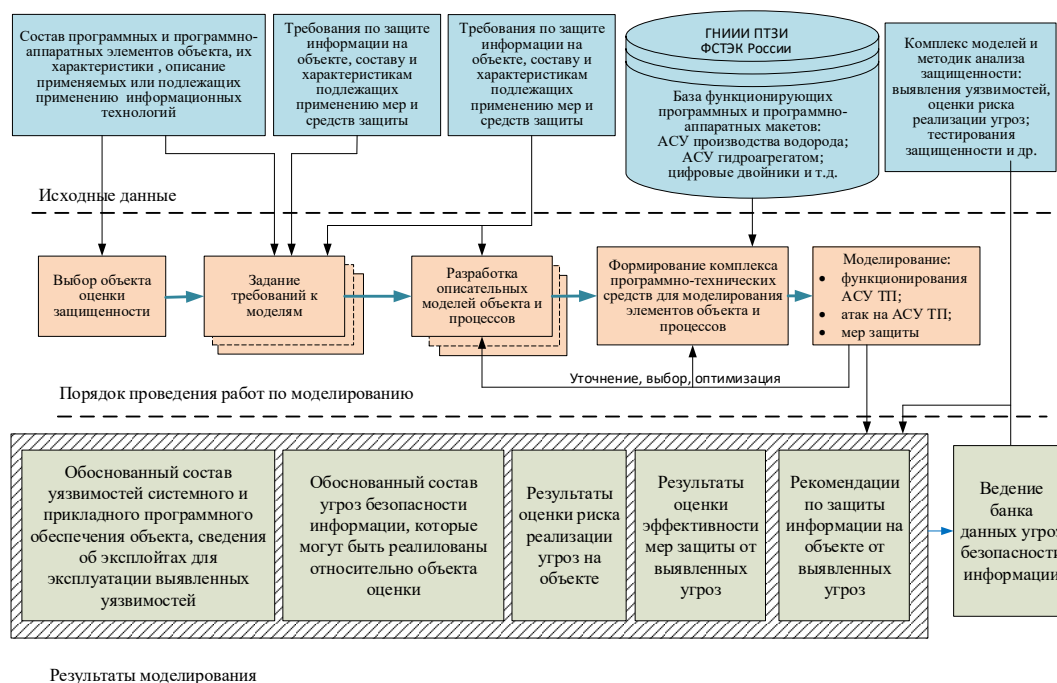


Рис. 1. Исходные данные, порядок и результаты моделирования

Методическое обеспечение ведения БДУ – это обширный комплекс моделей и методик, который должен охватывать все задачи, решаемые в каждой из указанных подсистем БДУ. Однако сегодня такое обеспечение находится в начальной стадии разработки и здесь есть определенные проблемы, связанные с созданием имитационных и аналитических моделей как процессов функционирования фрагментов ЗО КИИ, так и процессов реализации угроз безопасности информации в них. К основным проблемным вопросам при этом относятся следующие:

1) отсутствие методологии формирования риск-моделей процессов функционирования ЗО КИИ в условиях реализации весьма разнообразных и многочисленных угроз безопасности информации, позволяющих на количественной основе оценивать как возможность реализации угроз с учетом фактора времени, так и возможный ущерб от такой реализации;

2) парирование неопределенностей относительно способов реализации угроз, связанных с большим количеством возможных вариантов развития моделируемых процессов, способов преодоления применяемых мер защиты в ходе реализации угроз, с использованием уязвимостей «нулевого дня», с количественной оценкой влияния мер и средств защиты на процессы реализации угроз и зависимостью такого влияния от многочисленных настроек как программного обеспечения ЗО КИИ, так и самих средств защиты и т.д.;

3) необходимость весьма частой корректировки моделей в связи с высокой динамикой изменений состава и характеристик угроз безопасности информации.

Весьма значительные сложности как организационного, так и методического характера имеют место и в информационном обеспечении ведения БДУ. Прежде всего, это касается развития методов анализа контента по результатам сканирования интернет-пространства, разработки соответствующих экспертных систем с технологиями типа Data Mining, позволяющих в автоматизированном режиме осуществлять поиск взаимосвязей в «сырых» данных, выявлять по косвенным признакам необходимые сведения (например, об инцидентах безопасности, о создании новых средств реализации сетевых атак и вредоносных программ, о новых уязвимостях программного обеспечения и эксплойтах для их эксплуатации, о компаниях, занимающихся разработкой способов и средств реализации угроз безопасности информации и, прежде всего, относительно ЗО КИИ и др.). Однако информационное обеспечение ведения БДУ охватывает также и вопросы:

сбора и систематизации сведений о самих ЗО КИИ, а это далеко не простая задача в силу огромного количества и разнообразия таких объектов;

прогнозирования развития информационных технологий для реализации в ЗО КИИ;

ведения базы данных о мерах средствах защиты информации, которые применяют или планируют применять на таких объектах, об опыте построения систем защиты;

ведения базы данных по результатам контроля защищенности информации в ЗО КИИ, сертификации разрабатываемых и подлежащих применению новых средств защиты;

прогнозирования развития новых технологий защиты информации и оценки возможности их применения в ЗО КИИ

ведения базы данных по документам, регламентирующим требования по защите информации, предъявляемым как со стороны уполномоченных федеральных органов исполнительной власти, так и отраслевых структур и др.

Наконец самостоятельными вопросами ведения БДУ в условиях, когда необходимо оповещать многочисленные заинтересованные инстанции о результатах анализа защищенности ЗО КИИ, оперативно получать данные о самих объектах, ежедневное сканировать Internet-пространство и т.п., является защита соответствующих передаваемых сведений, а также исключение и затруднение возможности анализа деятельности по ведению БДУ.

Для передачи сведений заинтересованным инстанциям, как правило, используется Internet или отчуждаемые носители информации (CD-диски, флэш-память). Защита в этом случае в основном является криптографической. А вот для парирования попыток отслеживания деятельности по поиску информации на сайтах Internet целесообразно использовать опыт зарубежных организаций и спецслужб, где активно применяются, например, средства анонимизации, скрывания следов поиска и т.п.

Таким образом, интенсивное внедрение новых информационных технологий и их применение в ЗО КИИ, постоянно растущее количество угроз безопасности информации и невозможность проведения анализа ее защищенности на функционирующих объектах обуславливает острую необходимость развития методов моделирования процессов реализации угроз и исследования путей построения эффективных систем защиты от них.

Вместе с тем, опыт ведения БДУ ФСТЭК России и моделирования указанных процессов показал важность не только методического, но и информационного обеспечения исследований защищенности ЗО КИИ, что обуславливает решение широкого круга вопросов проблемного характера, связанных как со сбором и систематизацией сведений о самих ЗО КИИ и ведения соответствующих баз данных, так и прогнозированием развития и применения новых информационных технологий для реализации в ЗО КИИ, а также новых технологий защиты критически важной информации в них.

Литература

1. Алпеев А.С. Критически важные объекты. Терминология безопасности//Вопросы кибербезопасности. 2016. № 4 (17). С. 72-76.
2. Госькова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. №2. С.42-49. DOI: 10.21681/2311-3456-2019-2-42-49
3. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. №2. С. 2-15. DOI: 10.21681/2311-3456-2018-2-2-15
4. Калашников А.О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации // Вопросы кибербезопасности. 2014. № 3(4). С. 35-41.
5. Климов С.М., Поликарпов С.В., Рыжов Б.С., Тихонов Р.И., Шпырня И.В. Методика обеспечения устойчивости функционирования критической информационной инфраструктур в условиях информационных воздействий // Вопросы кибербезопасности. 2019. №6, 2019, С. 37-48.
6. Крюков Р.О., Глыбовский П.А., Фоменко К.Э. Модель взаимодействия элементов критической информационной инфраструктуры на основе онтологического подхода // Защита информации. Инсайд. 2020. № 3 (93). С. 20-23.
7. Кубарев А.В., Лапсарь А.П., Федорова Я.В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1. С. 8-17. DOI: 10.21681/2311-3456-2020-01-08-17
8. Петренко А.С., Петренко С.А. О кибербезопасности АСУ ТП транспортной инфраструктуры//Защита информации. Инсайд. 2017. № 6 (78). С. 38-43.
9. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1 (1). С. 17-27.
10. Probabilistic Modeling in System Engineering. / By ed. A.Kostogryzov, - London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
11. Барабанов А.В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. 2011. № 3. С. 48-52.

Simulation of Significant Objects of Critical Information Infrastructure in the Interest of Investigating the Security of Information Technologies Used Therein

Yazov Y.K.²⁴³, Solovyov S.V.²⁴⁴

Abstract. *The report substantiates the necessity of modeling of significant objects of critical information infrastructure. Conclusions about the need to develop methods for modeling processes of implementation of threats and research ways to build effective protection systems against them were made. Shows the importance of not only methodological, but also information support for research security of critical objects.*

Keywords: *critical facilities, conceptual modeling.*

²⁴³ Yazov Yuri, Dr.Sc., Professor, Federal Autonomous Institution "GNII PTZI FSTEC of Russia", Voronezh

²⁴⁴ Solovyov S.V., Ph.D., Associate Professor

О решении одной задачи олимпиады NSUCrypto'2019 и разделениях функций многих переменных над конечными полями

Чиликов А.А.²⁴⁵

В настоящей работе исследуются неполные разделения булевых отображений. Техника разделений функций и отображений используется для создания реализаций криптографических алгоритмов, защищенных от атак по побочным каналам. В рамках данной работы дано полное описание множества функций от n переменных, допускающих разделения на функции от $n-1$ переменной. Полученные результаты справедливы не только для булевых отображений, но и для отображений над произвольным конечным полем.

Ключевые слова: разделения функций, атаки по побочным каналам, маскировка

Введение

Международная Олимпиада по криптографии NSUCrypto проводится с 2014 года, и является одним из интереснейших мероприятий в мире криптографии. Главной площадкой и организатором олимпиады является Новосибирский Государственный Университет. В состав жюри входят авторитетные специалисты-криптографы из России и стран ближнего и дальнего зарубежья. В олимпиаде могут принять участие все интересующиеся криптографией - от школьников до профессионалов-криптографов (разумеется, призовой зачет в этих категориях раздельный).

Для решения участникам предлагаются задачи различного уровня сложности, в том числе и открытые математические проблемы. За первые семь лет участникам было дано около двадцати задач, отмеченных организаторами как нерешенные. По многим из них в ходе олимпиады были достигнуты интересные продвижения. Эти продвижения, вместе с остальными результатами, публикуются и обсуждаются в отчетных публикациях организаторов ([1],[2], [3]).

В 2019 году в качестве задачи 2 второго раунда была предложена задача об описании "неполных разделений" булевых отображений многих переменных. Эта задача была отмечена как нерешенная. В итоговом отчете ([3]) организаторы отметили продвижения, достигнутые некоторыми командами. Однако полного решения так и не было предложено.

Таким образом, насколько нам известно, данная задача считается нерешенной. В рамках данной работы мы исследуем близкий класс объектов - "слабые неполные разделения". Предложено полное описание данного класса объектов. Приводимые результаты справедливы не только для случая булевых функций, но и для случая функций многих переменных над произвольным конечным полем.

Данная работа была проведена с помощью Российского Научного Фонда Грант N 17-11-01377.

Основные конструкции

Определение 1. Пусть K – конечное поле, $V = K^n$ – конечномерное линейное пространство над K . Пусть f – обратимая функция из V в V и $F = \langle F_1, \dots, F_n \rangle$ – биективное отображение из V^n в V^n . Тогда

1) F называется n -разделением (n -sharing) для f , если для любого набора $(x_1, \dots, x_n) \in V^n$ выполняется равенство

²⁴⁵ Чиликов А.А., доцент МГТУ им. Н.Э.Баумана, chilikov@passware.com

$$f\left(\sum_{i=1}^n x_i\right) = \sum_{i=1}^n F_i(x_1, \dots, x_n) \quad (1)$$

2) F называется неполным n-разделением (non-complete n-sharing) для f, если оно является n-разделением для f, и при этом для любого $i \in \{1, \dots, n\}$ компонента F_i не зависит существенно от переменной x_i .

Задача, исходно поставленная на NSUCrypto'2019, состояла из трех подзадач:

1) по известному n-разделению функции $f(x)$ построить n-разделение для функции $g(x) = Af(Bx)$, где A, B - аффинные преобразования

2) описать множество отображений $V \rightarrow V$, $V = F24$, для которых существуют n-разделения при $n = 3, 4$

3) обобщить результаты пункта 2 на случай $V = F25$ и $V = F26$

Из постановки задачи логично предположить, что авторы подразумевали некое численное решение. Однако в данном случае общеалгебраический подход оказывается более продуктивным. В рамках данной работы мы получим более общий результат, а именно - полное описание отображений, для которых существуют "слабые неполные n-разделения". При этом областью определения и областью значений для этих отображений будут произвольные векторные пространства над произвольным конечным полем (не обязательно F2).

Отметим, что первый пункт не представляет особой сложности, однако служит полезным инструментом для получения дальнейших результатов.

Определение 2. Пусть K – конечное поле, $V = K^m$ – конечномерное линейное пространство над K. Пусть f – обратимая функция из V в V и $F = \langle F_1, \dots, F_n \rangle$ – произвольное отображение из V^n в V^n . Тогда

1) F называется слабым n-разделением (weak n-sharing) для f, если для любого набора $(x_1, \dots, x_n) \in V^n$ выполняется равенство (1).

2) F называется слабым неполным n-разделением (weak non-complete n-sharing) для f, если оно является n-разделением для f, и при этом для любого $i \in \{1, \dots, n\}$ компонента F_i не зависит существенно от переменной x_i .

Иными словами, "настоящие" разделения превращаются в "слабые" при отбрасывании требования обратимости. Или же, формально более точно, "настоящее" n-разделение есть частный случай "слабого" с дополнительным условием обратимости f и F.

Требование "неполноты" разделения является критически важным, поскольку без него задача становится тривиальной. В самом деле, любая функция

$f(x)$ может быть представлена слабым n-разделением $F_1(x_1, \dots, x_n) = f(x_1 + \dots + x_n)$, $F_i(x_1, \dots, x_n) = 0$ при $i = 2, \dots, n$. Оно небиективно, но проблема легко решается: $F_i(x_1, \dots,$

$x_n) = x_i$ при $i = 2, \dots, n$ и $F_1(x_1, \dots, x_n) = f(x_1 + \dots + x_n) - \sum_{i=2}^n x_i$ – будет "настоящим" n-

разделением. Таким образом, разделения, не являющиеся неполными, не представляют значительного интереса с точки зрения математики. Поэтому далее мы будем исследовать исключительно неполные разделения.

Правило гиперкуба

Будем обозначать через $\|x\|$ вес Хэмминга вектора x. Также пусть

$$\delta_\sigma(x) = \begin{cases} x, & \text{если } \sigma = 1 \\ 0, & \text{если } \sigma = 0 \end{cases}$$

и

$$\Delta_{\sigma}(x) = \langle \delta_{\sigma_1}(x_1), \dots, \delta_{\sigma_n}(x_n) \rangle$$

Имеет место следующий факт:

Теорема 1. Пусть V – линейное пространство над полем K , $f: V \rightarrow V$ – произвольная функция, и существует слабое неполное n -разделение $F = \langle F_1, \dots, F_n \rangle$ для f . Тогда для f выполняется следующее равенство ("правило гиперкуба"):

$$\sum_{\sigma \in \{0,1\}^n} (-1)^{|\sigma|} \cdot f\left(\sum_{i=1}^n \delta_{\sigma_i}(x_i)\right) = 0 \quad (2)$$

для любых $x_1, \dots, x_n \in V$. Более того, выполнение данного соотношения является необходимым и достаточным условием существования слабого неполного n -разделения.

Отображения, для которых выполняются требования Теоремы 1 (правило гиперкуба) далее мы будем называть n -гиперкубическими.

n -разделения, АНФ и расширения конечных полей

Как мы установили выше, "правило гиперкуба" является необходимым и достаточным условием существования слабого неполного n -разделения. Однако остается неясным, как по виду функции f эффективно проверить выполнение этого условия. Целью данного раздела будет получение эффективного алгоритма такой проверки.

Для решения этой задачи нам потребуется ввести еще несколько полезных определений.

Определение 3. Пусть K – конечное поле, $V = K^m$ – конечномерное линейное пространство над K , $f: V \rightarrow V$ – произвольная функция. Для любого $t \in V$ определим " t -разность" $\Delta_t f$ по правилу $(\Delta_t f)(x) = f(x+t) - f(x)$

Лемма 1

Пусть K – конечное поле, $V = K^m$ – конечномерное линейное пространство над K . Тогда функция $f: V \rightarrow V$ удовлетворяет правилу гиперкуба для n тогда и только тогда, когда для любого $t \rightarrow V$ функция $\Delta_t f$ удовлетворяет правилу гиперкуба для $(n-1)$.

Теперь введем еще одно определение:

Определение 4. Пусть $p = \text{char } F_q$ – характеристика основного поля (т.е. $q = p^k$). Тогда

- 1) p -адическим весом $\text{wp}(n)$ целого числа n назовем сумму цифр в его p -ичной записи
- 2) p -адическим весом $\text{wp}(x^n)$ монома x^n назовем $\text{wp}(n)$
- 3) p -адическим весом $\text{wp}(f)$ многочлена $f(x) \neq 0$ назовем максимальный из весов входящих в него мономов

Вес нулевой функции, вообще говоря, не определен. Но для наших целей можно положить его равным -1 (или же любому отрицательному целому числу).

Лемма 2. Пусть $p = \text{char } F_q$ – характеристика основного поля (т.е. $q = p^k$). Тогда для любого $t \in F_q^m$ и любого $f: F_q^m \rightarrow F_q^m$ выполнено

$$\text{wp}(\Delta_t f) \leq \text{wp}(f) - 1$$

Теперь мы готовы доказать следующий факт:

Теорема 2. Пусть $f: F_q^m \rightarrow F_q^m$ и $p = \text{char } F_q^m$. Тогда f имеет слабое неполное n -разделение в том и только том случае, когда $\text{wp}(f) \leq n-1$.

Интересным следствием Теоремы 2 является следующий факт:

Следствие. Преобразование, задаваемое S -блоком шифра AES имеет слабое неполное 8-разделение, но не имеет неполных 7-разделений.

Заключение

В настоящей работе получен эффективно проверяемый критерий представимости отображения в виде суммы отображений от меньшего числа переменных. Указанный

критерий может быть использован для построения реализаций криптографических алгоритмов, защищенных от атак по побочным каналам.

Литература

1. N. Tokareva, A. Gorodilova, S. Agievich, V. Idrisova, N. Kolomeec, A. Kutsenko, A. Oblaukhov, G. Shushuev. Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography. Прикладная дискретная математика, 2018, № 40, с. 34-58
2. A. Gorodilova, S. Agievich, C. Carlet, E. Gorkunov, V. Idrisova, N. Kolomeec, A. Kutsenko, S. Nikova, A. Oblaukhov, S. Picek, B. Preneel, V. Rijmen, N. Tokareva. Problems and solutions of the Fourth International Students' Olympiad in Cryptography NSUCRYPTO. <https://arxiv.org/abs/1806.02059>
3. А. А. Городилова, Н. Н. Токарева, С. В. Агиевич, К. Карле, Е. В. Горкунова, В. А. Идрисова, Н. А. Коломеец, А. В. Куценко, Р. К. Лебедев, С. Никова, А. К. Облаухов, И. А. Панкратова, М. А. Пудовкина, В. Реймен, А. Н. Удовенко. О шестой международной олимпиаде по криптографии NSUCRYPTO. Дискретн. анализ и исслед. опер., 2020, том 27, выпуск 4, страницы 21–57

About one problem from NSUCrypto'2019 and n -sharings of multivariate mappings over finite fields

Chilikov A. A.

In this work we consider a non-complete n -sharings of the boolean mappings The sharing technique is a very useful for design a "secure cryptosystems" which are resisted by side-channel attacks. But not any mapping can be represented as a sharing. In this work we provide a complete description of the set of mappings which could be represented as an $(n-1)$ sharing. These results are true not only for binary fields but for any finite fields.

Keywords: n -sharings, side-channel attacks, masking

Оглавление

1. Авдонин Р.Ю. , Костокрызов А.И. , Нистратов А.А. Вероятностная оценка рисков для реализации процесса управления человеческими ресурсами системы.....	2
2. Авдонин Р.Ю. , Костокрызов А.И. , Нистратов А.А. Методы анализа рисков для процесса управления знаниями о системе.....	12
3. Аносов С.С., Шахалов И.Ю. Оценка информационного риска методом декомпозиции и анализа сетевых и иерархических структур	20
4. Барабанов А.В. Method for collecting architecture security-specific information for microservice-based systems.....	27
5. Басараб М.А., Троицкий И.И., Онуфриева Е.В. Исследование функционирования SIEM - систем с помощью различных корреляторов для бинарных последовательностей вида (1, -1) при условии, что случайные величины принимают свои значения с одинаковыми вероятностями	32
6. Бельфер Р.А., Кравцов А.В. Разработка учебного имитатора объединенной сети передачи данных категории специального назначения	37
7. Бондарев В.В. Методика оценки угроз безопасности информации	49
8. Бураков А.Г., Полосухин Н.В. Подход к повышению оперативности обработки исполняемых файлов специалистами по компьютерной криминалистике	54
9. Быков А.Ю., Гришунин М.В., Федоров Е.Г., Маркова И.А. Алгоритм поиска седловой точки в игровой задаче выбора программных средств защиты информации для серверов вычислительной сети.....	59
10. Варфоломеев А.А. Некоторые методические замечания к российским криптографическим стандартам ГОСТ Р 34.10 и ГОСТ Р 34.12.....	66
11. Ворончихин И.С., Соколовский С.П. Асимптотическая устойчивости модели динамического конфигурирования структуры вычислительных сетей.....	70
12. Горбачев А.А., Соколовский С.П. Модель защиты сервиса электронной почты от сетевой разведки управлением параметрами передачи сообщений	77
13. Гордеев Э.Н., Леонтьев В.К. Зависимость среднего числа решений в задаче о ранце от параметров области ограничений	85
14. Горшков Ю.Г. Анализ засекреченных сигналов телефонных шифраторов	91
15. Гребнев С.В., Ключарёв П.Г., Коренева А.М., Кошелев Д.И., Тараскин О.Г., Тулебаев А.И. Постквантовый криптографический протокол выработки общего ключа, основанный на изогениях суперсингулярных эллиптических кривых.....	99
16. Дамдинова Т.Ц. Усовершенствование метода обработки граничных точек в задачах анализа изображений	104
17. Жуков А.Е. Клеточные автоматы и запреты булевых функций	108
18. Зеленецкий А.С. Исследование булевых функций с аффинными аннигиляторами..	120
19. Зимин Е.Е. Методика фаззинг-тестирования кода с помощью AFL	124
20. Казанцев И.С. О возможном подходе к аутентификации пользователя по клавиатурному почерку на основе ПЭМИ клавиатуры	130

21. Ключарёв П.Г. О криптографических алгоритмах, основанных на обобщенных клеточных автоматах, и перспективах их применения	135
22. Козачок А.В., Копылов С.А., Гайнов А.Е., Кондратьев Б.В. Модель стеганографического канала, основанного на использовании текстового стеганографического контейнера.....	139
23. Козачок А.В. , Кочетков Е.В. Многоуровневая модель политики безопасности управления доступом операционных систем семейства Windows.....	146
24. Козачок А.В., Спирин А.А. Моделирование псевдослучайных последовательностей, сформированных алгоритмами шифрования и сжатия данных.....	153
25. Козлов А.А. Разработка низкоресурсного блочного стохастического преобразования на базе ARX конструкции для обеспечения универсальной защиты информации, пересылаемой по каналу связи	159
26. Коннова Н.С, Сафина А.Д. Использование нейросетевых методов и атомарных функций в задаче биометрической аутентификации по ЭКГ.....	165
27. Корнеев Н.В., Сафин И.Р. Анализ информационной безопасности объектов критической информационной инфраструктуры на базе информационно-энергетического подхода	173
28. Костогрызов А.И. Подход к анализу влияния защищенности информации на реализацию процесса управления решениями	178
29. Кривошеева Д.А., Булдакова Т.И. Сетевое взаимодействие в телемедицинской системе	189
30. Ларин В.С. Улучшение метода аутентификации в алгоритме WPA2-PSK WI-FI.....	195
31. Малахов М.В., Воронина Е.Н. Методика разделения областей кода и данных в образе встраиваемого программного обеспечения контроллеров архитектуры ARM	199
32. Маркин Д.О., Миначев В.М. Средство распознавания полиморфных эксплойтов для ARM-систем на основе поведенческих признаков	205
33. Маркин Д.О., Архипов М.А. Средство идентификации признаков полиморфного программного обеспечения для ARM-систем на основе статических признаков	213
34. Маркин Д.О., Козин С.С. Система позиционирования подвижных источников радиосигналов на основе методов прогнозирования.....	220
35. Маркин Д.О., Хо Т. Ч. Подход по оцениванию уровня защищенности информации, обрабатываемой программным обеспечением доверенных сред исполнения на основе технологии TrustZone.....	229
36. Медведев Н.В., Карташова Ж.К. Профиль защиты для бортовой ОС реального времени	237
37. Медведев Н.В., Завадская Т.Е. Методика учета утечки излучения в оптическом волокне.....	243
38. Медведев Н.В., Глинская Е.В. Информационная безопасность бортовой операционной системы гражданского воздушного судна с учетом требований ГОСТ Р ИСО/МЭК 15408.....	249

39. Нистратов А.А. Подход к интеграции разнородных рисков на примере анализа целей, задач и угроз по доктрине энергетической безопасности	255
40. Осипова Н.С. Применение методов машинного обучения при проведении фаззинг-тестирования.....	263
41. Поляков М.В. Применение алгоритма Саймона для поиска линейных структур булевых отображений	270
42. Проскурин А.А., Яндашевская Э.А. Подсистема стегоанализа цифровых изображений на основе сверточной нейронной сети	276
43. Ревенков П.В., Бердюгин А.А., Макеев П.В. Оценка риска нарушения кибербезопасности в коммерческом банке (на примере атак на банкоматы “Brute force” и “Black box”)	282
44. Ромашкина Н.П. Стратегические проблемы применения информационно-коммуникационных технологий в военно-политической сфере.....	290
45. Северов В.С. Методы тестирования программного обеспечения для повышения безопасности продукта.....	296
46. Соколова А.В. Обеспечение защиты сетевых ресурсов в телемедицинской системе наблюдения пациентов с деменцией	301
47. Тарапанова Е.А., Бойко Е.В. Биометрические технологии аутентификации	306
48. Татаренков В.С. Обзор компьютерных атак на биометрические системы	318
49. Чеверкалов В.А. Сравнительный анализ методик атрибуции кибератак.....	326
50. Чемоданов Н.С., Гордеев Э.Н. Об одной модификации известной апробированной системы распознавания лиц	331
51. Шайтура С.В., Минитаева А.М., Сумзина Л.В., Максимов А.В. Система безопасности объектов с использованием трехмерной визуализации	336
52. Шевадронов А.С., Киселев В.В., Бабиченко О.А. Масштабирование размеров команд и управления правами доступа в групповых исследованиях по сетевому моделированию с использованием технологии биометрической идентификации.....	340
53. Шаршеева Ж. Исследование аномалий в поведении пользователей	346
54. Штанов Е.Ю., Поляков М.В. Методы построения малоресурсных систем защиты для 8-битных микроконтроллеров.....	352
55. Язов Ю.К., Гефнер И.С. Роль базовых систем ввода-вывода (UEFI BIOS) при оценке сценариев реализации угроз безопасности информации информационных систем ..	358
56. Язов Ю.К. Соловьев С.В. Моделирование значимых объектов критической информационной инфраструктуры в интересах исследования защищенности применяемых в них информационных технологий	363
57. Чиликов А.А. О решении одной задачи олимпиады NSUCrypto’2019 и разделениях функций многих переменных над конечными полями	370

ISBN 978-5-9906630-7-7



Издательство МГТУ им. Н.Э.Баумана
Россия, Москва, 105005, ул.2-я Бауманская, д.5, стр.1.
Тел. (499)263-6391, Факс: (499) 267-4844
Подписано в печать 29.04.2021 Заказ 039987
Формат 60х90.8. Гарнитура Times New Roman
Усл. печ. 29.04.2021 Тираж 100 экз.