Национальный исследовательский ядерный университет «МИФИ»

70 лет
Институту интеллектуальных кибернетических систем

Вторая Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность»

«КИБ-2024»

Сборник

научных трудов

22–23 октября 2024 г., Москва

Москва 2024

УДК 004.056 : 001(06)
ББК 32.973.202
В85

Вторая Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность «КИБ-2024». Сборник научных трудов. 22-23 октября 2024 г., Москва. М.: НИЯУ МИФИ, 2024. 292 с.

Настоящая книга содержит тезисы научных работ и докладов, предложенных специалистами на конференции «КИБ-2024».

Представленные материалы выполнены преподавателями, научными сотрудниками, молодыми учеными, аспирантами и студентами МИФИ и других вузов, специалистами академических научных и научно-производственных организаций Москвы и России, сотрудничающих с МИФИ. Работы отражают достижения и уровень исследований, тенденции и проблемы в развитии и обеспечении образования и научно-исследовательских работ по актуальным вопросам информационной безопасности, решению задач по защите информации, построения информационных и интеллектуальных систем управления в защищенном исполнении.

Книга предназначена читателям, интересующимся тематикой представленных научных направлений.

Статьи сборника издаются в авторской редакции.

Материалы получены 20.09.2024

ISBN 978-5-7262-3091-7

СОДЕРЖАНИЕ

БЕЗОПАСНОСТЬ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ

ЗАЩИЩЕННЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ТЕОРЕТИЧЕСКАЯ И ПРАКТИЧЕСКАЯ КРИПТОГРАФИЯ

ФИНАНСОВАЯ И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ВЫСШЕЙ ШКОЛЫ

Направление

Безопасность объектов критической информационной инфраструктуры. Технологический суверенитет

Руководители секции:

ДУРАКОВСКИЙ А.П. – к.т.н., доцент, директор аттестационно–испытательного центра НИЯУ МИФИ

МАРКОВ А.С. – д.т.н., заведующий кафедрой №43, президент НПО «Эшелон»

УДК 681.3.06 (075.32)

А.И. КОСТОГРЫЗОВ

Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва

ПОДХОД К ИНТЕРВАЛЬНОЙ ОЦЕНКЕ СИСТЕМНЫХ РИСКОВ ПРИ НЕПОЛНОТЕ ДАННЫХ О КРАТНОСТИ РЕЗЕРВИРОВАНИЯ В ПОДСИСТЕМАХ

Целью настоящей работы является изложение вероятностного подхода к оценке нижней и верхней количественных границ прогнозируемых рисков нарушения качества и/или безопасности компьютерных систем для случаев, когда есть лишь некоторые данные, догадки и/или уверенность, что в конкретных подсистемах какое–то двух-, трех- или более кратное резервирование имеет место быть. В качестве применяемых рекомендуются вероятностные модели из ГОСТ Р 59991.

Для обеспечения качества и информационной безопасности функционирующих компьютерных систем в их составных подсистемах активно применяются различные механизмы резервного копирования процессов обработки, хранения и восстановления информации. Так, для резервного копирования базы данных всегда осуществляется мониторинг успешного завершения процессов с возможностью восстановления. У каждого сервера или сетевого устройства есть паспорт восстановления и конфигурационный образ системы, а для резервного копирования виртуальных машин используются регулярные срезы данных и др. Т.е. для функционирующих систем имеет место определенная полнота данных о кратности резервирования в подсистемах. Это позволяет осуществлять достаточно адекватные оценки качества и безопасности эксплуатируемых систем по статистическим данным. Вместе с тем, на ранних этапах проектирования систем необходимой полноты таких данных еще нет, т.к. система лишь замышляется. Но в то же время количественное обоснование достижимого качества и безопасности в терминах рисков остро востребовано. Более того, востребованы сравнения показателей рисков для различных подсистем по идентичной вероятностной шкале, а также сравнения с другими системами, в том числе с СИСТЕМАМИ, охватывающими саму рассматриваемую систему (например, в сравнении с объемлющими рассматриваемую систему промышленными, транспортными, банковскими СИСТЕМАМИ, по которым необходимой полноты таких данных также может не быть, либо по каким-либо

соображениям владельцы СИСТЕМ препятствуют доступу к существующим полным данным). Т.е. на практике для системного анализа зачастую объективно имеет место неполнота данных о кратности резервирования в учитываемых подсистемах. Тем не менее, в этих и иных практически часто наблюдаемых случаях для любой компьютерной системы аналитическая востребованность вероятностного прогнозирования рисков нарушения качества и безопасности на определенный прогнозный период продолжает сохраняться. При этом понимается, что риски зависят от ожидаемых условий неопределенности, связанных с неоднородностью угроз и кратностью резервирования в каждой из учитываемых подсистем. Тем самым подтверждается острая актуальность настоящей работы.

Вместе с тем, в условиях реальной неполноты данных о кратности резервирования, как правило, есть некоторые данные, догадки и/или уверенность, что в конкретных подсистемах какое–то двух-, трех- или более кратное резервирование имеет место быть. В общем случае резервирование осуществляется для того, чтобы обеспечить надежное выполнение процессов обработки и хранения данных с необходимым восстановлением, несмотря на реализуемые разнородные угрозы (технические, информационные, от человеческого фактора, природные и т.д.), и в конечном итоге обеспечить требуемое качество и безопасность системы.

Для описанных случаев в работе предложен вероятностный подход к оценке нижней и верхней количественных границ прогнозируемых рисков. При этом может быть учтена неоднородность угроз для каждой из составных подсистем (и/или элементов) декомпозируемой системы, а также способы восстановления после нарушений качества и/или безопасности.

Предлагаемый подход к прогнозированию рисков основан на применении вероятностных моделей, рекомендуемых ГОСТ Р 59991–2022 «Системная инженерия. Системный анализ процесса управления рисками для системы» – варианты применения моделей см. в [1–8].

Рассмотрим практический пример системного анализа целостности такой моделируемой системы, как внешний портал крупной организации, обеспечивающий обслуживание информационных потоков с помощью подключаемых сервисов и используемых функциональных возможностей. В совокупность используемых средств системы могут входить, в частности, передатчик, линия связи, носитель информации, приемник, аппаратные и программные средства. В интересах конечных

пользователей применяются сервисы, обеспечивающие передачу информации от источника к получателю. Положим, для этой системы и ее составных подсистем требуется оценить риски нарушения целостности в условиях технических и информационных угроз. Учитываются 5 составных подсистем: подсистема 1 внешнего шлюза, подсистема 2 ведения личных кабинетов пользователей, подсистема 3 сервисов, подсистема 4 шифрования информации, подсистема 5 внутреннего шлюза. Нарушения в подсистемах на техническом уровне могут происходить из-за сбоев и отказов используемого оборудования, из-за зависаний программного обеспечения, из-за человеческого фактора. Информационные угрозы возникают из-за нарушения требований по защите информации. Руководствуясь имеющимися неполными данными, догадками и/или уверенностью в кратности резервирования для конкретных подсистем, с использованием моделей из ГОСТ Р 59991 проводятся:

– приближенная оценка рисков в предположении отсутствия резервирования (не привязываясь к исходным данным, на рис. 1 слева отражены лишь некоторые конечные результаты расчетов);

– оценка рисков сверху, используя дополнительные данные о как минимум двукратном обязательном резервировании для 2-й, 3-й и 5-й подсистем, и трехкратном обязательном резервировании для 2-й и 4-й подсистем (см. рис. 1 по центру для понимания логики в сравнениях);

– оценка рисков, используя дополнительные данные о вполне возможном трехкратном резервировании для 2-й, 3-й и 5-й подсистем, и четырехкратном возможном резервировании для 2-й и 4-й подсистем (см. рис. 1 справа для понимания логики предлагаемого подхода в сравнениях).

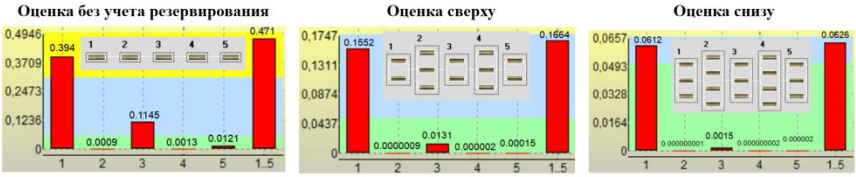


Рис. 1. Прогнозные оценки рисков с учетом моделируемых структур (для понимания логики подхода расчеты проводились на правдоподобных данных)

Сравнение рисков показывает, что без учета резервирования риски критичных нарушений за месячный период прогноза недопустимо велики (интегральный риск на рис. 1 слева – 0.471, риск для 1-й подсистемы – 0.394), а интервальные более точные оценки системных рисков

свидетельствуют – количественные значения рисков следует ожидать в диапазонах: интегральный риск от 0.0626 до 0.1664, риск для 1-й подсистемы – от 0.0612 до 0.1552. Последние оценки более реальные, они могут свидетельствовать о практической приемлемости системы в условиях ожидаемых технических и информационных угроз.

Применение предложенного подхода к учету обязательного и возможного резервирования (из-за неполноты реальных данных) позволяет проводить научные исследования на уровне анализа функции распределения вероятностей времени между критическими нарушениями в каждой подсистеме (элементе) и системе в целом, учитывая меры противодействия угрозам – по моделям из ГОСТ Р 59991. Основываясь на результатах прогнозирования рисков, оказывается возможным более аргументировано решать задачи выявления «узких мест» в системе, обоснования выполнимых требований к приемлемым условиям эксплуатации, выработки действенных мер упреждающего противодействия разнообразным угрозам, определения рациональных способов минимизации рисков, разработки рациональных планов технического обслуживания, совершенствования и развития системы.

Список литературы

1. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем. – М.: Изд. «Вооружение, политика, конверсия», 2008. – 404 с.

2. Абросимов Н.В., Костогрызов А.И., Махутов Н.А. и др. /Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Техногенная, технологическая и техносферная безопасность. М.: МГОФ «Знание», 2018. – 1016 с.

3. Probabilistic modeling in system engineering. InTechOpen, Edited by A. Kostogryzov, 2018, 279 p. – URL: http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering.

4. A. Kostogryzov and V. Korolev. Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, combinatorics and control / IntechOpen, 2020, p. 3–34. – URL: https://www.intechopen.com/books/probability-combinatorics-and-control

5. Нистратов А.А. Аналитическое прогнозирование интегрального риска нарушения приемлемого выполнения совокупности стандартных процессов в жизненном цикле систем высокой доступности. Часть 1. Математические модели и методы // Системы высокой доступности. 2021. Т. 17 № 3, с. 16–31. Часть 2. Программно-технологические решения. Примеры применения // Системы высокой доступности. 2022. Т. 18 № 2, с. 42–57.

6. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments. Time Series Analysis - New Insights. IntechOpen, 2023, p. 73–105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments.

7. Костогрызов А.И. Обоснование противодействия угрозам в системных процессах на основе вероятностного прогнозирования рисков. // Сборник материалов конференции «Кибернетика и информационная безопасность». МИФИ, 2023, с. 90–91

8. Костогрызов А.И., Нистратов А.А. Вероятностное прогнозирование рисков в стандартах системной инженерии// Электронный научный журнал «ИТ-Стандарт». 2023, № 1, с. 4–10.

УДК 004.056

А.С.МАРКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва
Научно-производственное объединение «Эшелон», Москва

О СЕРТИФИКАЦИИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Доклад посвящен оценке соответствия интеллектуальных средств защиты информации. Рассмотрены классификации, стандарты и системы сертификации систем искусственного интеллекта. Отмечена необходимость оценки соответствия интеллектуальных средств защиты информации.

Введение

Востребованность тематики оценки соответствия систем искусственного интеллекта (ИИ) по требованиям безопасности информации обусловлена следующим:

– отмечается интеграция технологий ИИ и кибербезопасности;
– растет уровень интеллектуализации кибератак;
– развивается класс кибератак на модели и приложения ИИ [1].

В [1–7] представлено множество таксономий ИИ-атак, основные можно свести к следующим:

– кибератаки на данные;
– кибератаки на алгоритмы;
– кибератака на наличие конфиденциальных данных;
– кибератаки нарушения среды и др.

Технологии ИИ начинают внедряться в практику организации защиты информации. На рис. 1 представлен вариант использования методов ИИ в области ИБ по версии ENISA.

Несмотря на то, что наша страна входит в Топ-20 по исследованию технологий ИИ, ряд наших специалистов пока скептически относятся к тематике ИИ, аргументируя это следующим:

– прогнозы не сбываются;
– имеется разрыв между реальными и академическими атаками;
– наблюдается большой разброс между датасетами;
– имеется смещенность между областями ИБ и методами ИИ;
– отечественный реестр интеллектуальных средств защиты почти пуст.

	DT	SVM	NB	K-means	HMM	GAN	ANN	CNN	RNN	Encoders	SNN
Обнаружение атак (IDS, IPS)	X	X	X	X	X	X	X	X	X		X
Обнаружение вредоносного ПО (AV)	X	X	X	X				X	X		
Поиск уязвимостей (VM)	X										
Фильтрация спама (antispam)			X								
Детектирование аномалий (SIEM, UEBA)					X					X	
Классификация вредоносного ПО (AV)						X	X				X
Детектирование фишинга (NGFW)							X				
Анализ трафика (NTA)								X	X		

Источник: Artificial intelligence and cybersecurity research, ENISA, 2023

Рис.1. Примеры использования методов ИИ при решении задач по ИБ

Возможность оценки соответствия ИИ рассмотрим в трех плоскостях:

– уровень учета базовых факторов информационной безопасности (ИБ), как-то: дефекты, уязвимости, угрозы, риски, атаки, инциденты;

– перспективы развития стандартов (ИБ, приватность данных, доверие, методы тестирования и испытаний);

– становление систем сертификаций (по доверию, по безопасности информации).

1. В качестве примеров можно привести следующие: наличие ИИ-угроз в БДУ ФСТЭК Росси и открытых базах уязвимостей систем ИИ (например, AVIDML), публикация дефектов в решениях, использующих ИИ (NIST NVD), поддержка матрицы MITRE ATLAS для описания атак на ИИ, нормативные документы (NIST AI RMF 1.0) по оценке уровней рисков в ИИ и пр. Следует указать на OWASP TOP 10 для приложений, использующих большие языковые модели, и каталоги угроз из OWASP AI Exchange.

2. Разработкой нормативных документов по линии ИИ заняты практически все зарубежные системы стандартизации, как-то:

– Европейский комитет по стандартизации (CEN) и Европейский комитет по электротехнической стандартизации (CENELEC);

– Европейский институт телекоммуникационных стандартов (ETSI);

– Международная организация по стандартизации (ISO);

– Международная электротехническая комиссия (IEC);

– Национальный институт стандартов и технологий США (NIST).

В ISO/IEC основные изыскания по линии ИИ проводит технический подкомитет 42 (ISO/IEC JTC 1/SC 42 Artificial intelligence). В России исследование проводит ТК-164 «Искусственный интеллект» [3] совместно с ТК-362 «Защита информации» и ТК-26 «Криптографическая защита информации».

3. Следует отметить, что в мире уже имеется опыт создания систем сертификации изделий ИИ, например: TUV (Германия), TUV (Австрия), CertifAI (конгломерат PwC, DEKRA и фонда инноваций города Гамбурга), SGS (Австрия).

Указанные системы сертификации проводят испытания изделий ИИ на соответствие следующим требованиям:

– по фактическому функционированию;
– по надежности обученной машины;
– по безопасности функционирования ПО (наличие уязвимостей);
– на соответствие требованиям сферы применения ПО (НДВ);
– по обеспечению защиты конфиденциальности данных;
– на предмет этических аспектов взаимодействия машины и человека.

Кроме систем сертификации в области ИИ, функционируют ряд систем сертификации по ИБ. Классическим примером является международная система «Общих критериев». Так, в базе профилей защиты и заданий по безопасности уже присутствуют средства защиты с интеллектуальными механизмами защиты, например, UEBA (machine learning) LogPoint SIEM (ОУД 3+).

Можно добавить, что в настоящее время весьма востребованными являются сертификации специалистов, например: ISACA (AI Fundamentals Certificate), ARTiBA (Artificial Intelligence Engineer), US AI Institute (Certified Artificial Intelligence Scientist, IBM (AI Engineering Professional Certificate).

Выводы

Вышесказанное позволяет сделать ряд выводов:

1. Понятийный аппарат ИБ систем ИИ сложился и развивается.

2. Имеется разрыв между теорией и практикой в отдельных областях ИБ.

3. Первенство в области стандартизации ИИ пока принадлежит ISO и NIST.

4. Имеются системы сертификации систем ИИ, в то же время имеется ряд ограничений по предоставлению гарантий.

5. Оценка соответствия систем ИИ может выйти за рамки ИБ, так как встает вопрос доверия, надежности и устойчивости ИИ.

6. Необходимость регулирования ИИ – объективная реальность, а область находится в чрезвычайно стремительном развитии.

Можно сделать ряд замечаний о создании систем сертификации в стране.

1. Надо понимать, что современная парадигма технологической независимости страны опирается на открытое ПО (opensource) [8]. Это значит, что вопросы безопасности открытых приложений ИИ и репозиториев ИИ будут определяющими.

2. В настоящее время основные фреймворки и представительные датасеты – иностранные со всеми вытекающими технологическими и информационными угрозами.

3. Принципиальные требования к системам ИИ – это организация производства. Это значит, что современные требования ФСТЭК России в указанной области актуальны как никогда [9].

Список литературы

1. Марков А.С. Актуальные вопросы оценки соответствия интеллектуальных средств защиты информации. // В сборнике: Безопасные информационные технологии. Материалы XII Международной научно-технической конференции, посвященной 25-летию кафедры ИУ8. Москва, 2024. С. 92–97.

2. Бирюков Д.Н., Ломако А.Г., Петренко С.А. Интеллектуальные системы предотвращения кибератак // Защита информации. Инсайд. 2019. № 5 (89). С. 60–70.

3. Гарбук С.В. Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности. 2021. № 3 (43). С. 68–83.

4. Горбачев А.А., Максимов Р.В. Проблема маскирования и применения технологий машинного обучения в киберпространстве // Вопросы кибербезопасности. 2023. № 5 (57). С. 37–49.

5. Запечников С.В. Модели и алгоритмы конфиденциального машинного обучения // Безопасность информационных технологий. 2020. Т. 27. № 1. С. 51–67.

6. Костогрызов А.И., Нистратов А.А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023. № 5 (57). С. 9–24.

7. Плугатарев А.В., Марухленко А.Л., Бугорский М.А., Булгаков А.С., Марченко М.А. Применение нейронных сетей в системах обеспечения информационной безопасности // Безопасность информационных технологий. 2021. Т. 28. № 3. С. 73–80.

8. Марков А.С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1 (53). С. 2–12.

9. Арустамян С.С., Варениса В.В., Марков А.С. Методические и реализационные аспекты внедрения процессов разработки безопасного программного обеспечения // Безопасность информационных технологий. 2023. Т. 30. № 2. С. 23–37.

УДК 004.056

А.И. ТЕРЕНТЬЕВ

Московский государственный технический университет гражданской авиации

ПЕРСПЕКТИВНЫЕ СВОЙСТВА ЧЛБ-ЦЕПЕЙ И ЧЛБ-КОНСТРУКЦИЙ, РАСШИРЯЮЩИЕ ВОЗМОЖНОСТИ ИХ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ

Рассматривается ряд характерных свойств ЧЛБ-цепей и ЧЛБ-конструкций, которые обусловлены принципами помехоустойчивого кодирования и не свойственны технологии блокчейн. Указанные особенности представляются перспективными и расширяют возможности практического применения ЧЛБ-цепей и ЧЛБ-конструкций в современных защищенных компьютерных системах и технологиях.

В настоящее время актуальной является задача преобразования различных массивов данных в вид, адекватный для использования современными информационными технологиями и компьютерными системами. В зависимости от прикладного назначения и специфики компьютерной системы такие данные могут представляться в виде линейно упорядоченного множества – цепи блоков цифровых данных или других более сложных конструкций.

Учитывая современные угрозы информации в цифровом пространстве, представляется целесообразным обеспечивать защиту цепи (иных конструкций) блоков цифровых данных от преднамеренной и не преднамеренной (случайной) модификации. В настоящее время для обеспечения такой защиты применяются различные методы и технологии, в том числе технология блокчейн (англ. Blockchain). Конкретные вопросы практического применения и стандартизации технологии блокчейн рассмотрены в [1], где приведены основные первоисточники и наиболее часто цитируемые определения технологии блокчейн. Для гармонизации общего понимания сути подобных технологий в [2] предложено использовать концептуальную схему (парадигму) технологии связных данных, согласно которой любые данные, локализованные во времени и пространстве, рассматриваются с позиции математики как некоторое множество M, элементами которого могут являться множества, а также конструктивные, гибридные и иные сложно структурированные объекты, включающие, в том числе, информационную и служебную составляющие. При этом любые данные могут быть тем или иным способом представлены в виде наборов чисел или одного числа. Если средством

обработки таких данных является электронное техническое устройство (электронная вычислительная машина), то соответствующие числа или число будут являться элементами кольца конечных десятичных дробей D. В целях обеспечения их связности и защиты от модификации необходимо применить к блокам, составляющим такие конструкции, специальные методы и процедуры [2, 3]. Предлагается использовать для этих целей процедуру построения устойчивой к модификации цепи блоков цифровых данных, основанную на методах кодирования элементов (блоков) цепи числовым линейным блоковым разделимым систематическим корректирующим кодом (ЧЛБ (n, k)-кодом) над кольцом конечных десятичных дробей D, что позволяет получить цепь блоков цифровых данных, устойчивую к модификации. Термин и понятие ЧЛБ-цепи введены в [4]. Согласно классификации, предложенной в [2], ЧЛБ-цепь является примером одномерной (n = 1) структуры. Также одномерную (n = 1) структуру имеет ЧЛБ-кольцо. Двумерной (n = 2) ЧЛБ-конструкцией являются таблица или матрица (в ортогональном базисе), а также труба или объекты спирально-винтового типа. Простейшим примером трехмерной (n = 3) ЧЛБ-конструкции является куб или параллелепипед (в ортогональном базисе). Результаты исследований, проведенных автором, показывают, что ЧЛБ-конструкции обладают более разнообразными и перспективными инструментами противодействия потенциальным деструктивным воздействиям (атакам) со стороны злоумышленника.

Список литературы

1. Будзко, Владимир И.; Милославская, Наталья Г. Вопросы практического применения технологии блокчейна. Безопасность информационных технологий, 2019, – Т. 26, – № 1. С. 36 – 45. doi:http://dx.doi.org/10.26583/bit.2019.1.04.

2. Терентьев, А. И. Концептуальная схема (парадигма) технологии связных данных // Безопасность информационных технологий, 2021. – Т. 28. – № 3. – С. 65–72. – doi:http://dx.doi.org/10.26583/bit.2021.3.05. – EDN ZQSWJX.

3. Терентьев, А. И. Виды порождающих процедур связного множества цифровых данных // Гражданская авиация на современном этапе развития науки, техники и общества: Сборник тезисов докладов Международной научно-технической конференции, посвященной 50-летию МГТУ ГА, Москва, 25–26 мая 2021 года. – Москва: ИД Академии Жуковского, 2021. – С. 383-386. – EDN ESWNUN.

4. Терентьев, А. И. Подходы к преобразованию больших массивов информации в цепь блоков цифровых данных, защищенную от модификации ЧЛБ (n, k)-кодом // Управление развитием крупномасштабных систем (MLSD'2022): Труды Пятнадцатой международной конференции, Москва, 26–28 сентября 2022 года / Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2022. – С. 1231-1236. – doi:http://dx.doi.org/10.25728/mlsd.2022.1231. – EDN RICMBP.)

УДК 33.338.45.1

В.А. МИНАЕВ, А.О. ФАДДЕЕВ

Московский университет МВД России им. В.Я. Кикотя

ГЕОДИНАМИЧЕСКИЕ ФАКТОРЫ И БЕЗОПАСНОСТЬ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА РОССИИ

Рассматриваются факторы формирования рисков функционирования топливно-энергетического комплекса (ТЭК) России. Особое внимание обращается на их геодинамические обусловленности. ТЭК представляется как территориально-распределенная система (ТРС), реализующая стратегические цели обеспечения безопасности Российской Федерации. Показаны стратегии управления рисками. Приведены результаты модельных экспериментов рисков нефтегазового комплекса (НГК). Делается вывод, что риски требуют учета особенностей их реализации применительно к ТЭК страны, являющемуся основным компонентом ее инновационного развития.

Топливно-энергетический комплекс (ТЭК) России, включающий отрасли, занимающиеся добычей, переработкой и транспортировкой углеводородов, производством, транспортировкой и распределением электроэнергии, является одной из самых важных, но и самых уязвимых, в смысле рисковых ситуаций, частей народного хозяйства страны.

Указанный комплекс относится к территориально-распределённым системам (ТРС), со всеми характерными для них свойствами, учитывая наличие среди его компонент природной, техногенной и антропогенной составляющих. Факторы формирования рисков для ТРС определяются при решении задач защиты территорий от проявления опасных природных и природно-техногенных процессов и безопасности жизни и здоровья проживающего на этих территориях населения.

Задачи и пути управления рисками

В России в рамках Государственной научно-технической программы «Безопасность населения и народнохозяйственных объектов с учетом риска возникновения природных и техногенных катастроф» предложены три основные стратегии решения задач минимизации риска, формирующегося при реализации указанных процессов и явлений [1]:

1) предотвращение причин возникновения природно-техногенных аварий и катастроф и обеспечение регламентного функционирования опасных в техногенном отношении объектов;

2) локализация аварий (катастроф) и предотвращение формирования опасной обстановки, когда ее причину по технологическим, экономическим, социальным или иным причинам устранить невозможно, и начинается цепная реакция событий, ведущих к аварии или катастрофе;

3) максимально возможное недопущение или ослабление воздействий опасных природно-техногенных факторов на людей и окружающую среду и ликвидация последствий аварии, катастрофы в кратчайшие сроки.

Эксперименты и новые результаты

Авторами проведены модельные эксперименты на примере анализа рисков применительно к конкретному типу ТРС, содержащей нефтегазовый комплекс (НГК), структурно входящий в ТЭК России.

Выявлены [2, 3]:

1) зависимость рисков от природных условий и ресурсов;

2) вероятностный характер показателей нефтегазовых месторождений;

3) характеристики капиталовложений при добыче;

4) ошибки при поиске нового месторождения.

Описаны опасные техногенные риски для территорий НГК, проживающего на них населении, обусловленные рисками и деградации окружающей природной среды, формирующиеся вследствие непродуманной производственной и иной хозяйственной деятельности.

Заключение и выводы

Значимыми геодинамическими угрозами, формирующими риски на объектах ТЭК России, являются землетрясения, криповые подвижки, карстово-деформационные процессы, оползни, провалы, проседания («медленные» катастрофы). Они влияют на технологическое состояние геологической среды, сооружения, сети коммуникаций, и на психические и медико-биологические показатели населения, а также персонала, размещённого на объектах ТЭК России.

Список литературы

1. Фаддеев А.О. Оценка геоэкологического риска на заселенных и промышленных территориях // Проблемы управления рисками в техносфере. 2008. № 4. – С. 36–47.

2. Ахметшин Т.Р. Модель и алгоритм минимизации геодинамических рисков при размещении объектов на территории нефтегазовых комплексов. // Моделирование, оптимизация и информационные технологии. 2021. № 9.

3. Минаев В.А., Фаддеев А.О. Оценки геоэкологических рисков. Моделирование безопасности туристско-рекреационных территорий. М.: Финансы и статистика, Изд. дом ИНФРА-М, 2009. – 370 с.

УДК 004.051

Д.И. ПРАВИКОВ, В.А. МУРАШКИН

РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва

ПОКАЗАТЕЛЬ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ НА ОБЪЕКТАХ НЕФТЕГАЗОВОЙ ОТРАСЛИ

В работе освещается вопрос применения для объектов нефтегазовой отрасли «Методики оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», которая была утверждена ФСТЭК России 2 мая 2024 г. Адаптация методики необходима для учета специфики отрасли, её критической важности для экономики и сложных технологических процессов.

Объекты нефтегазовой отрасли входят в состав критической информационной инфраструктуры России. Любое нарушение их функционирования может иметь серьёзные последствия, включая экономические потери и экологические катастрофы.

Нефтегазовая отрасль активно использует информационные технологии и системы автоматизированного управления (АСУ ТП) для мониторинга и управления производственными процессами. Эти системы требуют постоянной защиты от кибератак, поскольку атаки на АСУ ТП могут привести к авариям и сбоям в работе предприятий, что ставит под угрозу их безопасность и стабильность.

Нефтегазовые объекты, как правило, обладают следующими особенностями:

1. **Широкомасштабная и распределённая инфраструктура** (добыча, транспортировка, переработка).
2. **Высокая технологическая зависимость** от автоматизированных систем управления и технологических сетей.
3. **Высокий уровень интеграции с внешними системами** — например, взаимодействие с международными системами поставок и управления логистикой.

Это создаёт дополнительные вызовы для защиты информации, поскольку необходимо учитывать как внутренние, так и внешние угрозы.

Методика оценки ТЗИ и безопасности КИИ может быть адаптирована для нужд объектов нефтегазовой отрасли следующим образом:

1. **Оценка уровня защищенности автоматизированных систем управления технологическими процессами (АСУ ТП)**. Это критически

важные системы, которые требуют особого подхода к оценке безопасности.

2. **Анализ информационных систем, участвующих в управлении добычей и транспортировкой нефти и газа**. Защита этих систем от атак, направленных на нарушение цепочки поставок, жизненно необходима.

3. **Проведение аудита корпоративных сетей**, а также сетей, взаимодействующих с внешними подрядчиками и поставщиками.

4. **Оценка рисков, связанных с распределенной инфраструктурой**. Например, системы управления на удаленных объектах, таких как морские платформы или отдаленные месторождения, требуют особых мер защиты.

Для нефтегазовой отрасли можно предложить следующие специфические этапы оценки:

1. **Классификация объектов по степени значимости и критичности**. Нефтепроводы, морские платформы и заводы по переработке нефти могут иметь различную степень критичности, требующую различных уровней защиты.

2. **Определение уязвимостей АСУ ТП и SCADA-систем**, используемых в технологических процессах.

3. **Оценка защищенности коммуникационных сетей** (включая спутниковую связь и сети передачи данных), которые используются для связи между удаленными объектами.

Вывод

Методика оценки ТЗИ и безопасности КИИ, разработанная для объектов критической информационной инфраструктуры, вполне применима для нефтегазовой отрасли. Адаптация методики к особенностям нефтегазовых объектов позволит повысить уровень их защищенности и минимизировать риски, связанные с кибератаками и техногенными угрозами.

Список литературы

1. Методический документ «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» Утвержден ФСТЭК России 2 мая 2024 г.

2. ГОСТ Р 58276-2018 «"Информационная безопасность. Управление безопасностью автоматизированных систем управления технологическими процессами».

УДК 004.056

Н.В. КОРНЕЕВ[1, 2], К.А. ШАМКО[1]

[1]*РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва*

[2]*Финансовый университет при Правительстве Российской Федерации, Москва*

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ ОЦЕНКИ ПРОГНОЗИРОВАНИЯ ЭКСПЛОЙТОВ ДЛЯ РАСЧЕТА ИНТЕГРАЛЬНОЙ ОЦЕНКИ УЯЗВИМОСТЕЙ УЗЛОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

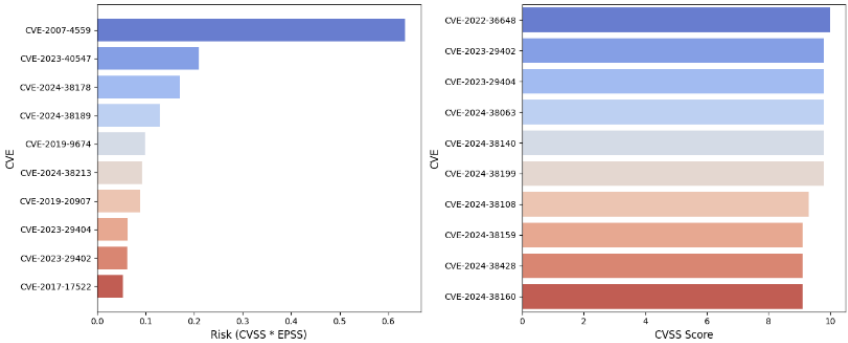
Рассмотрена ключевая задача в процессе управления уязвимостями на базе CVSS и EPSS. Показана возможность минимизировать вероятность эксплуатации критических уязвимостей и снизить риск для инфраструктуры используя ключевые показатели EPSS совместно с CVSS. Сопоставлены высокорейтинговые уязвимости по риску и проведена интегральная оценка CVSS и EPSS с рейтингом CVSS путем ранжирования уязвимостей с высоким риском.

Приоритезация уязвимостей – это ключевая задача в процессе управления уязвимостями. Традиционные методы оценки уязвимостей, такие как CVSS, предоставляют важную информацию о потенциальном воздействии уязвимостей, но не всегда учитывают реальную вероятность их эксплуатации злоумышленниками [1]. Компании могут тратить значительные усилия на исправление уязвимостей с высокой оценкой CVSS, в то время как реальная угроза может исходить от других. Тогда на первый план выходит необходимость динамической оценки риска, которая учитывает, как серьёзность уязвимости, так и вероятность её эксплуатации в реальном времени. Это задача EPSS – система, которая помогает приоритизировать уязвимости на основе анализа вероятности их эксплуатации. Использование инструментов EPSS, даёт возможность более точно и эффективно управлять уязвимостями в условиях ограниченных ресурсов, минимизируя вероятность эксплуатации критических уязвимостей и снижая риск для инфраструктуры [2].

EPSS имеет следующие ключевые показателей для оценки риска эксплуатации уязвимостей. EPSS Score – числовое значение, которое отражает вероятность того, что уязвимость будет эксплуатирована в ближайшие 30 дней. Оценка варьируется от 0 до 1, где 1 – максимальная вероятность эксплуатации. Percentile (далее – персентиль) – вероятность эксплуатации уязвимости относительно других уязвимостей.

В рамках исследования использовался список уязвимостей из Microsoft Patch Tuesday за август 2024 г., где были отобраны 10 уязвимостей с самой высокой вероятностью эксплуатации относительно других уязвимостей. После интерпретации полученных результатов и проведения дополнительного анализа получены следующие выводы: изменение рейтинга EPSS при проведении приоритезации должно быть ненулевое за годовой период для уязвимостей, выявленных годом ранее; уязвимости, выявленные годом ранее с персентилем около единицы и нулевым изменением должны быть устранены в первую очередь, не в рамках анализа по устранению актуальных уязвимостей.

Были сопоставлены высокорейтинговые уязвимости по риску (произведение рейтинга CVSS и EPSS) с рейтингом CVSS (см. рис.). Это дает возможность провести интегральную оценку уязвимостей путем ранжирования высокорисковых уязвимостей по CVSS. Из рис. видно, что уязвимости с высокими CVSS могут не всегда занимать лидирующие позиции в рейтинге по риску, что подтверждает необходимость использования EPSS в дополнение к CVSS.



Использование EPSS, даёт возможность точно и эффективно управлять уязвимостями в условиях ограниченных ресурсов, минимизируя вероятность эксплуатации критических уязвимостей и снижая риск для инфраструктуры.

Список литературы

1. Jacobs J. et al. Exploit prediction scoring system (epss). Digital Threats: Research and Practice. 2021, Т. 2, № 3. с. 1–17.

2. Jacobs J. et al. Enhancing Vulnerability prioritization: Data-driven exploit predictions with community-driven insights. 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2023. с. 194–206.

УДК 004.056

Д.И. ПРАВИКОВ, Г.Д. ПОТАПОВ

РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва

ОЦЕНКА КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ НЕФТЕГАЗОВОЙ ОТРАСЛИ

Оценка комплексной безопасности производственных объектов предполагает всестороннее рассмотрение различного рода воздействующих негативных факторов, сравнение их опасности, ранжирование. Высокий уровень автоматизации технологических процессов на производственных объектах нефтегазовой отрасли определяет значимость вопросов обеспечения информационной безопасности. Поддержание функционирования сложных технических систем зависит от информационной безопасности, которая имеет большое значение, однако объективная оценка уровня безопасности производственного объекта не может быть получена без учета других потенциально опасных факторов, для ранжирования которых могут быть применены различные методы.

Объекты нефтегазовой отрасли являются стратегически важными для национальной экономики и безопасности. Они представляют собой сложные системы, которые включают в себя множество компонентов, таких как трубопроводы, резервуары, насосные станции, системы управления и контроля. Эти компоненты связаны между собой сетью коммуникаций, которая обеспечивает их работу и взаимодействие. Информационная безопасность этих объектов является одним из ключевых факторов устойчивости их функционирования.

Основные проблемы информационной безопасности объектов нефтегазовой отрасли: угрозы кибербезопасности; недостаточная защита периметра; отсутствие единой системы управления безопасностью человеческий фактор; неэффективное использование средств защиты. [1].

Для решения этих проблем необходимо разработать и внедрить комплексную систему информационной безопасности, которая будет включать в себя следующие элементы: политика безопасности; система управления доступом; антивирусная защита; шифрование данных; резервное копирование данных; мониторинг событий безопасности.

Важно понимать, что обеспечение комплексной безопасности представляет собой непрерывный процесс, требующий постоянного внимания и усилий. Появление новых угроз и изменение степени

опасности существующих требует периодической оценки систем комплексной безопасности производственных объектов.

При оценке степени значимости факторов, воздействующих на уровень безопасности, можно применять модели, основанные на сравнении параметров: сравнение по абсолютным значениям; ранжирование; парное сравнение; метод анализа иерархий (МАИ); статистические методы; статистические методы; экспертные оценки; анализ чувствительности; сравнительный анализ; бенчмаркинг. [2].

Выбор метода сравнения зависит от конкретной задачи и доступных данных. Важно выбрать метод, который наиболее точно соответствует цели сравнения и обеспечивает надёжные результаты.

Комплексные модели оценки эффективности защиты технических систем позволяют получить более полное представление о состоянии безопасности объектов нефтегазовой отрасли и определить направления для дальнейшего улучшения их защиты. Это особенно важно для обеспечения устойчивости функционирования стратегически важных объектов национальной экономики.

Список литературы

1. Зенков А.В. Информационная безопасность и защита информации. Учебное пособие / А.В. Зенков. – М.: Издательство Юрайт. 2024 – 107 с.

2. Покатилов В.В. Теоретические основы информационно-аналитической работы (ИАР). Учебное пособие / В.В. Покатилов, В.Д. Ловчиков, М.О. Матвеев. – М.: Издательство: ООО Издательско-торговый Дом «Перспектива». – 170 с.

УДК 004.056

В.А. ВОЕВОДИН

Национальный исследовательский университет «МИЭТ»

АКТУАЛЬНЫЕ ВОПРОСЫ КОЛИЧЕСТВЕННОГО ОЦЕНИВАНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В докладе приводится обзор методических средств оценивания устойчивости функционирования критической информационной инфраструктуры (КИИ). Результаты обзора позволяют утверждать, что существующие методики нацелены на оценивание устойчивости КИИ для штатных условий. Предложен подход для оценивания устойчивости КИИ, основанный на оценивании экстремальных значений функции устойчивости на периоде воздействия угроз, что позволяет ослабить требования к стационарности и эргодичности случайного процесса.

Введение

Отношения в области обеспечения безопасности КИИ регулируются силой закона. Регулирование отношений нацелено на обеспечение устойчивого функционирования КИИ в различных условиях обстановки [1]. Для чего выделяется ресурс, применение которого основано на соответствующих управленческих решениях. Для обоснования таких решений требуется инструмент количественного оценивания устойчивости КИИ. В настоящее время сложилась нормативно-правовая база и накоплен опыт обеспечения устойчивости КИИ для штатных условий, которые базируются на императивных номах права по схеме: требования Регулятора, с одной стороны, и ответственность за их неисполнение, с другой. Такой подход не требует количественного оценивания устойчивости КИИ, но и не обеспечивает эффективного применения выделенного ресурса. Предлагается постановка и решение задачи количественной оценки устойчивости КИИ в условиях угроз.

Концептуальная модель оценивания устойчивости КИИ

Задача формулируется следующим образом.

Дано: исходные данные, характеризующие:

а) $C(u,t)_{\substack{t\in(0,T],\\ u\in U_{E_0}}} = \{S_0, P(u,t), \mathrm{H}_i(u,t), \Theta(u)\}$ – *управляемые параметры*,

$S_0=\{A_0, L_0\}$ – структуру графа обеспечения функциональности объекта КИИ,

A_0 – семейство узлов, L_0 – семейство ребер, $E_0=A_0\cup L_0$; $P(u,t)=\left\{P\left(u_{A_0}\right),P\left(u_{L_0}\right)\right\}$ – защищенность объекта КИИ от угрозы u, $P\left(u_{A_0}\right)$ – защищенность узлов; $P\left(u_{L_0}\right)$ – защищенность ребер; $\Pi\left(u_{E_0},t\right)\underset{\substack{t\in(0,T]\\E_0=A_0\cup L_0}}{=}\left\{\Pi\left(u_{A_0},t\right),\Pi\left(u_{L_0},t\right)\right\}$ – оценку требуемого времени восстановления функциональности семейства поврежденных элементов E_0, узлов A_0 и ребер L_0; $\Theta\left(u_E\right)\underset{E=A_0\cup L_0}{=}\left\{\Theta\left(u_{A_0}\right),\Theta\left(u_{L_0}\right)\right\}$ – оценка ресурсных потребностей для восстановления функционала объекта КИИ;

б) $\mathrm{H}\left(u_E\right)\underset{E=A_0\cup L_0}{=}\left\{\mathrm{H}\left(u_{A_0}\right),\mathrm{H}\left(u_{L_0}\right)\right\}$ – *неуправляемые параметры*, характеризующие случайное время до воздействия угрозы и число воздействий.

Требуется: построить оператор ***B***, позволяющий отобразить совокупность исходных данных $C(u),\mathrm{H}(u)$ в функцию устойчивости на интервале $t\in(0,T]$, для угроз безопасности информации $u\in U_E$

$$\mathrm{H}(u,t)\underset{\substack{t\in(0,T]\\u^*\in U_e}}{=}\boldsymbol{B}\left\{C(u),\mathrm{H}(u)\right\}.$$

В докладе будут детализированы постановка задачи, ограничения, методы решения, продемонстрирована работа программы для ЭВМ.

Заключение

1. Решение поставленной задачи позволяет разработать программу для ЭВМ [2], с помощью которой возможно построить частные функций устойчивости элементов, а на их основе функцию устойчивости объекта КИИ.

2. Минимальное значение функции устойчивости объекта КИИ на периоде воздействия угроз $t\in(0,T]$ предлагается использовать как оценку устойчивости объекта КИИ.

Список литературы

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Д.П. Зегжды. М.: Горячая линия-Телеком, 2021. 560 с.

2. Воеводин В.А., Крахотин Н.А. Свидетельство о государственной регистрации программы для ЭВМ № 2024614666 РФ. Программа расчета функции живучести графа двухполюсной структуры, подверженной угрозам информационной безопасности. Свидетельство о государственной регистрации базы данных № 2024614666 от. 28.02.2024. (RU). Бюл. № 3, 28.02.2024.

УДК 004.056.53

А.А. ЧУМАКОВ

Национальный исследовательский университет «МИЭТ», Москва

МОДЕЛЬ УСТРОЙСТВА ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ОРГАНИЗУЕМОГО С ИСПОЛЬЗОВАНИЕМ РАДИОМОДУЛЕЙ

Одно из направлений внедрения технологии RFID – центральные процессоры (ЦП) средств вычислительной техники (СВТ). Наличие на подложке ЦП радиомодуля ставит под угрозу несанкционированного доступа (НСД) информацию, обрабатываемую в ЦП СВТ. Для защиты от возможных угроз НСД к информации предложена одна из моделей устройства защиты СВТ от НСД, организуемого при помощи радиомодулей.

Одним из направлений внедрения технологии RFID являются центральные процессоры (далее – ЦП) средств вычислительной техники (далее – СВТ) [1]. Радиомодули RFID, интегрируемые в ЦП СВТ, могут использоваться для создания канала несанкционированного доступа (далее НСД) к ЦП и обрабатываемой на них информации. Поэтому разработка модели устройства защиты СВТ от НСД к информации, организуемого с использованием радиомодулей, является несомненно актуальной научной задачей. Целью работы предложить одну из моделей устройства защиты СВТ от НСД, организуемого с использованием радиомодулей.

На основе имеющихся сведений была высказана гипотеза, что для защиты СВТ от угроз, связанных с использованием радиомодулей, интегрированных в ЦП, можно осуществлять периодическое сканирование шины SMBus на предмет поиска на ней радиомодуля. При обнаружении радимомодуля, необходимо заблокировать его работу и стереть его содержимое внутренней памяти.

Для возможности анализа данных, передаваемых радиомодулем, необходимо реализовать возможность прослушивания шины взаимодействия радиомодуля с другими устройствами СВТ.

Таким образом, для того чтобы обезопасить СВТ от угроз, которые могут возникнуть при наличии в СВТ радиомодулей, была предложена модель устройства защиты, включающий в себя (рис. 1):

а) блок обнаружения радиомодулей на шине I2C/SMBus путем периодического её сканирования и сигнализации об успешном обнаружении для последующей блокировки.

б) блок блокирования радиомодулей путем его перепрограммирования с целью недопущения:

- взаимодействия с ним по радиоканалу;
- возможности использования его памяти (установка запрета на доступ);
- восстановления связи ЦП с радиомодулем (сброс устройства на шине).

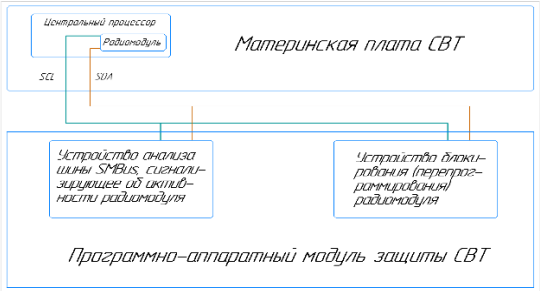


Рис. 1. Модель устройства защиты

Таким образом, была предложена модель устройства защиты СВТ от НСД к информации, реализуемого при помощи интегрированных в ЦП радиомодулей. В дальнейшем, на основании построенной модели планируется определить характеристики, свойства и программно-аппаратную платформу макета устройства защиты. Также планируется проведение экспериментальной проверки возможности защиты СВТ от НСД к информации с использованием радиомодулей.

Список литературы

1. Elyan J. Avec le RFID, Intel veut mieux recenser le matériel des datacenters // Le Monde Informatique [Электронный ресурс]. – URL: https://clck.ru/3Aa3jc (дата обращения: 10.09.2024).

УДК 004.056

В.Б. ГИСИН

Финансовый университет при Правительстве Российской Федерации, Москва

ДЕКОМПОЗИЦИЯ МОДЕЛЕЙ КИБЕРФИЗИЧЕСКИХ СИСТЕМ: ТЕОРЕТИКО-КАТЕГОРНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ

В работе предложен теоретико-категорный подход к моделированию безопасности киберфизических систем на уровне их компонент. В основе подхода идея леммы Йонеды: если модель системы и представление о ней порождают эквивалентные функторы, то представление о модели может быть использовано для структурной атаки.

В работе представлен формализованный подход к анализу потенциальных угроз действий злоумышленника на уровне архитектуры модели. Декомпозиция модели может использоваться как инструмент анализа угроз и выявления уязвимостей. Как отмечается в [1] (см. также, [2, 3]), единый взгляд на широкий спектр классов злоумышленников и обоснование свойств безопасности систем являются краеугольными камнями науки о безопасности. Теория категорий является инструментом, специально созданным для изучения свойств композиции. Поэтому там, где декомпозиция модели играет ключевую роль, применение языка методов теории категорий выглядит совершенно оправданно.

Следуя [4], модель системы мы представляем объектом некоторой категории **Mod**. На этом уровне модель описывается своими входными и выходными параметрами. Морфизму в **Mod** соответствует декомпозиция модели. Композиция морфизмов позволяет описать сборку модели из компонентов различных уровней. Изменение модели отражается на возможных вариантах ее поведения (функционирования). Этим задается функтор $\boldsymbol{F}$:**Mod** ---> **Func**. Объектами категории **Func** являются категории функционирования систем. Конкретная система представляется в виде пары (X,S), где X – модель, а S – поведение системы – объект из $\boldsymbol{F}(X)$. При моделировании угроз безопасности, предполагается, что нарушитель имеет доступ к базе знаний – набору объектов $\mathbf{K}_{\boldsymbol{F}(X)}$ категории $\boldsymbol{F}(X)$. Тестом на системе (X,S) называется функтор $\boldsymbol{T}$ на $\boldsymbol{F}(X)$ в категорию множество **Set**. Применение теста к любому объекту V дает информацию $\boldsymbol{T}(V)$. Нарушитель имеет доступ к $\boldsymbol{T}(V)$ при любом V из $\mathbf{K}_{\boldsymbol{F}(X)}$, в частности, к $\boldsymbol{T}(S)$. Согласно лемме Йонеды, если представимые функторы $\boldsymbol{F}(X)(S, –)$ и

$\boldsymbol{F}(X)(S', -)$ эквивалентны, то S и S' изоморфны. Если множество тестов достаточно велико (плотно том или ином смысле в $\mathbf{Set}^{\boldsymbol{F}(X)}$), вывод об изоморфизме S и S' можно сделать на основе совпадения $\boldsymbol{T}(S)$ и $\boldsymbol{T}(S')$ для всех тестов $\boldsymbol{T}$. Содержательно это означает, что представление о системе адекватно, если результаты тестирования согласуются с представлением о ней. Важность алгебраического оформления этого достаточно тривиального вывода в том, что всем его условиям и заключению может быть придан точный смысл.

В настоящей работе предлагается развитие идеи из [4]. Так, в [4] в качестве категории **Mod** берется категория диаграмм (которая по существу является категорией, так называемых, линз). Эта категория налагает ряд ограничений на модели. Во-первых, требуется, чтобы входные и выходные канал/порты были однородны и были связаны с одним и тем же типом данных. Это требование оказывается чрезмерно ограничительным даже для ключевого примера из [4] (управление БПЛА). Во-вторых, оказывается затруднительной декомпозиция моделей, состоящих из нескольких компонент.

Устранить указанные недостатки удается за счет учета типа данных, идущих по информационным каналам. В отличие от [4] в качестве категории **Mod** мы берем категорию, объектами которой являются боксы («черные ящики») с типизированными портами. А морфизмы определяются отображениями типизированных множеств. При использовании типизированных множеств композиция диаграмм обеспечивает согласование типов входных и выходных данных. Кроме того, в категории линз морфизмов между диаграммами «слишком много». Типизация данных позволяет существенно сократить множество морфизмов между моделями, что упрощает анализ Hom-функторов. При таком подходе декомпозицию многокомпонентных моделей можно описывать, используя аппарат окрашенных операд.

Список литературы

1. Datta A., Franklin J., Garg D., Jia L., Kaynar D. On adversary models and compositional security IEEE Security & Privacy. 2010, №. 3(9), с. 26–32. https://doi.org/10.1109/MSP.2010.203

2. Gancher J., Gibso, S., Singh P., Dharanikota S., Parno B. OWL: Compositional verification of security protocols via an information-flow type system. 2023, IEEE Symposium on Security and Privacy. IEEE, 2023, с. 1130–1147.

3. Рыженко А.А., Селезнёв В.М. Алгоритм оценки уровня цифровой автономии компонентов инфраструктуры цифрового пространства. Вопросы кибербезопасности. 2024, №. 4, с. 131–139.

4. Bakirtzis G., Genovese F., Fleming C. H. Yoneda hacking: The algebra of attacker actions. ACM Transactions on Cyber-Physical Systems. 2022, №. 3(6), с. 1–27.

УДК 004.056

М.Ю. ТОЛСТЫХ, А.О. ВАЩЕНКО

Московский государственный лингвистический университет

СОВЕРШЕНСТВОВАНИЕ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА НЕКОТОРЫХ ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Рассматривается необходимость обеспечения информационной безопасности учреждений, занимающихся авиатопливообеспечением, как субъектов критической информационной инфраструктуры. Аргументируется необходимость создания системы управления информационной безопасностью на основе стандартов серии ISO 27000 как базиса для планирования и проведения эффективных мероприятий по защите информации, а также в процессах соблюдения требований действующего законодательства в соответствующей области.

Коммерческие организации, чья деятельность связана с обеспечением критически важной инфраструктуры государства (КИИ) [1], сталкиваются с необходимостью защиты своих информационных ресурсов от актуальных угроз безопасности. В данном контексте достижение определенного уровня информационной безопасности (ИБ), соответствующего международным стандартам, является особенно важной задачей.

Одними из упомянутых объектов, реализующих обеспечение штатного функционирования КИИ, являются топливозаправочные комплексы (ТЗК) аэропортов, которые имеют высокую значимость для работы компаний в области гражданской авиации [2]. Они отвечают за хранение, поставку и заправку топлива и необходимы для поддержания бесперебойного процесса авиаперевозок. Любое нарушение в их работе может привести к серьезным последствиям: от задержек рейсов до критических аварий, которые могут поставить под угрозу жизни людей и нанести значительный экономический, экологический и др. ущерб. Аэропортовые ТЗК и компании по авиатопливообеспечению занимают важное место в авиационном сегменте России, обеспечивая безопасность и эффективность процессов заправки воздушных судов. Помимо общих норм по ИБ (например, соблюдение требований законодательства о персональных данных) к поставщикам топлива применяются специальные правила как для субъектов значимых объектов КИИ, данная отрасль также подчиняется требованиям Воздушного кодекса РФ.

В условиях стремительного роста информационных технологий, нестабильной политической обстановки в мире и, как следствие, ежедневного увеличения рисков и угроз компании, занимающиеся ресурсным обеспечением ТЗК, становятся мишенью не только для хакеров и организованных преступных группировок, но и для недружественных государств, стремящихся нанести ущерб России посредством кибератак. Таким образом, вопросы ИБ для предприятий ТЗК имеют стратегическое значение и выходят за рамки стандартного управления рисками, становясь одним их ключевых элементов национальной безопасности [3].

На наш взгляд, с точки зрения исполнения законодательства о КИИ, приведение системы управления ИБ организаций, функционирующих для потребностей указанной инфраструктуры государства, в соответствие с международными стандартами семейства ISO 27000 [4] является наиболее приемлемым способом реализации комплаенса, а также необходимым условием для поддержания конкурентоспособности и защиты от информационных атак, минимизации рисков киберугроз, обеспечения устойчивости и непрерывности бизнес-процессов. Стандарты ISO 27000 обеспечивают системный подход к управлению ИБ, включающий в себя политику безопасности, управление доступом, контроль над инцидентами, обработку компьютерных атак, а также другие ключевые аспекты.

Организационная защита информации предполагает создание системы мер, направленных на управление безопасностью данных и минимизацию рисков утечки или несанкционированного доступа. В условиях роста кибератак и необходимости соблюдения национальных требований по защите КИИ внедрение документов ISO 27000 позволит организациям не только улучшить собственную безопасность, но и легче взаимодействовать с международными партнерами, для которых выполнение таких стандартов является обязательным условием для сотрудничества.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // URL: https://base.garant.ru/71730198/ (дата обращения: 09.09.2024).

2. Неруш, Ю.М. Транспортная логистика: учебник для вузов / Ю.М. Неруш, С.В. Саркисов. – М.: Издательство Юрайт, 2024. – 351 с.

3. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 09.09.2024).

4. Стандарты. Серия ISO/IEC 27000 «Менеджмент информационной безопасности» [Электронный ресурс] // URL: https://www.iso.org/ru/standard/iso-iec-27000-family (дата обращения: 09.09.2024).

УДК 004.056

Н.А. НИЛОВ
Научный руководитель – к.т.н., доцент А.П. ДУРАКОВСКИЙ
Национальный исследовательский ядерный университет «МИФИ», Москва

НЕДОПУСТИМЫЕ СОБЫТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЛАТЕЖНОЙ СИСТЕМЫ СУБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Цель исследования – оценка эффективности применения мер для исключения недопустимых событий в платежной системе субъекта критической информационной инфраструктуры (КИИ). Основные задачи: построение перечня недопустимых событий информационной безопасности (ИБ) платежной системы кредитно-финансовой организации (КФО) как субъекта КИИ; расчет вероятности появления ущерба от наступления недопустимых событий ИБ; оценка эффективности применения перечня недопустимых событий для платежной системы субъекта КИИ.

В январе 2023 г. был подготовлен проект Указа Президента РФ «Об утверждении Положения о государственной системе защиты информации в Российской Федерации» [1], в котором также говорится об определении недопустимых событий (последствий) в органе или организации, наступление которых может привести к ущербу (рискам) для обладателя защищаемой информации. Предполагается разработать реестр недопустимых событий, который будет представлять собой классифицированный по отраслям деятельности организаций типовой перечень событий, наступление которых делает невозможным функционирование организации либо влечет к длительному нарушению основной деятельности. В финансовой сфере, недопустимым событием будет являться кража денежных средств со счетов кредитно-финансовой организации либо утечка защищаемой информации (персональные данные, данные, составляющие коммерческую и банковские тайны и т.д.). В первую очередь формировать перечень недопустимых событий необходимо для платежной системы КФО, так как успешно реализованная кибератака на платежную систему КФО может нанести финансовый ущерб свыше 500 млн рублей [2].

Концепция применения недопустимых событий подразумевает отказ от построения модели угроз безопасности, основанной на составлении перечня актуальных угроз безопасности.

В настоящее время ключевые регуляторы в области обеспечения информационной безопасности, такие как ФСТЭК России, Банк России, Минцифры России реализуют концепцию, которая сводится к тому, что для обеспечения информационной безопасности организации необходимо определить: актуальный угрозы безопасности информации; риски (негативные последствия) информационной безопасности; недопустимые события информационной безопасности. Однако, у каждого регулятора разная терминология по информационной безопасности и каждый из регуляторов по-разному подходит к построению системы обеспечения информационной безопасности (СОИБ), однако смысл их сводится к необходимости определить события, наступление (реализация) которых нанесет значительный ущерб, как материальный, так и сопутствующий, а также реализовать комплекс мероприятий по недопущению возникновения указанных событий [3]. Разработан пошаговый план, состоящий из шести этапов для формирования перечня недопустимых событий, сформирован перечень недопустимых событий КФО как субъекта КИИ. Проведен расчет вероятности появления ущерба от наступления недопустимых событий ИБ с использованием [4]. Вероятность наступления недопустимого события ИБ классифицирована на 6 уровней, от «несущественного» до «критического», проведены расчеты вероятностей: наступления недопустимого события; ущерба от наступления недопустимого события. Установлено, что при наступлении определенных недопустимых событий имеет место наступление сопутствующих недопустимых событий. С учетом данных особенной скорректированы показатели ожидаемых потерь. Проведена оценка эффективности применения перечня недопустимых событий для платежной системы субъекта КИИ.

Список литературы

1. Проект Указа Президента Российской Федерации "Об утверждении Положения о государственной системе защиты информации в Российской Федерации" (подготовлен ФСТЭК России 23.01.2023). https://base.garant.ru/56946774/ (дата обращения: 01.09.2024)

2. Хакеры впервые за три года украли деньги банка с его корсчета в ЦБ. URL: https://www.rbc.ru/finances/15/12/2021/61b89ab59a7947ba31ae3163?from=copyhttps://www.rbc.ru/finances/15/12/2021/61b89ab59a7947ba31ae3163 (дата обращения: 11.07.2024).

3. Савин М.В. Методика выявления и оценки недопустимых событий на основе модели зрелости управления информационной безопасностью / М.В. Савин, М.А. Кондратенко // Защита информации. Инсайд. – 2023. – № 1(109). – С. 24–31. – EDN BAOTEJ. URL: https://www.elibrary.ru/item.asp?id=50246119 (дата обращения: 24.07.2024).

4. Чипига А.Ф. Организационное обеспечение информационной безопасности / А.Ф. Чипига, М.А. Лапина. – Ставрополь: Северо-Кавказский государственный технический университет, 2009. – 439 с. – EDN WAUWHD. URL: https://www.elibrary.ru/item.asp?id=26175685 (дата обращения: 12.08.2024).

УДК 004.056

П.А. КОЗЫРЕВ
Российский экономический университет им. Г.В. Плеханова, Москва

МЕТОДЫ И АЛГОРИТМЫ МИКРОСЕРВИСНОЙ РЕАЛИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОИЗВОДСТВЕННЫХ ЦЕПОЧЕК СЕТЕВОГО ПРЕДПРИЯТИЯ

Целью работы является разработка методов и алгоритмов для обеспечения информационной безопасности производственных цепочек сетевого предприятия с использованием микросервисной архитектуры. В рамках исследования предложены решения для минимизации рисков, связанных с угрозами информационной безопасности, в том числе на основе модели нулевого доверия. Разработаны алгоритмы микросервисной защиты компонентов производственных цепочек, которые снижают риски и повышают устойчивость к киберугрозам. Описаны принципы аутентификации и авторизации, методы микросегментации, формирование виртуального периметра безопасности, внедрение политик минимальных привилегий, а также мониторинг и сбор телеметрии с объектов инфраструктуры сетевого предприятия. Уделено внимание вопросам автоматизации управления безопасностью и адаптации механизмов защиты к различным сценариям работы производственных цепочек в сетевом предприятии.

Введение

В рамках исследования предложены решения для минимизации рисков информационной безопасности производственных цепочек сетевого предприятия с использованием микросервисной архитектуры. Микросервисная архитектура, ставшая популярной в современных цифровых платформах, обеспечивает гибкость и масштабируемость, создает новые подходы к вопросам в области информационной безопасности. Одной из ключевых проблем является защита данных и ресурсов от несанкционированного доступа и кибератак, которые могут нарушить работу производственных процессов и нанести значительный ущерб сетевым предприятиям. Для решения этих проблем применяются инновационные подходы, включающие микросервисные методы защиты с применение модели нулевого доверия.

Решение задачи микросервисной реализации информационной безопасности производственных цепочек сетевого предприятия

Разработка методов и алгоритмов для обеспечения информационной безопасности производственных цепочек сетевого предприятия на основе микросервисной архитектуры представляет собой актуальную задачу [1].

Особое внимание уделяется минимизации рисков, связанных с несанкционированным доступом и кибератаками, применяя подходы микросервисной защиты и модель нулевого доверия [2].

Традиционную архитектуру информационной безопасности, применяемую в различных организациях, называют моделью с периметром безопасности в честь подхода «Стена замка», используемого в физической безопасности. Этот подход защищает чувствительные объекты, выстраивая линии защиты, через которые злоумышленник должен проникнуть, прежде чем получит доступ к необходимой ему информации [3]. К сожалению, этот подход в контексте цифровых, а тем более, сетевых предприятий больше не является достаточным.

Сетевые предприятия не имеют периметра безопасности. Отсутствие периметра безопасности предполагает, что каждый отдельный узел в сети, будет иметь свой личный контур безопасности. При выборе архитектуры безопасности в сетевых предприятиях, предлагается использовать модель нулевого доверия [4]. Вместе с тем, в этой концепции предлагается ввести понятие виртуального конкура безопасности, который будет формироваться для каждой производственной цепочки отдельно, а контролироваться будет разработанными микросервисами обеспечения информационной безопасности. Каждый микросервис будет реализовывать отдельную функцию, заложенную в концепции нулевого доверия: аутентификацию и авторизацию, при взаимодействии компонентов сетевого предприятия, мониторинг событий сети, распределение правд доступа и контроль доступа в сети предприятия и в процессе работы производственной цепочки.

Заключение

Проведенное исследование позволило разработать эффективные методы и алгоритмы для обеспечения информационной безопасности производственных цепочек сетевого предприятия на основе микросервисной архитектуры. Разработанные алгоритмы микросервисной защиты позволяют снизить риски и повысить устойчивость к киберугрозам.

Список литературы

1. Иванов П.А., Капгер И.В., Шабуров А.С. Модель реализации управления доступом к информационным активам в концепции нулевого доверия // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. 2023. №45.

2. Аррыкова Г.К., Гуванджов А., Гарабегова Л., Аширова Х. Обеспечение безопасности удаленных сотрудников и устройств // Всемирный ученый. 2024. №27.

3. Соболев Сергей Павлович Кибериммунный подход к разработке. Иллюстрация применения на базе микросервисной архитектуры.

4. NIST SP 800-207. "Zero Trust Architecture". National Institute of Standards and Technology, 2020.

УДК 004.056

Э.П. РЫБАЛКО[1]

Научный руководитель – доцент Г.П. ГАВДАН[2]

[1]*АО «Межотраслевой центр мониторинга», Москва*

[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

УСТОЙЧИВОСТЬ ФУНКЦИОНИРОВАНИЯ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

В настоящее время в Российской Федерации уделяется достаточно большое внимание и качественной работе государственных информационных систем (ГИС) и организации их устойчивого функционирования, которая к тому же не утратила свою актуальность. В свою очередь, оценка эффективности применяемых мер по обеспечению безопасности ГИС требует проведения оценки (их) устойчивого функционирования, которая определяется устойчивостью критических процессов этих ГИС. Объектом исследования являются ГИС. Предмет исследования есть устойчивость функционирования данных ГИС в условиях угроз информационной безопасности. Проведённый анализ научных публикаций по теме исследования показал, что в данном направлении в настоящее время имеется мало публикаций. По результатам работы установлено, что в данной области существуют нерешенные проблемы.

Введение

Открытость государственных информационных систем (ГИС) имеет большое значение для общества и правительства и обеспечивает прозрачность деятельности государственных органов [1]. Это означает, что граждане могут легко получать доступ к информации о действиях и решениях правительства, что обеспечивает им получить представление и сформулировать мнение о состоянии российского общества [1]. Так, в соответствии с базовым Федеральным Законом от 27 июля 2006 г. № 149-ФЗ в области информатизации, информационных технологий и защите информации. Данные, содержащиеся в ГИС, а также иные имеющиеся в распоряжении (государственных органов) сведения и документы являются национальными информационными ресурсами [2].

Устойчивость функционирования ГИС

Объективно существующая вероятность нарушения устойчивого функционирования ГИС, обусловленная возможностью возникновения нежелательных антропогенных, техногенных или стихийных воздействий на их информационные элементы, заставляет рассматривать устойчивость ГИС в условиях влияния на них угроз информационной безопасности [2].

Для оценки эффективности применяемых мер по обеспечению безопасности ГИС необходимо проведение оценки устойчивости их функционирования. В настоящее время общепринятый подход к проведению такой оценки отсутствует и его определение остаётся актуальной задачей [2]. Проблема устойчивости критической информационной инфраструктуры представлена [3] в работе авторской группы. В качестве угроз нарушителя – компьютерных атак могут рассматриваются целенаправленные программно-аппаратные воздействия, приводящие к нарушению (блокированию, искажению) информационно-вычислительных процессов функционирования ГИС [4].

Заключение

Сформулируем следующее определение устойчивости функционирования ГИС – это способность ГИС выполнять свои основные функции:

– в неблагоприятных условиях (т.е. при попытках реализации УИБ);

– в условиях непосредственной реализации на ГИС отдельных из УИБ;

– при отказе части компонентов объекта (т.е. в случае, когда отдельные угрозы ИБ уже реализуются);

– восстанавливать штатное функционирование в допустимые сроки.

Способность ГИС выполнять свои основные функции в любых условиях можно рассматривать как защищенность ГИС, в условиях реализации в отношении её угроз ИБ – живучесть ГИС в случае целенаправленных угроз либо стойкость ГИС (в случае если эти угрозы случайные – обусловлены программными ошибками, техническими сбоями или ошибками персонала).

Список литературы

1. Шматова У. В. Вопросы обеспечения открытости государственных информационных систем в России / У.В. Шматова // Актуальные проблемы и перспективы развития потребительского рынка: Материалы XII Международной научно-практической конференции студентов и учащихся, Пермь, 04–12 декабря 2023 года. Том 1. – Пермь: Пермский институт (филиал) ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», 2023. – С. 396–400. – EDN BOLPBC (дата обращения: 01.09.2024).

2.Пенерджи Рустем В., Гавдан Григорий П. Информационная безопасность государственных информационных систем. Безопасность информационных технологий, [S.l.], т. 27, № 3, с. 26–42, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.3.03. – EDN PEHWST.

3.Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И. Критическая информационная инфраструктура: оценка устойчивости функционирования. Радиопромышленность. 2018, № 4, с. 59–67. URL: https://elibrary.ru/item.asp?id=36511234 – EDN YPERPV (дата обращения: 01.09.2024).

4.Антонов С.Г., Анциферов И.И., Климов С.М. Методика инструментально-расчетной оценки устойчивости объектов критической информационной инфраструктуры при информационно-технических воздействиях. Надежность. 2020, 20(4):35–41. DOI: https://doi.org/10.21683/1729-2646-2020-20-4-35-41 (дата обращения: 10.09.2024).

УДК 004.056

Г.П. ГАВДАН, З.С. КУТЬИН
Национальный исследовательский ядерный университет «МИФИ», Москва

СПОСОБЫ И МЕТОДЫ РЕШЕНИЯ ПОДМЕНЫ ДОВЕРЕННОГО НОСИТЕЛЯ ИНФОРМАЦИИ В СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. Рассматривается обеспечение безопасности информационных систем, как первостепенная задача деятельности организации. В системах организации всегда присутствует множество уязвимостей, которые могут привести к реализации различного рода угроз. Актуальной проблемой является подмена доверенного носителя информации. Предметом исследования являются средства защиты информации, обеспечивающие безопасность информационных систем организации. Проведенный анализ различных источников по теме показал, что данная проблема актуальна. По результатам работы выделены основные подходы к решению выделенной проблемы.

Введение

В настоящее время объем информации, создаваемой и обрабатываемой в различных сферах жизни, стремительно увеличивается. Организации сталкиваются с огромных количеством данных, которые являются ключевым активом и становятся целями кибератак. В отчете, предоставленном Positive Technologies за IV квартал 2023 г., показана доля использования вредоносного программного обеспечения в атаках на организации равной 68%, а процент эксплуатации уязвимостей – 34% [1].

Проблема подмены доверенных носителей информации

Для хранения и обработки данных, необходимых для осуществления деятельности организации, существуют машинные носители информации (далее – МНИ). Специализированное программное обеспечение поможет не только повысить эффективность работы компании, но и улучшить общий уровень информационной безопасности за счет снижения рисков, связанных с человеческим фактором.

Модули защиты МНИ реализованы во многих средствах защиты. Одним из таких является программа Secret Net Studio (далее – SNS) от компании «Код безопасности» – российского лидера в области средств защиты информации [2]. SNS содержит модуль «Контроль устройств». Программа сохраняет информацию о подключенных устройствах, включая их идентификатор вендора (vid), идентификатор продукта (pid) и серийный номер устройства.

Злоумышленник может изменить эти данные, выдав свое устройство за одобренное программой. Кроме того, сама программа хранит данные о подключаемых устройствах в открытом виде. С помощью различных утилит, позволяющих изменять параметры устройств, злоумышленник перепрошивает нелегитимную флешку. К таким утилитам можно отнести «SMI MPT», позволяющая изменить PID, VID, Vendor Str, Product Str, Serial Mask на значения, соответствующие доверенному устройству [3]. Вследствие эксплуатации уязвимости у нарушителя открывается обширный перечень атак, среди которых можно выделить установку вирусного ПО с подменного носителя, доступ через виртуальные рабочие места сотрудников к серверу и др. Также стоит отметить, что злоумышленник должен иметь или когда-нибудь имел хотя бы кратковременный физический доступ к информационной системе.

Заключение

Необходимо применить ряд действий для предотвращения эксплуатации данной уязвимости. Для этого можно выделить ряд способов и методов:

– Использование всей доступной информации о носителе, для его идентификации, в том числе: Controller vendor, controller port-number, Flash ID code;

– Хранение в базе данных хэшированной информации о МНИ;

– Использование антивирусного ПО, позволяющего предотвратить последствия внедрения нелегитимного МНИ;

– Внедрение администраторами безопасности доменных политик, запрещающих запуск исполняемых файлов и добавление служб.

Для применения хэширования возможно использование алгоритма описанного в ГОСТ 34.11-2018 «Стрибог» [4]. Хэш-функция, осуществляющая хэширование, обладает свойством невозможности определения исходных данных по выходным за полиноминальное время.

Список литературы

1. Актуальные киберугрозы: I квартал 2024 // Positive technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1 (дата обращения: 19.09.2024).

2. Secret Net Studio // Код Безопасности. URL: https://www.securitycode.ru/products/secret-net-studio (дата обращения: 18.09.2024).

3. SMI MPToll SM32X \ SM34X [SMI Mass Production Tool] // USBDev. URL: https://www.usbdev.ru/files/smi/smimptool (дата обращения: 18.09.2024).

4. ГОСТ 34.11-2018 – Межгосударственный стандарт «Информационная технология. Криптографическая защита информации. Функция хэширования» – Введ. 01.06.2019. – М.: Стандартинформ, 2018 – 18 с

УДК 004.056

А.А. МАНЮГИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ОЦЕНКА СООТВЕТСТВИЯ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ СФЕРЫ ЭНЕРГЕТИКИ ПО ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Анализируются требования к оценке соответствия значимого объекта критической информационной инфраструктуры (КИИ) сферы энергетики по требованиям информационной безопасности информации. Одним из приоритетов являются исследования, направленные на функциональные требования безопасности и уровни доверия, установленными приказами ФСТЭК России. Предметом исследования является требования к защите информации объекта КИИ.

Введение

Одним из главных требований информационной безопасности объекта критической информационной инфраструктуры сферы энергетики по требованиям безопасности информации является оценка соответствия ЗО (значимый объект) КИИ требованиям информационной безопасности, что в свою очередь напрямую влияет на защищенность объекта информатизации. приоритетным направлением [1].

Цель и задачи

В связи вступлением в силу федерального закона от 26.07.2018 № 187-ФЗ «О безопасности информационной инфраструктуры Российской Федерации» появляются требования, которые необходимо соблюдать для обеспечения безопасности объекта КИИ. С принятием ФСТЭК России приказов №239 и №17 в части формирования требований по информационной безопасности к объектам КИИ, потребовалось реализовать требования по безопасности комплексной системы защиты информации (КСЗИ) на этапе проектирования и дальнейшего проведения оценки соответствия применяемых средств защиты информации. Для оценки соответствия, нужно написать программу и методику приемочных испытаний, по которой будет даваться оценка соответствия ЗО КИИ. Для средств защиты информации применяется ГОСТ 19.301-79, согласно которому, программа и методика испытаний оформляется в соответствие ГОСТ 19.105-78. Рассмотрим средства защиты информации,

которые предполагается использовать на ЗО КИИ.

Средства защиты информации, которые используются на объектах ЗО КИИ имеют определенные класс защиты. Перед владельцем ЗО КИИ стоит задача по использованию только сертифицированных средств защиты информации и только определенного класса, разрешенного к использованию на данном объекте [2].

Оценка соответствия может производиться в форме сертификации или испытаний. В случае, если на объекте уже внедрен КСЗИ, необходимо провести оценку соответствия самостоятельно на этапах внедрения организационных и технических мер по обеспечению безопасности информации.

Необходимость защиты информации ЗО КИИ обусловлена большими рисками утечки информации третьим лицам. По статистике, наибольшую опасность представляют собой внутренние нарушители. То есть, использование на рабочем месте недоверенных программных продуктов ведет к серьезным последствиям, которые в будущем могут привести к угрозе жизни людей и вред окружающей среды [3].

Заключение

Необходимо проводить оценку соответствия ЗО КИИ на этапе проектирования КСЗИ. При невозможности проведения этой своевременной процедуры, необходимо использовать только доверенное и сертифицированное программное и программно-аппаратное обеспечение соответствующего класса защиты информации. Методы проведения программы и методики испытаний могут быть полезны при подготовке частных заданий для проведения оценки отдельных систем ЗО КИИ

Список литературы

1. Приказ Минэнерго России от 26.12.2023 N 1215 «Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике» (Зарегистрировано в Минюсте России 16.05.2024 N 78165) URL: https://www.consultant.ru/law/hotdocs/84739.html?ysclid=m1b3zwb63q600659135 (дата обращения: 19.09.2024).

2. Голдобина А.С., Исаева Ю.А., Селифанов В.В. Основные аспекты соответствия DLP-систем, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, 2019.

3. Исаева Ю.А., Селифанов В.В. Оценка соответствия средств защиты информации в критических информационных инфраструктурах Российской Федерации, 2019.

УДК 004.056

В.В. КОЗЛОВ
Научный руководитель – к.т.н., доцент А.П. ДУРАКОВСКИЙ
Национальный исследовательский ядерный университет «МИФИ», Москва

АДМИНИСТРИРОВАНИЕ ПОЛЬЗОВАТЕЛЕЙ С ПОМОЩЬЮ МЕТОДА УНИФИЦИРОВАННОГО УПРАВЛЕНИЯ КОНЕЧНЫМИ УСТРОЙСТВАМИ

Цель исследования – разработка предложений по внедрению метода унифицированного управления конечными устройствами. Критерии для выбора платформы унифицированного управления конечными устройствами: поддержка операционной системы; поддержка программ использования собственных устройств; интеграция с другими ИТ-продуктами, партнерство поставщика с другими платформами, используемыми для поддержки ИТ или конечных пользователей в целом; политики безопасности устройства; сертификаты соответствия нормативным требованиям, условный доступ, поддержка удаленной среды.

В настоящее время мало компаний уделяют должное внимание защищенности корпоративных конечных устройств и информационных систем (ИС). Из-за пандемии большей части сотрудников был разрешен удаленный доступ, в связи с чем пользователи подключались к корпоративным конечным устройствам. В результате злоумышленники получили дополнительные способы к краже конфиденциальной информации и внедрению вредоносного ПО на корпоративные конечные устройства [1]. Чтобы избежать такие проблемы, предлагается подключать систему администрирования пользователей с помощью метода унифицированного управления конечными устройствами (УУКУ), которая поможет в отслеживании действий внутренних пользователей и обнаружит атаки злоумышленников. Благодаря этому можно будет следить за работой пользователей на конечных устройствах как внутри компании, так и за удаленным подключением сотрудников. Тем самым можно будет соблюдать все правила политики информационной безопасности, что поможет в предотвращении случаев применения злоумышленником неправомерных действий. Необходимо контролировать весть трафик корпоративных данных, которые передаются с помощью конечных устройств, следить за целостностью конечных устройств, ввести журнал, в котором будут записаны все действия сотрудников на конечных

устройствах, а также иметь полный контроль над управлением учетными записями пользователей и иметь возможность их блокировки для ограничения доступа к конечным устройствам [2]. Метод УУКУ снижает риски внутреннего и внешнего воздействия на внутреннюю систему компании. Тем самым обеспечивая стабильную работу для всех конечных устройств, подключенных к системе компании. Метод УУКУ предусматривает следующие преимущества для работы компаний:

- Комплексная интеграция управления конечными точками. Унифицированное управление конечными точками работает на нескольких платформах, настраивая, контролируя и отслеживая любое устройство с единой консоли управления
- Повышение производительности на конечных устройствах, так как происходит согласованный доступ к приложениям и контенту на конечных устройствах
- Защита корпоративных данных и приложений в любой сети. УУКУ защищает конфиденциальные данные компании и приложения с доступом пользователей, автоматическим применением правил, рекомендациями по соблюдению требований и защитой от потери данных, а также автоматически и немедленно устраняет угрозы кибербезопасности. Это также позволяет администраторам идентифицировать взлом устройства и блокировать его
- Модернизация управления настольными компьютерами. УУКУ преобразует операционные системы настольных компьютеров с помощью усовершенствованных технологий для упрощения развертывания, безопасно обеспечивая полное управление облачными политиками с оптимизированной доставкой приложений и автоматическим исправлением. Это также позволяет администраторам отслеживать, проверять контент и приложения
- Снижение затрат. Благодаря комплексной автоматизации процессов и задач унифицированное управление конечными точками помогает снизить накладные расходы на ИТ и расходы на оборудование

Список литературы

1. Как компании защищают конечные точки и почему это не спасает их от целевых атак https://safe.cnews.ru/articles/2024-03-11_kak_kompanii_zashchishchayut_konechnye_tochki?erid=LjN8KEBmH (дата обращения: 01.09.2024)

2. Котенко И.В., Федорченко Е.В., Новикова Е.С., Саенко И.Б., Данилов А.С. Методология сбора данных для анализа безопасности промышленных киберфизических систем. Вопросы кибербезопасности.2023, № 5 (57), с. 69–79, DOI:10.21681/2311-3456-2023-5-69-79

УДК 004.056

А.Н. ВАВИЧКИН, Д.А. ДЯТЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В СФЕРЕ НАУКА

Анализируется опыт категорирования объектов критической информационной инфраструктуры в высшем учебном заведении, а именно особенности категорирования в сфере наука. Рассмотрена подготовительная работа по выявлению объектов, подлежащих категорированию, и этапы проведения категорирования. Предложен порядок действий по подготовке к категорированию, формированию перечня объектов, подлежащих категорированию, и процессу категорирования, а также документальное сопровождение всего процесса для объектов, функционирующих в сфере науки.

Введение

В соответствии с федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» к объектам критической информационной инфраструктуры (КИИ) относятся информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети субъектов КИИ, то есть организаций, функционирующих в нескольких сферах, в частности, в сфере наука [1]. Из этих объектов выделяют те, которые подлежат категорированию.

Категорирование является первым этапом в создании системы безопасности значимых объектов КИИ [2]. Выявление объектов КИИ, которые подлежат категорированию, а также дальнейшее проведение категорирования в каждой сфере деятельности имеют свои особенности. В исследовании представлена организация данного процесса для научной сферы деятельности, а также обозначены основные этапы работ.

Основные этапы категорирования

Для проведения категорирования в организации создается соответствующая комиссия. Для научных учреждений важно, чтобы в нее входили руководители всех подразделений, ведущих научные работы. Это во многом упростит задачу получения сведений от научных подразделений об объектах, которые могут относиться к КИИ.

Для получения информации об имеющихся объектах кроме сведений,

которые можно получить из управлений бухгалтерского учета, научных исследований, инновационного развития и других, целесообразно провести инвентаризацию имеющихся информационных объектов [3].

Для определения объектов КИИ и необходимости их категорирования используется ряд документов, которые утверждаются руководителями подразделений. Собирается как можно больше информации о каждом из объектов (его архитектура, состав программно-аппаратных и иных средств, пользователи и т.д.)

Эти этапы позволяют сформировать перечень объектов КИИ, подлежащих категорированию [4]. Важно учитывать то, что на момент рассмотрения не все научные объекты могут участвовать в каких-либо научных работах, а используются только в образовательном процессе.

Непосредственно этап категорирования заключается в присвоении объектам категории значимости. Для обоснования сведений о результатах категорирования готовится акт категорирования, который в свою очередь, подготавливается на основании рабочих материалов, заверенных ответственными работниками за эксплуатацию и безопасность объекта.

Заключение

Поэтапная организация процесса категорирования объектов КИИ, ведение документального сопровождения на каждом этапе, привлечение научных работников, участвующих в работе рассматриваемых объектов, принятие во внимание особенностей функционирования объектов в научной сфере деятельности и рабочие материалы, полученные в ходе категорирования, обеспечивают в дальнейшем формирование системы обеспечения информационной безопасности значимых объектов КИИ.

Список литературы

1. Бондаренко А.В., Мушовец К.В., Поршнев С.В., Рогова О.К. Структура действующих нормативных правовых актов в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации. Безопасность информационных технологий. 2023, Т. 30, № 3, с. 126–148. DOI: 10.26583/bit.2023.3.09.

2. Репьева В.Д., Ханмагомедов А.Х. Особенности и проблемы категорирования объектов критической информационной инфраструктуры. Вестник науки. 2023, № 1 (58), с. 193–196. URL: https://www.вестник-науки.рф/article/7156.

3. Салкуцан А.А., Гавдан Г.П., Полуянов А. А. Методика определения критических процессов на объектах информационной инфраструктуры. Безопасность информационных технологий. 2020, Т. 27, № 2, с. 18–34. DOI: 10.26583/bit.2020.2.02.

4. Бакулин М.А. Управление рисками нарушения информационной безопасности значимых объектов критической информационной инфраструктуры. Системная инженерия и информационные технологии. 2023, № 5 (14), с. 78–87. DOI: 10.54708/2658-5014-SIIT-2023-no5-p78.

УДК 004.056

С.В. МОНХ
Научный руководитель – Д.А. ДЯТЛОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПРОТИВОДЕЙСТВИЕ МЕТОДАМ ОБХОДА МЕЖСЕТЕВЫХ ЭКРАНОВ

Цель исследования – разработка рекомендаций по противодействию методам обхода межсетевых экранов. Для достижения этой цели проведена классификация методов обхода, проведено исследование средств и техник, используемых злоумышленниками, и разработаны практические рекомендаций по противодействию методам обхода межсетевых экранов.

Сетевые угрозы в современном мире становятся всё более сложными, и традиционные защитные механизмы, такие как межсетевые экраны, требуют постоянного обновления и адаптации [1]. Цифровизация и глобальная взаимосвязанность сетей создают новые вызовы для информационной безопасности. Межсетевые экраны выступают барьером между внутренними сетями организаций и внешним миром, фильтруя входящий и исходящий трафик. Однако злоумышленники находят способы обойти эту защиту, используя как технические уязвимости, так и психологические методы, такие как социальная инженерия. В исследовании произведен анализ методов обхода межсетевых экранов, который разделён на две основные категории: технические и нетехнические методы.

Технические методы включают: эксплойты, туннелирование, полиморфное и метаморфное ПО, шифрование и стеганографию.

Нетехнические методы включают социальную инженерию и фишинг. Злоумышленники могут использовать обманные письма или поддельные сайты для того, чтобы получить доступ к сетям. Эти методы часто оказываются эффективными, так как многие пользователи недостаточно осведомлены о существующих киберугрозах и рисках.

Был проведен анализ программных и аппаратных средств обхода.

Среди программных средств, активно используемых злоумышленниками, выделяются Tor, OpenVPN, PuTTY, Proxifier и Psiphon. Эти программы позволяют обходить межсетевые экраны путём маскировки трафика, шифрования данных или создания туннелей [2].

Каждая из этих программ имеет свои особенности и сценарии использования, однако все они могут быть использованы для обхода

стандартных защитных механизмов. Это требует от организаций внедрения более сложных методов обнаружения, таких как глубокий анализ пакетов (DPI), который способен идентифицировать аномалии в зашифрованном трафике.

Кроме программных средств, злоумышленники могут использовать аппаратные решения, такие как Raspberry Pi или Wi-Fi Pineapple. Эти устройства позволяют создавать скрытые туннели или перехватывать беспроводной трафик. Например, Raspberry Pi может быть использован для установки VPN-сервера внутри корпоративной сети, что делает трафик незаметным для стандартных межсетевых экранов.

Были перечислены и методы сокрытия трафика: стеганография и шифрование, туннелирование через протоколы HTTPS или DNS,

Для повышения безопасности межсетевых экранов предложено внедрение следующих мер: глубокий анализ пакетов (DPI), регулярное обновление ПО, многофакторная аутентификация (MFA), сегментация сети [3].

Также следует подчеркнуть важность обучения персонала. Зачастую человеческий фактор является слабым звеном в системе безопасности, и злоумышленники используют это с помощью методов социальной инженерии. Повышение осведомлённости сотрудников и регулярные тренинги помогут снизить риск успешных атак.

В условиях постоянно развивающихся киберугроз, важно использовать как технические, так и организационные меры для повышения уровня защиты сетей. Разработанные в ходе исследования рекомендации, такие как внедрение DPI, сегментация сети и регулярное обновление ПО, помогут организациям эффективно противостоять современным атакам и снизить риск компрометации их информационных систем.

Список литературы

1. Евтеев Д. О. Методы обхода Web Application Firewall [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/download/PT-devteev-CC-WAF.pdf (дата обращения: 08.06.2024).

2. Методы обхода межсетевых экранов для приложений / В.Г. Мельников, А.В. Трифанов // Интерэкспо Гео-Сибирь. – 2017. – Т. 9, № 2. – С. 113–117 (дата обращения: 08.06.2024).

3. Методы обхода межсетевых экранов / Д.А. Украинцева, В.Г. Бурлов // Информационные технологии в образовании: Сборник статей научно-практической конференции студентов, аспирантов и молодых ученых, Санкт-Петербург, 31 марта 2021 года / Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. – Санкт-Петербург: Российский государственный гидрометеорологический университет, 2021. – С. 97–101 (дата обращения: 09.08.2024).

УДК 004.056

В.Г. ИВАНЕНКО[1], Н.Д. ИВАНОВА[2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Российский университет транспорта (МИИТ), Москва*

МЕТОДИКА НЕЧЕТКОЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель исследования: разработка методики оценки рисков информационной безопасности (ИБ) с использованием аппарата теории нечеткой логики и нечетких множеств. Построена модель риска в виде дерева, где каждая вершина соответствует лингвистической переменной характеристики риска. В результате предложена человеко-компьютерная система оценки рисков ИБ с применением технологий гибридного интеллекта (как сочетания метода экспертной оценки рисков и возможностей искусственного интеллекта).

Предлагаемая модель риска информационной безопасности (ИБ) представляет собой дерево (рис.), каждая вершина которого – лингвистическая переменная (ЛП), определенная на некотором терм-множестве (например, ЛП «Риск» может принимать лингвистические значения «Низкий», «Средний, «Высокий»). Концевые вершина дерева (на рис. обозначены пунктиром) назовем индикаторами риска ИБ.

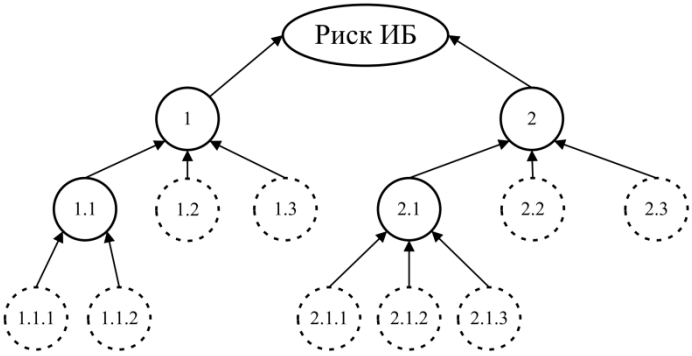


Рис. Модель риска информационной безопасности (ИБ)

В табл. 1 приведен перечень характеристик риска ИБ (применимых для рисков ИБ интеллектуальных систем водного транспорта).

Таблица 1. Перечень характеристик риска ИБ

1	Вероятность реализации угрозы безопасности информации
1.1	Серьезность уязвимости
1.1.1	Оценка уязвимости CVSS (Common Vulnerability Scoring System)
1.1.2	Статистика использования уязвимости
1.2	Возможности нарушителя, достаточные для использования уязвимости
1.3	Защищенность системы
2	Негативные последствия реализации угрозы безопасности информации
2.1	Социальные потери
2.1.1	Ущерб физическим лицам и окружающей среде
2.1.2	Ущерб от утечки информации
2.1.3	Репутационные потери
2.2	Финансовые потери
2.3	Последствия для выполнения технологического процесса

Числовые (четкие) значения индикаторов рисков ИБ задаются методом экспертной оценки с выбранными критериями качества (например, коэффициент конкордации и предпочтительности варианта решения [1]). Для определения степеней принадлежности термам из терм-множества проводится процедура фаззификации с применением выбранной функцией принадлежности [2]. Значения для вышестоящих вершин определяются с использованием операторов агрегирования (логического «ИЛИ» и «И») [3]. Для определения итогового числового (четкого) значения риска ИБ проводится процедура дефаззификации [2]. Пример оценки риска ИБ интеллектуальной системы водного транспорта согласно методике представлен в [3]. Применение аппарата нечеткой логики позволяет интегрировать знания (четко либо нечетко определенные) и опыт экспертов и автоматизировать процесс оценки рисков

Список литературы

1. Лецкий Э.К., Панкратов В.И., Яковлев В.В. Информационные технологии на железнодорожном транспорте / под ред. Э.К. Лецкого, Э.С. Поддавашкина, В.В. Яковлева. – М.: УМК МПС России. – 2000. – 678 с.

2. Rizvi S.S., Mitchell J., Razaque A., Rizvi M.R. A fuzzy inference system (FIS) to evaluate the security readiness of cloud service providers // Journal of Cloud Computing. 2020. № 9(1). 17 p. DOI:10.1186/s13677-020-00192-9.

3. Баранов Л.А., Иванова Н.Д., Михалевич И.Ф. Нечеткая система оценки рисков информационной безопасности интеллектуальных систем водного транспорта // Автоматика на транспорте. – 2024. – № 1 (10). – С. 7–17. – DOI: 10.20295/2412-9186-2024-10-01-7-1

УДК 004.056

Д.А. ШИНЯЕВ, Л.Н. КЕССАРИНСКИЙ, Е.А. СИМАХИН

Национальный исследовательский ядерный университет «МИФИ», Москва

МЕТОДЫ ЗАЩИТЫ ОТ ВОССТАНОВЛЕНИЯ ИЗОБРАЖЕНИЯ ПО ПЭМИ ИНТЕРФЕЙСА DISPLAY PORT

Современные технологии стремительно развиваются, предоставляя широкий спектр интерфейсов для передачи данных. Однако любой интерфейс создает побочные электромагнитные излучения (ПЭМИ), которые могут негативно повлиять на целостность и безопасность передаваемых данных. Авторами предлагаются способы защиты информации, поступающей на экран монитора по различным интерфейсам, в том числе Display Port.

Обнаружение ПЭМИ и его анализ возможен в пределах определенной зоны [1]. Однако размеры данной территории могут быть весьма большими, а внутри границ не гарантироваться значительное уменьшение мощности излучаемых побочных электромагнитных полей. Вследствие чего специалистами были разработаны различные пассивные и активные методы защиты: безэховые или полубезэховые камеры для средств вычислительной техники и генераторы шума в широком диапазоне. С появлением интерфейса Display Port данные средства защиты становятся более затратны из-за увеличения диапазонов частот для подавления и могут блокировать другие частоты, необходимые для взаимодействия компьютерных систем.

В работе предлагаются более точечные методы защиты информативных частот, создаваемых интерфейсом Display Port. Видеосигнал пересылаемый по внешнему интерфейсу в соответствии со стандартом DisplayPort 1.2 для уменьшения излучаемой энергии при преобразовании сигнала использует частотную модуляцию с расширенным спектром (SSFM) [2]. Данный вид частотной модуляции применяется для уменьшения уровня электромагнитных помех при передаче сигнала и эффективно снижает пиковую амплитуду на несущей частоте и ее гармонических частотах.

По частотам, на которых возможно восстановление изображения, например на рис. 1, предлагается построение карты покрытия и создание по ней задания. По заданиям с помощью недорогих программно-определяемых радиоприборов создаются динамические помехи. Данные шумы на каждой из гармоник пересылают сигнал, позволяющий

перекрывать границы базы информативного сигнала образованной при SSFM. Кроме того, шумы несут в себе маскирующее изображение, которое перекрывает основное (скрываемое) изображение монитора, что не позволит нейронным сетям по обученным моделям восстановить исходное изображение с высокой точностью.

Для настройки соединения интерфейса DisplayPort используется специальная структура – DisplayPort Configuration Data (DPCD) [3]. При изменении полей настроек DPCD возможно изменять настройки скремблирования. Изменять значения полей DPCD в операционной системе Windows на уровне пользователя возможно при использовании функции DXGKDDI_DPAUXIOTRANSMISSION callback function. Изменение значений буфера позволит уменьшить уровень мощности на более 7 дБ.

Рис. 1. Анализ изображения монитора с разрешением 1920x1080 без помех

Благодаря описанным методам и разрабатываемому для этого программному обеспечению, специалисты смогут программно уменьшить амплитуды излучаемых информативных сигналов и создать помехи на границах их спектра для скрытия полезной информации, излучаемой интерфейсом Display Port.

Список литературы

1. Хорев Р. Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера // Доклады Томского государственного университета систем управления и радиоэлектроники, 2014, №2, том 32, с. 207–213, ISSN 1818-0442, URL: https://journal.tusur.ru/storage/44795/40.pdf?1465979492. (дата обращения: 17.09.2024)

2. Симахин Е.А. и др. Анализ компонентов архитектуры интерфейса DisplayPort, влияющих на побочное электромагнитное излучение // Безопасность информационных технологий, том 29, №. 1(2022), с. 109–125. DOI: http://dx.doi.org/10.26583/bit.2022.1.10.

3. E.A. Simakhin, D.A. Shinyaev, I.I. Kagin, L.N. Kessarinskiy and A.P. Durakovskiy, "Analysis of Electromagnetic Radiation of LCD Monitor with DisplayPort Interface," 2022 Moscow Workshop on Electronic and Networking Technologies (MWENT), 2022, pp. 1–5. DOI: http://dx.doi.org/10.1109/MWENT55238.2022.9802294

УДК 004.056

А.С. ПОТАПОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

ТЕХНИЧЕСКАЯ ПРОВЕРКА СЛОВАРНЫХ ПАРОЛЕЙ

Брутфорс – серьезная угроза для информационной безопасности (ИБ), так как атака проста в реализации и предоставляет злоумышленнику доступ во внутреннюю сеть с возможностью продвижения. Словарные пароли делают информационную систему (ИС) более уязвимой к компрометации учетных данных. Анализ научных публикаций и различных источников по теме исследования выявил наличие проблемы в данной области. Требуется регулярная проверка для обнаружения недостатков парольной системы. Проанализированы проблемы безопасности слабых аутентификационных данных, современные методы проверки паролей, предложена методика аудита по данному вектору.

Введение

Важно отметить, что брутфорс входит в топ-10 обнаруженных атак и составляет 50,63% от всех угроз [1], выявленных защитным решением, за последний месяц. В 2022–2023 гг. на долю компрометации учетных данных приходилось 11% всех успешных атак [2].

Исследователи [3, 4] отмечают, что большинство пользователей придумывают словарные комбинации, что значительно снижает стойкость пароля. После анализа научных статей [4, 5] сделан вывод, что тестирование на проникновение для проверки паролей не является универсальным подходом, так как, во-первых, не любая организация может позволить такую процедуру, во-вторых, не охватывает все возможные комбинации словарных паролей, в-третьих, отчет по проверке не предоставляет конкретных статистических данных по рассматриваемому аспекту. Таким образом, данная проблема требует особого внимания.

Постановка задачи

Цель исследования: разработать технологию парольного аудита и подготовить рекомендаций по повышению эффективности практики использования паролей. Для достижения поставленной цели предполагается решить следующие основные задачи:

1) анализ проблем безопасности использования словарных паролей. При анализе используется теория вероятностей и математическая статистика, теория игр, методы принятия решений и экспертных оценок;

2) разработка технологии для аудита словарных паролей;

3) разработка рекомендаций по повышению эффективности практического применения результатов исследования;

4) оценка эффективности разработанной технологии и предложенных подходов с использованием теории графов и математической статистики.

Решение задачи

Часто для взлома паролей используются hashcat и John the Ripper. Но запуск этих утилит создает ненужную нагрузку на сеть, требует установки специализированных операционных систем, что может противоречить политики ИБ организации, а также предоставляет пароли в открытом виде, нарушая конфиденциальность проверки и этичные нормы. Поэтому данные механизмы используются косвенно для расширения базы словарей. На рис. 1 представлена методика проверки словарных паролей.

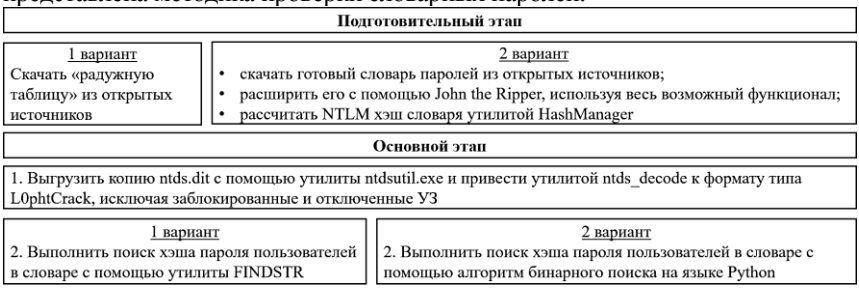


Рис. 1. Обобщенная схема методики аудита словарных паролей

В процессе разработки обнаружилось, что работа утилиты FIND требует больших временных ресурсов. Поэтому использовался вариант написания алгоритма на языке Python, сокративший время поиска с 10 дней до 5 минут. Для автоматизации весь основной этап объединен в полноценный скрипт.

Заключение

В результате создана технология и разработаны рекомендации, позволяющие эффективно проводить аудит словарных паролей, своевременно выявляя недостатки безопасности и предупреждая реализацию угроз ИБ. В дальнейшем предлагается провести анализ УЗ и парольной политики.

Список литературы

1. SECURELIST «Статистика по угрозам, обнаруженным компонентом «Защита от сетевых атак» URL: https://statistics.securelist.com/ru/intrusion-detection-scan/month (дата обращения: 18.09.2024).

2. PTsecurity «Актуальные киберугрозы в странах СНГ 2023–2024» URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024 (дата обращения: 15.09.2024).

3. Гуфан К.Ю., Новосядлый В.А., Эдель Д.А. Оценка стойкости парольных фраз к методам подбора // Открытое образование. 2011. №2. С. 127–130.

4. Тюрин К.А., Семин Р.В. Анализ стойкости парольных фраз на основе информационной энтропии // Известия ЮФУ. Технические науки. 2015. – С. 18–27.

5. Беленко А. Пароли: стойкость, политика назначения и аудит // Защита информации. Инсайд.2019. № 1 (25). С. 61–64.

УДК 004.056

А.М. ПЕРМИНОВ
Научный руководитель – к.т.н., доцент А.П. ДУРАКОВСКИЙ
Национальный исследовательский ядерный университет «МИФИ», Москва

БЕЗОПАСНОСТЬ АУТСОРСИНГА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МОДЕЛИ «БЕЗОПАСНОСТЬ КАК УСЛУГА» (SECAAS)»

Цель исследования – разработка методики оценки доверия аутсорсинга в области информационной безопасности (ИБ) на основе модели SecaaS. Основные задачи: анализ модели SecaaS и принципов работы организаций по модели SecaaS; анализ нормативных и правовых актов Российской Федерации в области регулирования услуг по ИБ; разработка описательной модели информационной системы организации; разработка критериев доверия аутсорсинга в области ИБ на основе модели SecaaS.

Объем рынка публичных облачных услуг в России очень быстро растёт. Основные причины роста являются: удобство, минимизация трудозатрат, уровень вычислительных мощностей, отказоустойчивость. Однако все это не говорит о том, что при помощи внедрений облачных услуг будут решены проблемы информационной безопасности и надёжности [1].

В связи с этим внимание киберпреступников все чаще акцентируется на облачных инфраструктурах и сервисах. Это связано с увеличением популярности всевозможных «облаков» как у обычных пользователей, так и у компаний, некоторые из которых даже перевели в облачное пространство часть корпоративной инфраструктуры.

Основные причины роста популярности SecaaS: удобство, минимизация трудозатрат, уровень вычислительных мощностей, отказоустойчивость.

Сравнение трудозатрат разработки системы защиты своими силами и с использованием аутсорсинга по модели SecaaS идет в пользу аутсорсинга, однако существуют угрозы и проблемы взаимодействия.

Угрозы для заказчика: потеря управления, потеря доверия, осуществления незащищённого подключения пользователями облачных услуг, недостаток управления информацией/облачными ресурсами, потери и утечки данных.

Угрозы для поставщика: приостановка оказания услуг вследствие технических сбоев, конфликт юрисдикций различных стран, эксплуатация угроз технологий виртуализации, непрерывная модернизация.

Потенциальные проблемы установления взаимодействия для заказчика: неопределённость ответственности, привязка и зависимость от поставщика услуг, несогласованность политик безопасности. И **для поставщика:** неопределённость ответственности, несогласованность политик безопасности, недобросовестность исполнения обязательств поставщиками облачных услуг, незащищённое администрирование облачных услуг; политики лицензирования.

При разработке критериев доверия аутсорсингу в области ИБ, необходимо использовать риск-ориентированный подход [2]. Анализ рисков, связанных с передачей части бизнес-процессов на аутсорсинг, поможет отсеять не подходящих поставщиков услуг ещё на этапе их поиска.

Исходя из этого, критериями доверия аутсорсинга в области ИБ являются: безопасность, опыт и наличие компетенции, финансовые и юридические риски, соглашение об уровне предоставления услуг, оперативность в предоставлении информации, гибкость предлагаемых решений. Каждому критерию экспертным методом присваивается балл.

Должна проводиться регулярная проверка поставщика услуг. Оценка финансовых и юридических рисков, SLA, оперативности в предоставлении информации и гибкости предлагаемых решений должна проводиться не реже одного раза в 2 года. При проверке поставщику отправляются блоки вопросов, например, такие: организации защиты данных, анализа защищенности, управления доступом, физической защиты, доступности и производительности, безопасности приложений, управления инцидентами, обеспечения непрерывности бизнеса, регистрации событий безопасности.

Проведя двухэтапную оценку поставщиков услуг в области информационной безопасности, заказчик сможет получит достоверное понимание о том, насколько успешными окажутся его проекты с выбранным поставщиком.

Список литературы

1. Kroenke, D. M., & Boyle, R. J. Upper Saddle River, New Jersey, U.S.A.: Pearson. Experiencing MIS (7th ed.) 2016. [Электронный ресурс] URL: https://online.utsa.edu/experiencing-mis-7th-edition-mypearsonstore/ (дата обращения: 01.09.2024).

2. Премудрости аутсорсинга: как доверять аутсорсеру? – Xbsoftware .URL: https://xbsoftware.ru/blog/premudrosti-autsorsinga-kak-doveryat-autsorseru/ (дата обращения: 01.09.2024).

КИБ-2024
КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Защищенные компьютерные системы и технологии

Руководитель секции – ИВАНОВ М.А., д.т.н.,

заведующий кафедрой №12

УДК 004.056

И.Ю. ЖУКОВ[1, 2], Т.И. КОМАРОВ[2], А.В. ЗУЙКОВ[3]

[1]*ООО «Группа компаний «Инфотактика», Москва*

[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[3]*ООО «Гексагон», Москва*

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ ДЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Реализация импортозамещения в области построения программно-аппаратных комплексов (ПАК) для критической информационной инфраструктуры (КИИ) требует комплексных решений, которые обеспечат существенное повышение их защищённости. Предлагается разработка отечественных программных и программно-аппаратных решений, которые будут формировать иерархию доверия и соответствующую экосистему, применимую на устройствах практически любых классов.

В настоящее время информационные технологии обеспечивают контроль геолокации промышленного оборудования и транспортных средств, область применения, состояние и выполняемые функции, позволяют удаленно обновлять перечень сервисов, а в случае нарушения лицензионных соглашений, имеют возможность анализировать все события и информационные потоки контролируемого оборудования, а также принимать решения на блокирование как части функций, так и оборудования в целом.

Производители оборудования обладают инструментами [1], позволяющими ему «следить» за проданными ИТ-изделиями, за их пользователями, за технологическим оборудованием, а также вмешиваться в функционирование систем с враждебными целями.

В связи с ужесточением санкционной политики со стороны недружественных стран, резко возросла угроза блокирования или перехвата управления технологическим оборудованием особо важных объектов критической информационной инфраструктуры государства. Следовательно, необходимо интенсифицировать процессы перехода на отечественные решения.

Предлагается построение комплексного решения – выстраивание иерархии доверия (цепочек доверия), которое сможет существенным образом повысить защищённость ПАК, применяемых в КИИ:

- встроенное ПО, выполняющее требования спецификации UEFI (Unified Extensible Firmware Interface) [2] и реализующее безопасные механизмы загрузки с использованием концепций, применяемых как в отечественных аппаратно-программных модулях доверенной загрузки (АПМДЗ), так и в зарубежных решениях, соответствующих спецификации TPM (Trusted Platform Module) [3, 4]);
- хостовая ОС на базе ядра Linux со средствами виртуализации и контейнеризации, которые в полной мере удовлетворяют актуальным требованиям ФСТЭК по защите информации;
- пакетный менеджер и соответствующая инфраструктура (система сборки пакетов, репозитории пакетов), которые смогут обеспечить безопасную доставку пакетов, надёжные обновления и конфигурирование ОС;
- корневой и промежуточные удостоверяющие центры для работы сертификатами и электронными цифровыми подписями, которые должны использоваться во всех компонентах предлагаемого решения;
- специализированные ОС на основе конечных автоматов [5] для особо ответственных применений, где ОС на базе ядра Linux могут являться избыточными, неэффективными или недостаточно защищёнными.

Практическая реализация предложений, представленных выше, является одним из необходимых шагов по переходу на отечественные решения и позволяет существенно повысить безопасность, надёжность и доверие компонентов КИИ.

Список литературы

1. Зегжда Д.П., Жуков И.Ю. Особенности обеспечения информационной безопасности вычислительных систем. Безопасность информационных технологий. Т. 28, № 1, 2021. С. 42–61.

2. UEFI Specification 2.10. URL: https://uefi.org/specs/UEFI/2.10 (дата обращения: 20.09.2023).

3. Matrosov A., Rodionov E., Bratus S. Rootkits and Bootkits. San Francisco: No Starch Press Inc., 2019. – 413 с.

4. TPM 2.0 Library Specification. URL: https://trustedcomputinggroup.org/resource/tpm-library-specification (дата обращения: 20.09.2023).

5. Astier J.Y., Zhukov I.Y., Murashov O.N., Bardin A.P. A new OS architecture for IoT. Безопасность информационных технологий. Т. 25б, №1, 2018. С. 19–33.

УДК 004.056

Р.В. ДЗВИНКО[1], В.Д. ПАСТУХОВ[2]

[1]*НПЦ «Бизнесавтоматика», Москва*

[2]*АНО «Институт инженерной физики», Серпухов*

МЕТОДИКА СТЕГАНОГРАФИЧЕСКОГО АНАЛИЗА ИЗОБРАЖЕНИЙ НА ОСНОВЕ ИЕРАРХИЧЕСКОГО АНАЛИЗА АНОМАЛИЙ

В докладе представлена методика стеганографического анализа изображений на основе иерархического анализа аномалий. Вначале анализируются аномалии отдельных пикселов затем – областей изображения и, наконец – всего изображения. Приведены соображения по эффективности методики и ее дальнейшему развитию.

Применение стеганографии для скрытого общения нарушителей является одной из угроз информационной безопасности. Для контейнеров-изображений информация обычно внедряется при помощи современных методов адаптивной стеганографии HUGO, S-UNIWARD и WOW [1–3]. Для противодействия этой угрозе используются методы стеганографического анализа (СА), которые основаны на поверхностном либо глубоком машинном обучении (МО). К недостаткам СА на основе поверхностного МО можно отнести:

- Субъективное, «ручное» формирование признаков;
- Невысокая точность СА.

К недостаткам СА на основе глубокого МО можно отнести:

- Высокая вычислительная сложность обучения;
- Высокая вычислительная сложность эксплуатации;
- Требование большого количества обучающих данных;
- Непрозрачность принимаемых решений.

Для преодоления этих недостатков предлагается методика СА, сочетающая в себе достоинства подходов поверхностного и глубокого МО и лишенная их недостатков.

Вместо ручного формирования признаков на первом шаге методики выполняется обнаружение аномальных пикселов (в которых потенциально могло быть выполнено внедрение). Изображение разбивается на перекрывающиеся прямоугольные фрагменты небольшого размера (например, 5x5). Для каждого фрагмента выполняется декоррелирующее преобразование Карунена-Лоэва, и оценивается аномальность центрального пиксела относительно окружения. Для оценки аномальности используется

бинарный классификатор, обученный на преобразованных фрагментах «чистых» изображений и изображений, содержащих стеговложения. В результате получаются оценки аномальности для всех пикселов изображения.

На втором шаге методики анализируется соотношение оценок аномальности отдельных пикселов и их окружения, находятся аномальные области, в которых было возможно выполнено внедрение.

На третьем шаге методики объединяются оценки аномальности отдельных пикселов и оценки аномальности областей встраивания, и выносится решение за все изображение в целом за счет применения ансамблей классификаторов.

Если сравнить предлагаемый подход к СА с СА на основе поверхностного и глубокого МО, можно сделать следующие выводы:

1. Этап предварительной обработки изображений, имеющийся в известных алгоритмах, в методике отсутствует. Оценка аномалии каждого пикселя получается посредством процесса обучения с учителем.

2. Известные алгоритмы работают сразу со всем изображением, тогда как большинство операций в предлагаемой методике связано с локальными областями изображения. Эту локальную обработку можно распараллелить, кроме того, потребности в памяти меньше.

3. Для классификации на уровне двоичного изображения традиционные СА зачастую используют ансамбль из нескольких классификаторов (например, ансамбль SVM). Ансамблевый классификатор SVM на практике работает медленно из-за многомерных функций. Стегоанализ на основе глубокого МО использует полносвязные (FC) и softmax слои для принятия окончательного решения. Количество обучаемых параметров в слоях FC большое. Напротив, в методике используется усредненная аномалия множества аномальных мест в качестве признаков для тренировки нескольких легковесных бинарных классификаторов и ансамблевый классификатор. Поэтому, стоимость вычислений меньше.

Дальнейшим направлением работы будет изучение вопросов предварительной классификации без учителя фрагментов изображения с целью декомпозировать применение бинарных классификаторов.

Список литературы

1. Pevny X, Bas P., Filler X. Using high-dimensional image models to perform highly undetectable steganography // LNCS. 6387, pp.161–177.

2. Holub V., Fridrich J. Digital image steganography using universal distortion // Proc. 1st ACM Workshop on Inform. Hiding and Multimedia Security, 2013, Montpellier, France, ACM, pp. 59–68.

3. Holub V., Fridrich J. Designing steganographic distortion using directional filters // Proc. 4th IEEE Intern. Workshop on Inform. Forensics and Security, 2012, Tenerife, Spain, pp. 234–239.

УДК 004.056

Р.В. ДЗВИНКО[1], В.Д. ПАСТУХОВ[2]

[1]*НПЦ «Бизнесавтоматика», Москва*

[2]*АНО «Институт инженерной физики», Серпухов*

МОДЕЛЬ ПРИЗНАКОВ ДЛЯ ОБНАРУЖЕНИЯ ОТРАВЛЕННЫХ ИЗОБРАЖЕНИЙ В НАБОРЕ ОБУЧАЮЩИХ ДАННЫХ

В докладе представлена модель признаков, позволяющая обнаруживать отравленные изображения, в которые нарушителем внедрен бэкдор. На основе модели возможно построение методики обнаружения отравленных изображений в наборе данных, то есть его санитизации.

Одним из наиболее опасных классов состязательных атак на нейросетевые системы классификации изображений являются так называемые патч-атаки. Основная идея патч-атак состоит в том, чтобы исказить при обучении модель таким образом, чтобы наличие некоторого триггера, бэкдора во входных данных во время эксплуатации вызывало определенное поведение модели (например, присвоение определенной метки) по выбору атакующего. Таким образом, эта атака выполняется как на этапе обучения (отравление данных), так и на этапе эксплуатации (обман классификатора).

Обнаружение отравленных изображений является не до конца решенной задачей, что связано с тем, что бэкдор может представлять собой незаметный для глаза фрагмент, и методы обнаружения аномалий оказываются неприменимы. В настоящем докладе предлагается модель признаков отравленных изображений, на основе которой возможно построение методики обнаружения отравленных изображений путем последовательного добавления подозрительных изображений в обучающий датасет.

Введем понятие признака изображения как функции $\varphi \in X \to \{0,1\}$. Например, признак $\varphi_{колесо}$ может отображать для изображения $x \in X$ наличие у автоколеса. Тогда любая патч-атака соответствует признаку φ_p, который «обнаруживает» преобразование τ (то есть $\varphi_p = 1$) для тех изображений, к которым было применено преобразование τ (внедрение бэкдора) и $\varphi_p = 0$ для остальных изображений.

Для фиксированного обучающего датасета $S \in Z^n$ введем понятие области поддержки признака φ, в качестве которого примем количество

изображений обучающего датасета, которые активируют соответствующую функцию:

$$\Phi(S) = \{z \in S | \varphi(x) = 1\}. \quad (1)$$

Таким образом в случае бэкдор-атаки с использованием триггера φ_p область поддержки $\Phi_p(S)$ есть множество обучающих изображений, содержащих этот триггер.

Назовем признак сильным если добавление к обучающему датасету изображения, содержащего этот признак, существенно изменяет решения модели.

Пусть имеется распределение D_S всех подмножеств обучающего множества *S*. Для произвольного признака φ и натурального числа *k*, введем понятие функции *k*-выхода модели для признака φ, отображающей это число *k* в решение модели:

$$g_\varphi(k) = \mathrm{E}_{z\sim\Phi(S)}\left[\mathrm{E}_{S`\sim D_S}\left[q\left(z; S`\right) \mid \left|\Phi\left(S`\right)\right| = k, z \notin S`\right]\right], \quad (2)$$

где $z\sim\Phi(S)$ означает случайное изображение из области поддержки $\Phi(S)$ признака φ в множестве S.

Представляется справедливым, что функция выхода $g_\varphi(k)$ должна быстро возрастать с увеличением аргумента для сильных признаков и слабо – для остальных признаков. Например, добавление какой-либо редкой модификации машины к датасету приведет к существенному улучшению классификации этой модификации машины, а добавление часто встречающейся модели к обучающему датасету – не приведет к существенному улучшению классификации этой модели.

В контексте обнаружения триггера φ_p свойство эффективности патч-атаки [1] означает, что $g_{\varphi_p}(|P|) - g_{\varphi_p}(0)$ должно быть большим. Поэтому *k*-силу признака можно определить, как скорость изменения соответствующей функции выхода:

$$s_\varphi(k) = g_\varphi(k+1) - g_\varphi(k). \quad (3)$$

Аналогично функцию выхода и силу признака можно записать для конкретных экземпляров:

$$g_\varphi(z,k) = \mathrm{E}_{S`\sim D_S; z\notin S`}\left[q\left(z; S`\right) \mid \left|\Phi\left(S`\right)\right| = k\right] \quad (4)$$

и

$$s_\varphi(z,k) = g_\varphi(z,k+1) - g_\varphi(z,k). \quad (5)$$

Список литературы

1. Дзвинко Р.В. Модель патч-атак на нейросетевой классификатор изображений / И.А. Созыкин, Р.В. Дзвинко , В.Д. Пастухов // Сборник научных трудов ВНТК «КИБ-2023». – М: МИФИ. – 2023. – С. 16–17.

УДК 004.056

Л.Я. ДОБКАЧ[1], В.Л. ЦИРЛОВ[2]

[1]*АО «Центр эксплуатации объектов космической наземной инфраструктуры», Москва*

[2]*Научно-производственное объединение «Эшелон», Москва*

СПОСОБ ФОРМАЛИЗАЦИИ КОМПЛЕКСНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Ранние средства защиты информации основывались на методах, известных до программно-технического воплощения. Их эволюция привела к созданию сложных систем безопасности. Не всегда имеется полноценная теоретическая база для новых комплексных средств защиты информации. Поскольку недобросовестные производители и некомпетентные пользователи могут внедрять неэффективные решения, предлагается формализованная архитектура системы расширенного обнаружения и реагирования на атаки для решения означенных проблем.

Введение

Средства антивирусной защиты (САВЗ) и межсетевые экраны (МЭ) получили широкое распространение в информационных системах и сетях. Системы обнаружения вторжений (СОВ) также играют важную роль в защите информации.

Объединение данных с различных СЗИ в одном интерфейсе привело к тому, что несколько администраторов могут видеть данные о состоянии сети в общем окне, что облегчает их работу. Помимо непосредственного вывода всех событий безопасности на наглядный график, комплексные СЗИ должны быть способны анализировать поступающие данные и делать выводы на их основе.

Классы комплексных средств защиты информации

Среди современных комплексных систем можно назвать следующие: NGFW; TI, или TIP; SIEM, IRP, SOAR, XDR и другие [1]. Последняя технология входит в класс средств обнаружения и реагирования (*DR), куда также входят EDR, NDR, MDR.

Общие черты вышеперечисленных комплексных СЗИ – интеграция в единой многофункциональной платформе САВЗ, СОВ, межсетевых экранов и других классических СЗИ, автоматизация анализа событий безопасности и связанных инцидентов, реже – меры по активному реагированию.

Формализация структуры XDR

Класс обнаружения и реагирования – один из наиболее современных классов комплексных СЗИ [2], в связи с чем не все его образцы имеют формализованную архитектуру. Так, XDR задумана как средство расширенного обнаружения и реагирования.

Предлагается рассматривать структуру XDR как объединение системы обнаружения и реагирования на конечных узлах (EDR) и сетевой СОВ, как это показано в [3]. Ключевым компонентом выступает терминальный классификатор H на основе взвешенного голосования, что отражено в формуле (1):

$$H = \max\left(\text{sign}\sum_{i=0}^{n} \alpha_i' h^{(i)}, h^{(s)}\right), \quad (1)$$

где $\alpha_i' \in [0;\beta]$ – приведённый весовой коэффициент одного из n классификаторов $h^{(i)}$, $h^{(s)}$ – сигнатурный классификатор. Порог чувствительности $\beta \in [0,1]$ определяет степень взаимного влияния классификаторов.

Оценка точности классификации событий безопасности проводилась на CICIDS 2017 и показала высокие результаты [3], что может говорить об эффективности описанного подхода.

Заключение

Формальное представление общей структуры XDR закладывает недостающую основу под эффективное развитие и применение данного вида комплексных СЗИ.

Предложенный подход не обязан быть единственно возможным, что оставляет задел под альтернативные варианты исполнения XDR-систем, но позволяет более грамотно внедрять данную технологию.

Список литературы

1. Нужный А.С. Регуляризация Байеса при подборе весовых коэффициентов в ансамблях предикторов. Труды Института системного программирования РАН, 2019, т. 31, № 4, с. 113–120.

2. Горбатов В.С., Жуков И.Ю., Кравченко В.В., Правиков Д.И. Кибербезопасность сетевого периметра объекта критической информационной инфраструктуры. Безопасность информационных технологий, 2022, т. 29, № 4, с. 12–26.

3. Сакулин С.А., Алфимцев А.Н., Ломанов А.А., Добкач Л.Я., Недашковский В.М. Выявление сетевых аномалий на основе взвешенного агрегирования с учетом узловых параметров. Вестник компьютерных и информационных технологий, 2022, т. 19, № 7 (217), с. 48–56.

УДК 004.056+004.85

А.Б. АРУСТАМЯН[1, 2], В.Л. ЦИРЛОВ[1, 2], И.И. ШИШКИН[1]

[1] *Московский государственный технический университет им. Н.Э. Баумана*

[2] *Научно-производственное объединение «Эшелон», Москва*

ОБНАРУЖЕНИЕ И ФИЛЬТРАЦИЯ АНОМАЛИЙ В МОДЕЛЯХ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПРОТИВОДЕЙСТВИЯ АТАКАМ ОТРАВЛЕНИЯ ДАННЫХ

В современном мире модели машинного обучения становятся ключевыми элементами многих критически важных систем, что делает их уязвимыми к кибератакам, включая атаки отравления данных. Такие атаки заключаются в добавлении искажённых данных в обучающую выборку, что существенно снижает точность и надёжность моделей.

Введение

В современном мире модели машинного обучения играют важную роль в критически значимых системах, что делает их уязвимыми к кибератакам [1–8]. Одной из таких угроз является атака через отравление данных, при которой в обучающую выборку целенаправленно добавляются искажённые данные [7]. Это ухудшает точность и надёжность модели, что может привести к серьёзным последствиям [4].

Обзор основных типов атак отравления данных

Атаки отравление данных представляют собой внедрение ложной или искаженной информации в тренировочные наборы данных.

Основные типы атак отравления данных:

1. Атаки на выборку – подразумевают изменения поведения модели путем модификации данных в тренировочный набор.
2. Атаки на метки представляют собой изменение меток данных исходных данных (Label Flipping Attacks);
3. Атаки размытия границ (Boundary Attacks) позволяют изменить границы между классами, что приведет к неправильной классификации.

Методы защиты от атак отравления данных

Для защиты от атак отравления данных используются различные методы, а именно:

Анализ данных (Data Sanitization) представляет собой процесс предварительной проверки и очистки обучающего набора [6].

Робастые алгоритмы обучения (Robust Learning Algorithms) – устойчивые к искажениям алгоритмы.

Мониторинг и обнаружение аномалий (Anomaly Detection) предполагает наблюдение за входящими данными и поведением модели [2, 8].

Использование защищенных наборов данных (Secure Datasets).

Заключение

В результате проведённого анализа методов обнаружения и фильтрации аномалий в моделях машинного обучения было рассмотрено, что атаки отравления данных могут существенно снизить точность и надёжность работы систем. Для противодействия таким атакам разработаны различные методы защиты, включая фильтрацию аномалий, использование робастных алгоритмов и мониторинг данных.

Список литературы

1. Горбачев А.А., Максимов Р.В. Проблема маскирования и применения технологий машинного обучения в киберпространстве // Вопросы кибербезопасности. 2023. № 5 (57). С. 37–49.

2. Жилкин С.Д. Выявление аномалий работы по с помощью моделей поведения // Безопасность информационных технологий. 2011. Т. 18. № 1. С. 93–94.

3. Запечников С.В. Модели и алгоритмы конфиденциального машинного обучения // Безопасность информационных технологий. 2020. Т. 27. № 1. С. 51–67.

4. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под. ред. Д.П. Зегжды. – М.: Горячая линия – Телеком. – 2021. – 560 с.

5. Костогрызов А.И., Нистратов А.А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023. № 5 (57). С. 9–24.

6. Котенко И.В., Саенко И.Б., Лаута О.С., Васильев Н.А., Садовников В.Е. Атаки и методы защиты в системах машинного обучения: анализ современных исследований // Вопросы кибербезопасности. 2024. № 1 (59). С. 24–37.

7. Марков А.С. Актуальные вопросы оценки соответствия интеллектуальных средств защиты информации. // В сборнике: Безопасные информационные технологии. Материалы XII Международной научно-технической конференции, посвященной 25-летию кафедры ИУ8. Москва, 2024. С. 92–97.

8. Шелухин О.И., Рябинин В.С. Обнаружение аномалий больших данных неструктурированных системных журналов // Вопросы кибербезопасности. 2019. № 2 (30). С. 36–41.

УДК 004.451

Т.И. КОМАРОВ[1], И.Ю. ЖУКОВ[1,2],
Н.А. ЧЕПИК[1,3], Ю.А. ПОЛОВНЕВА[1]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*ООО «Группа компаний «Инфотактика», Москва*

[3]*АНО «Институт инженерной физики», Серпухов*

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПАКЕТНЫХ МЕНЕДЖЕРОВ

Анализируются основные сложности и тенденции в области управления пакетами и конфигурациями ОС: проблемы традиционных пакетных менеджеров, распространение «неизменяемых» дистрибутивов и контейнеров, развитие функциональных пакетных менеджеров – в частности, Nix и Guix. Предлагаются подходы к развитию отечественных решений в данной области с учётом мирового опыта.

Пакетный менеджер – это программный комплекс, который обеспечивает автоматизацию процесса установки, обновления, конфигурации и удаления ПО на компьютере. Наиболее распространённые дистрибутивы ОС на базе ядра Linux используют классические пакетные менеджеры apt на основе dpkg (apt) или RPM (yum, dnf, zypper) [1].

Основные недостатки классических пакетных менеджеров:

- возможность некорректного/неполного указания зависимостей;
- «ад зависимостей»;
- возможность взаимного влияния пакетов друг на друга;
- отсутствие атомарных обновлений;
- отсутствие полной воспроизводимости сборок.

Кроме того, широкое распространение получила практика использования пакетных менеджеров, специфичных для конкретных технологий или языков программирования (ЯП), например: pip для ЯП Python. Одновременное использование нескольких пакетных менеджеров – потенциальный источник конфликтов и причина проблем с безопасностью.

Данные проблемы не остаются незамеченными. Большое распространение получают «неизменяемые» (immutable) дистрибутивы ОС на базе ядра Linux (например: Fedora Silverblue, Ubuntu Core и др.),

которые воплощают идею, схожую с той, что применяется в мобильных ОС (например, Android) уже достаточно давно: приложения отделены от основной ОС, которая является неизменяемой и атомарно обновляемой.

Однако переход к «неизменяемым» дистрибутивам видится полумерой, т.к. распространение приложений в контейнерах препятствует обеспечению должного уровня безопасности разработчиками ОС.

Но существует альтернативный подход, который был описан в PhD-диссертации E. Dolstra в 2006 г. [2]. Предложенная автором модель функционального пакетного менеджера Nix заключается в том, что пакеты обрабатываются аналогично значениям в функциональных ЯП – они собираются функциями, не содержащими побочных эффектов.

Согласно принципам Nix, пакеты должны находиться в хранилище, размещённом в каталоге /nix/store. При этом, каждый пакет должен храниться в отдельном каталоге с именем вида: /nix/store/<HASH>-<NAME>-<VER>/, где hash – это хеш-сумма, полученная в результате обработки всех входных данных пакета, name – имя пакета, ver – версия пакета.

Основные преимущества пакетного менеджера Nix:

- отсутствие «ада зависимостей»;
- отсутствие влияния пакетов друг на друга;
- атомарность и возможность лёгкого отката обновлений;
- повторяемость сборки отдельных пакетов и всей системы.

В качестве недостатков Nix и NixOS можно отметить сложность использования «обычных» исполняемых файлов и не самое эффективное использование дискового пространства.

Следует обратить внимание, что пакетный менеджер Nix использует собственный функциональный ЯП Nix. Это послужило основной причиной создания построенного на схожих принципах пакетного менеджера Guix [3], который предполагает использование ЯП Guile.

Несмотря на указанные недостатки, функциональные пакетные менеджеры являются востребованной технологией для отечественных разработчиков безопасного программного обеспечения и для органов сертификации средств защиты информации.

Список литературы

1. Usage statistics of Linux for websites [Электронный ресурс] // URL: https://w3techs.com/technologies/details/os-linux (дата обращения: 15.09.2024).

2. Dolstra E. The Purely Functional Software Deployment Model [Электронный ресурс] // URL: https://edolstra.github.io/pubs/phd-thesis.pdf (дата обращения: 15.09.2024).

3. Courtès L. Functional Package Management with Guix [Электронный ресурс] // URL: https://arxiv.org/pdf/1305.4584 (дата обращения: 15.09.2024).

УДК 511.1

Ю.Л. ЗАЧЁСОВ[1], И.М. ЯДЫКИН[2]

[1]*Независимый эксперт, Москва*

[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

ЧЕРЕДОВАНИЕ ЧЁТНОСТИ СУММ МЛАДШИХ РАЗРЯДОВ У ПРОСТЫХ ЧИСЕЛ

Трудность теории чисел состоит в том, что свойства целых чисел относительно умножения (мультипликативные свойства) с их свойствами относительно сложения (с их аддитивными свойствами) связаны очень сложно. Понятие чётности имеет различные применения в математике и информатике, в том числе: проверка делимости; решение линейных уравнений; криптографии; теории чисел и алгоритмов. В докладе дается аксиоматическое утверждение об аддитивной чётности свойственной простым числам, подтверждённое экспериментальным программированием.

В 1797 г. австрийский артиллерист Георг Вега опубликовал книгу [1] со списком подряд идущих простых чисел, а позже Izidor Hafner [2] написал программу проверки таблицы простых чисел. В XVII в. Лежандр «глазками» высмотрел формулу расстояния между простыми числами на примере последовательности, состоящей из миллиона подряд идущих чисел (стр. 9, [3]). Возможности программы Hafner's [2] были расширены до 10^{15} чисел в генерируемой последовательности. Эксперименты с программой показали, что, за исключением первого десятка (в десятичной системе счисления), где простыми числами являются: 2, 3, 5, 7, все дальнейшие простые числа заканчиваются цифрами: 1, 3, 7 и 9. В каждом простом числе сумма двух младших цифр может быть чётным или нечётным числом. В последовательности подряд идущих (десятками) чисел происходит чередование, попадающихся в каждом десятке простые числа бывают либо все чётные, в указанном выше смысле, либо нечётные. Чередование чётности и нечётности происходит с учетом десятков, в которых нет простых чисел. В выделенных двух младших десятичных разрядах цифра младшего разряда указывает на место числа в строке, а цифра старшего разряда указывает на место числа в столбце текущей страницы таблицы.

Определение. Чётность числа, полученного суммированием двух последних младших десятичных разрядов простого числа, назовём аддитивной чётностью простого числа. В каждом десятке (за исключением первого) подряд идущих натуральных чисел у всех простых чисел, попадающих в десяток, значение сумм двух младших десятичных разрядов будет либо чётными, либо нечётными. Возможны десятки, в

которых вовсе нет простых чисел, но при определении аддитивной чётности простых в следующих десятках они все равно учитываются. Определение подтверждено экспериментальным программированием.

Число десятков подряд идущих натуральных чисел, в которых нет простых чисел не всегда одинаково, поэтому с ростом значения натурального числа часто попадаются подряд идущие десятки без простых чисел. По теореме П.Л. Чебышева $0.921\frac{x}{\log_e x} < \pi(x) < 1.106\frac{x}{\log_e x}$ неравенства определяют число простых чисел меньших x [3], поэтому плотность распределения простых чисел можно оценить с помощью функции $\frac{1}{\log_e x}$, тогда расстояние между двумя простыми в среднем будет $\approx \log_e x$. С ростом x это расстояние будет увеличиваться, для больших значений может составлять несколько десятков.

Разработана несложная программа, которая вычисляет средние расстояния между простыми числами в зависимости от числа битов в исследуемом числе. Некоторые результаты сведены в табл. 1.

Таблица 1. Результаты сложения аддитивных признаков чётности

Число бит в исследуемом числе	50	100	350	512	795	1024	2048	4096
Расстояние между простыми числами в десятичных разрядах	16	30	116	159	271	328	676	1372

Экспериментально установлено число бит в модуле факторизации, когда экспоненциальные алгоритмы факторизации становятся неприемлемыми из-за времени их выполнения и для укладывания в приемлемое время начинают требоваться субэкспоненциальные алгоритмы. Это число равно 350 битам. Число битов 512 и 795 – установленные рекорды факторизации в 2003, 2009 и 2019 гг., остальные числа в верхней строке таблицы в настоящее время не поддаются факторизации.

Аддитивное определение чётности при работе с большими числами в случае, когда исследователя интересуют скоростные или временные изменения параметров [4], на основании определения можно забывать значения старших разрядов больших чисел и работать только с младшими разрядами.

Список литературы

1. Vega G., Logarithmische, trigonometrische, und andere zum Gebrauche der Mathematik eingerichtete Tafeln und Formeln, Leipzig: Weidmannischen Buchhandlung, 1797.

2. Сайт www.demonstrations.wolfram.com, демонстрационный пример «Prime Factorizations Table» и «Permutation Group» (дата обращения: 12.09.2024).

3. Чебышев П.Л. Избранные труды. Классики науки. М.: Изд-во Акад. Наук СССР, 1955 – 927 с.

4. Зачёсов Ю.Л., Ядыкин И.М., Алгоритм получения инвариантов. Безопасность информационных технологий, [S.l.], т. 31, № 2, с. 65–80, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1634. DOI: http://dx.doi.org/10.26583/bit.2024.2.04.

УДК 511.1

Ю.Л. ЗАЧЁСОВ[1], И.М. ЯДЫКИН[2]

[1]*Независимый эксперт, Москва*

[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

ПРИМЕНЕНИЯ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ ДЛЯ ФАКТОРИЗАЦИИ ЧИСЕЛ

Факторизация – разложение натурального числа $N = pq$ на простые множители. Существование и единственность такого разложения следует из основной теоремы арифметики. Факторизация предположительно является сложной задачей. Вопрос о существовании алгоритма факторизации с полиномиальной сложностью на доступной вычислительной технике является одной из важных открытых проблем современной теории чисел. В докладе обосновывается эффективность применения алгоритма китайской теоремы об остатках для факторизации чисел, состоящих из двух множителей.

Предположим, что известны остатки $r_{i_1}, \dots, r_{i_s}$ от деления p на p_i, которые получаются по формуле $p = p_i m_i + r_i$, (1)
где r_i – остаток, m_i –натуральное число, а i=i_1,..., i_s.

Тогда, как это экспериментально будет показано ниже, при выполнении условия $\prod_{i=i_1,\dots,i_s} p_i > p$, сравнения вида $p \equiv r_i (\mathrm{mod}\, p_i)$, где i=i_1,..., i_s, по китайской теореме об остатках однозначно дадут истинное значение p [1]. Разработана программа, в которой генерируются два простых числа заданной размерности, по которым вычисляется модуль факторизации N. Формируется список простых чисел $p_1 < \dots < p_s$ из заданного интервала. Тривиальным способом вычисляются предположительно известные остатки от деления заданного простого p на простые числа $p_1 \dots p_s$. Далее применяется функция, выполняющая алгоритм китайской теоремы об остатках [2]. Значение полученного от функции числа сравнивается с p. Если они совпадают, то решение задачи завершено, и можно оценить требуемую длину списка s из маленьких простых чисел. Если ничего не известно об остатках из формулы (1), то трудоёмкость алгоритма будет соответствовать произведению всех простых чисел из списка длиной в s, иначе сумме все тех же простых чисел.

Сначала была проведена серия экспериментов, направленная на выявление факта, какие простые числа лучше брать в список (результаты см. в табл. 1). Эксперименты показали, что самые меньшие подряд идущие простые числа дают лучшие оценки, несмотря на больший размер списка. Далее рассматривались только диапазоны, начинающиеся с 2 и далее по возрастанию (табл. 2).

Таблица 1. Результат обработки различных диапазонов

Диапазон для простых чисел из списка	Количество простых чисел в списке	Мощность перебора (трудоемкость)
2-193	44	3.8×10^3
4000-4153	22	8.9×10^4
500000-500177	15	7.5×10^6

Таблица 2. Изменения трудоемкости в зависимости от размера модуля

Количество бит в модуле	Мощность перебора (трудоемкость)	Количество простых чисел в списке	Мощность полного перебора (трудоемкость в худшем случае)
64	1.2×10^2	10	1.0×10^9
128	3.7×10^2	16	4.4×10^{18}
256	1.1×10^3	26	2.8×10^{37}
512	3.8×10^3	44	2.1×10^{76}
640	5.5×10^3	52	1.1×10^{95}
762	7.6×10^3	60	2.4×10^{114}
1024	1.3×10^4	76	6.2×10^{154}
2048	4.5×10^4	132	2.5×10^{308}
4096	1.6×10^5	235	1.5×10^{621}

Сравним оценки трудоёмкости из табл. 2 с оценками, полученными для: алгоритма факторизации делением пополам (случай, $\sqrt{N}$, [3]); алгоритма NFS по формуле (2) из [3] в табл. 3.

$$L_b = e^{1{,}902\cdot\sqrt[3]{\log_2 N}\cdot\sqrt[3]{(\ln(\log_2 N))^2}}. \qquad (2)$$

Таблица 3. Изменения трудоемкости в зависимости от размера модуля

Количество бит в модуле	$\sqrt{N}$	Мощность полного перебора по формуле (2)
64	$\sim10^9$	$\sim10^8$
128	$\sim10^{19}$	$\sim10^{11}$
256	$\sim10^{38}$	$\sim10^{16}$
512	$\sim10^{76}$	$\sim10^{22}$
640	$\sim10^{96}$	$\sim10^{24}$
762	$\sim10^{114}$	$\sim10^{26}$
1024	$\sim10^{154}$	$\sim10^{30}$
2048	$\sim10^{308}$	$\sim10^{40}$
4096	$\sim10^{616}$	$\sim10^{54}$

Если рассматривать решение задачи факторизации как некую динамическую систему [4], то изложенный подход будет являться последним этапом её работы.

Список литературы

1. Айерлэнд К., Роузен М. Классическое введение в теорию чисел. – М.: Мир, 1987 – 416 с.
2. Сайт www.wolfram.com, (дата обращения: 12.09.2024).
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. − М.: МЦНМО, 2006. −333 с.
4. Зачёсов Ю.Л., Ядыкин И.М., Алгоритм получения инвариантов. Безопасность информационных технологий, [S.l.], т. 31, № 2, с.65-80, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1634. DOI: http://dx.doi.org/10.26583/bit.2024.2.04.

УДК 004.056

М.О. ПАСЕЧНИК, М.А. ФИНОШИН, А.В. ЗУЙКОВ

ООО «Гексагон», Москва

СКРЫТЫЕ КАНАЛЫ В ПРОМЫШЛЕННОЙ СЕТИ CAN ТРАНСПОРТНЫХ СРЕДСТВ

Цель работы заключается в сравнительном анализе скрытых каналов в сети CAN транспортных средств для повышения безопасности передачи сообщений. Исследованы существующие способы и средства построения скрытых каналов в сети CAN для аутентификации сообщений. Основным результатом работы является сравнительный анализ способов аутентификации с использованием скрытых каналов в сети CAN, что особенно актуально в условиях роста подключений транспортных средств к сети Интернет.

Введение

Протокол CAN, разработанный для применения в автотранспорте в середине 1980-х годов и в настоящее время являющийся частью одноименного стандарта, проектировался без учета возможности удаленного подключения, а в логику его работы не заложено механизмов безопасности, например, аутентификации. В связи с ростом функциональных возможностей транспортных средств и подключением их к сети Интернет, протокол CAN требует внедрения дополнительных мер безопасности. Перспективным направлением в данном контексте является изучение механизмов аутентификации сообщений с использованием скрытых каналов в CAN шине, что может повысить безопасность автомобильных сетей без перегрузки дополнительными объемами трафика.

CAN-шина

Шина CAN является витой парой проводов. С ее помощью электронные блоки управления (далее ЭБУ) в автомобиле соединены в единую информационную сеть. В CAN кадре не содержатся данные об отправителе, а значит невозможна аутентификация. Злоумышленник может использовать скомпрометированный ЭБУ для выполнения атак [1, 2], рис. 1.

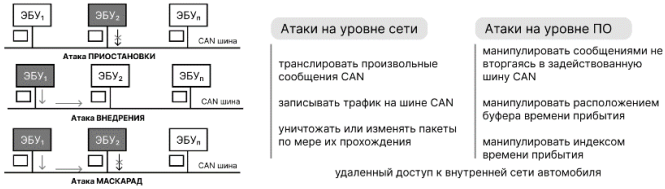


Рис. 1. Атаки на шину CAN с удаленным доступом

Сравнительный анализ способов и средств защиты сети CAN

Проведен сравнительный анализ основных способов защиты шины CAN от атак, добавляющих аутентификацию ЭБУ с использованием скрытых каналов, таб. 1.

Таблица 1. Способы построения скрытого канала на CAN-шине

Название	CANAuth	LiBrA	TACAN	VulCAN	Вандерхалена
CAN+	Да	Да	Нет	Нет	Нет
Исходный код	Нет	Нет	Нет	Да	Нет
Аутентиф. сообщений	Есть	Есть	Нет	Есть	Есть
Аутентиф. передатчика	Нет	Нет	Есть	Есть	Есть
Синхронизации счетчика	Нет	Есть	Есть	Есть	Есть
Защита от атак повторами	Да	Да	Да	Да	Да
Устой-ть к потере сооб-ий	Нет	Частично	Частично	Частичная	Есть
Легковесность ПО	Нет	Нет	Да	Да	Да
Устойчивость к маскараду	Нет	Есть	Нет	Есть	Есть
Актуальность	2011	2012	2019	2019	2021

Система VulCAN [3] использует все преимущества протоколов, исследуемых в работе. Однако была найдена уязвимость в синхронизации счетчиков ЭБУ, для защиты от нее предложен метод Вандерхалена [4]. Скрытый канал позволяет произвести синхронизацию счетчиков безопасным образом, однако он не работает в CAN+ сети и ему необходимо предварительное условие периодичности базового трафика. Важно отметить, что скрытый канал не устойчив к атаке внедрения шума.

Заключение

Скрытые каналы могут повысить безопасность сети CAN. Применение скрытых каналов предложено как эффективное решение для усиления защиты автомобильных сетей в условиях роста подключений и объема данных. Актуальным направлением дальнейших исследований является построение устойчивого к шуму скрытого канала в сети CAN FD на основе метода Вандерхалена.

Список литературы

1. S. Fröschle and A. Stühring. Analyzing the capabilities of the CAN attacker. In Computer Security – ESORICS 2017, p. 464–482. Springer, 2017.

2. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al. Experimental security analysis of a modern automobile. In 2010 IEEE Symposium on Security and Privacy (SP), p. 447–462. IEEE, 2010.

3. J. Van Bulck, J.T. Mühlberg, F. Piessens, VulCAN: Efficient component authentication and software isolation for automotive control networks, in: Proceedings of the 33rd Annual Computer Security Applications Conference, ACM, 2017, p. 225–237.

4. Vanderhallen S. et al. Robust authentication for automotive control networks through covert channels //Computer Networks. – 2021. – Т. 193. – С. 108079.

5. Lotto A. et al. A Survey and Comparative Analysis of Security Properties of CAN Authentication Protocols //arXiv preprint arXiv:2401.10736. – 2024.

УДК 004.056.52

А.М. МАХМУТОВ[1], А.А. СКИТЕВ[2]

[1]*ООО «Оу Эйч Ти», Москва*

[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

АНАЛИЗ ЭФФЕКТИВНОСТИ АППАРАТНЫХ СИСТЕМ ОБНАРУЖЕНИЯ И СМЯГЧЕНИЯ DDOS-АТАК

Проблема безопасности сетевой инфраструктуры становится всё более актуальной. DDoS-атаки представляют серьёзную угрозу для онлайн-сервисов организаций. Анализ существующих аппаратных систем обнаружения атак показал, что они неэффективны против современных DDoS-атак. Для защиты сетевой инфраструктуры необходимы современные алгоритмы, основанные на машинном обучении и энтропии.

Согласно отчету группы компаний «Солар» [1] за первое полугодие 2024 г. на Российские организации было совершено больше на 355 тыс. DDoS-атак чем за весь 2023 г. Средняя мощность атак на Российские компании также выросла с 2.4 Гбит/с за аналогичный период в 2023 г. до 4 Гбит/с.

Критически важно иметь средство обнаружения и смягчения DDOS-атак. Для этих целей был проведен анализ аппаратных решений в области обнаружения атак на предмет возможности их использования в современных реалиях.

В [2] представлен метод вычисления корреляционной меры для сравнения трафика с эталонным. Несмотря на то, что авторами указано, что время определения атаки на их реализации на FPGA составляет менее одной микросекунды, алгоритм требует одну секунду на сбор признаков из трафика. Это не позволяет использовать данный алгоритм для достаточно быстрой реакции на атаку.

В [3] представлен механизм смягчения атаки, основанный на алгоритмах «Hop Count Filtering» [4] и Ingress/Egress-фильтрации. В проведенном эксперименте алгоритм Ingress/Egress-фильтрации сводится к черному и белому спискам. В [3] и [4] трафик для оценки алгоритма был сгенерирован самостоятельно, и авторы не проводят параметры экспериментов, поэтому проведенные эксперименты нельзя воспроизвести точно. Нами проведено моделирование работы алгоритма на наборах данных, используемых для оценки систем обнаружения вторжения. При анализе алгоритма «Hop Count Filtering» на наборе данных, собранном на основе атаки ботнета MIRAI

(2016 г.), удалось получить корректное определение 7% нелегитимного трафика. Результаты представлены на рис. 1. При использовании набора данных CIC-DDoS2019 [5] алгоритм считал все пакеты легитимными.

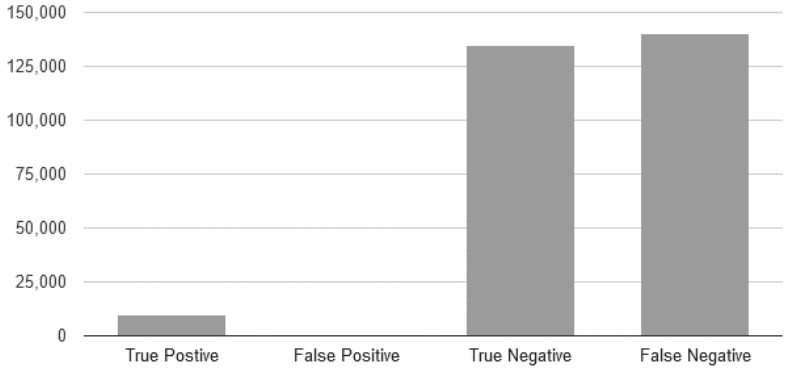


Рис. 1. Результаты HCF на наборе данных ботнета MIRAI

Заключение

Таким образом, на в настоящее время аппаратные системы, представленные в работе, не являются эффективным средством обнаружения и смягчения DDOS-атак. В связи с этим для защиты критически важной сетевой инфраструктуры необходимо использовать современные алгоритмы, основанные на машинном обучении, энтропии. Для того, чтобы справиться с постоянным возрастанием мощности атак, необходимо также использовать специально разработанные аппаратные решения.

Список литературы

1. Отчет о DDoS-атаках на онлайн-ресурсы российских компаний в I полугодии 2024 г. // ГК Солар URL: https://rt-solar.ru/analytics/reports/4677/ (дата обращения: 09.09.2024).
2. Hoque N., Kashyap H., Bhattacharyya D. K. Real-time DDoS attack detection using FPGA. Computer Communications. 2017. Т. 110. С. 48–58.
3. Pham-Quoc C., Nguyen B., Thinh T. N. Fpga-based multicore architecture for integrating multiple ddos defense mechanisms. ACM SIGARCH Computer Architecture News. 2017. Т. 44. №. 4. С. 14–19.
4. Jin C., Wang H., Shin K. G. Hop-count filtering: an effective defense against spoofed DDoS traffic. Proceedings of the 10th ACM conference on Computer and communications security. 2003. С. 30–41.

УДК 004.056

М.П. ГРИГОРЬЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

МЕТОДЫ КОНТРОЛЯ ХОДА ВЫПОЛНЕНИЯ ПРОГРАММ

Предлагается анализ современных уязвимостей, эксплуатируемых злоумышленниками для осуществления атак на ход выполнения программы. Подробно рассмотрены разновидности атак с повторным использованием кода: для каждой атаки приведён листинг уязвимого кода, пример возможной атаки, а также пример безопасного аналога для рассматриваемого кода. Проведён анализ программных и аппаратных подходов к обеспечению защиты хода выполнения программ.

В настоящее время одним из активно развивающихся направлений в области защиты компьютерных систем является применение механизмов контроля целостности потока управления (Control Flow Integrity, CFI). Основными видами атак, с помощью которых может осуществляться воздействие на ход выполнения программы, являются атаки внедрения кода (Code Injection, CI) и атаки с использованием существующего кода (Code-Reuse Attacks, CRA). Современные системы обычно достаточно хорошо защищены от CI, но CRA до сих пор представляют серьёзную опасность.

Одной из наиболее частых причин атак на поток программ является уязвимость переполнения буфера. Разного рода переполнения обычно возникают как следствие программных ошибок и приводят к появлению опасных уязвимостей в конечном программном обеспечении. Переполнение буфера представляет угрозу безопасности, поскольку помимо буфера в памяти находятся критически важные данные. Изменение таких данных может привести к выполнению произвольного кода.

Одной из первых эксплуатаций уязвимости такого рода являлось семейство атак «Ret2libc», осуществление которых приводило к появлению у злоумышленника возможности запуска командной оболочки операционной системы пользователя.

Прямым продолжением данного семейства атак стало возвратно-ориентированное программирование (Return-Oriented Programming, ROP). Злоумышленник использует фрагменты инструкций из существующего кода бинарного файла или библиотеки, заканчивающиеся инструкцией возврата ret. Цепочка таких фрагментов программы может быть использована для выполнения произвольного кода. Особенностью является то, что данный механизм не подразумевает вставки

дополнительного кода. Данный вид атак имеет множество усовершенствований, которые появляются и в настоящее время: JOP, COP, SROP, COOP, BROP, JIT-ROP и другие.

С развитием подходов к эксплуатации уязвимостей происходит и постоянное улучшение методов защиты потока управления.

Механизмы защиты целостности потока программ можно разделить на 2 категории: предоставляемые операционной системой и предоставляемые компилятором.

Одним из классических механизмов защиты является «Ограничение исполняемых областей». В операционной системе Linux он известен как Non-Executable бит, в Windows как «Data Execution Prevention». Механизм «Write XOR Execute» не допускает одновременный доступ к участку памяти на запись и на выполнение. «Stack canary» используется для разделения пространства между локальными переменными и важными служебными данными. Механизм «Position Independent Executable» заключается в загрузке бинарного файла и его зависимостей в случайные адреса при каждом запуске приложения. «Address Space Layout Randomization» случайным образом располагает ключевые элементы процесса во время загрузки исполняемого файла. «Shadow stack» представляет собой отдельный стек в оперативной памяти, который отражает стек вызова основной программы. Механизм «Pointer Encryption» заключается в шифрование всех указателей на инструкции, делая их недоступными для злоумышленников.

Набирающим популярность подходом к защите является ограничение потока управления программой для защиты от атак, изменяющих данный поток. Данная концепция получила название Control Flow Integrity (CFI) и включает анализ схемы потока управления и построение графа потока управления, определяющего набор разрешенных косвенных вызовов. Существует два основных вида механизмов Control Flow Integrity (CFI), которые различаются по способу реализации: программный и аппаратный. Подход «Intel Control-Flow Enforcement Technology» является набором аппаратных механизмов, представленных компанией Intel с целью защиты от уязвимостей. «Control Flow Guard» – механизм Microsoft который добавляет механизмы защиты на этапе компиляции программы. «Reuse Attack Protector» компании PaX работает на этапе исполнения программы.

Одними из перспективных направлений являются «сторожевой» сопроцессор, используемый для выявления ошибок в основном процессоре, и программно-аппаратная архитектура S.O.F.I.A. (Software and Control Flow Integrity Architecture), объединяющую в себе CFI и механизм System Integrity.

УДК 004.056

М.П. ГРИГОРЬЕВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ОЦЕНКА ВОЗМОЖНОСТИ ПОСТРОЕНИЯ ЦЕПОЧЕК ГАДЖЕТОВ ДЛЯ АТАК ПОВТОРНОГО ИСПОЛЬЗОВАНИЯ КОДА В ДИНАМИЧЕСКИ ПОДКЛЮЧАЕМЫХ БИБЛИОТЕКАХ WINDOWS

Предлагается программное обеспечение для поиска фрагментов кода, составляющих ROP-цепочку в бинарном файле. Искомую цепочку гаджетов можно задать на виртуальном языке с помощью набора команд. Отличительной особенностью является полнота по Тьюрингу используемого набора команда. Проведён анализ системных DLL библиотек Windows 7, 10 и 11. Программное обеспечение ориентировано на тестирование различных исполняемых файлов на уязвимость современным атакам на основе повторного использования кода.

В настоящее время на программном и аппаратном уровне повсеместно встраиваются механизмы защиты Control flow integrity. В операционной системе Windows таким механизмом является Control Flow Guard (CFG). Разработчики должны самостоятельно поддерживать данный механизм, компилируя приложения со специальным флагом. Лишь малая доля популярных приложений из официального магазина «Microsoft Store» в действительности поддерживает этот флаг. CFG работает в пространстве ядра и проверяет все косвенные ветвления на предмет допустимости. При этом некоторые динамические библиотеки Windows загружаются по фиксированным адресам, что упрощает возможность проведения атак на основе повторного использования кода.

Рассмотрены различные инструменты, работа которых связана с поиском гаджетов в исполняемых файлах. Инструмент «RopMenu» основан на эмуляции и позволяет анализировать сложные атаки, а также разделять, реконструировать и упрощать цепочки гаджетов. «SpecRop» основан на спекулятивной эксплуатации ROP-цепочек. «AMOCO» строит направленный ациклический граф и использует анализ символьного исполнения для автоматической генерации цепочек ROP. Инструмент «deROP» удаляет ROP-гаджеты из вредоносного программного обеспечения. «ROPium» позволяет искать ROP-цепочки с помощью семантических запросов. «Frankenstein» способен пересобрать вредоносный код из фрагментов кода, полностью взятых из других программ, признанных системами защиты «доброкачественными». Для

описанных программ проведён анализ скорости работы и количества поддерживаемых расширений файлов. Выявлены следующие недостатки рассмотренных инструментов: сложность установки и настройки, высокие требования к ресурсам, ограниченные возможности анализа, ограниченная поддержка архитектур, медленная производительность в условиях большого объёма данных, сложность или отсутствие пользовательского интерфейса. Для работы с Windows DLL библиотеками не разработано специализированного программного обеспечения с пользовательским интерфейсом.

Для разрабатываемого программного обеспечения создан полный по Тьюрингу виртуальный язык. Каждой операции ставится в соответствие набор гаджетов. После начала работы программы в загруженном для анализа файле происходит поиск всех гаджетов, удовлетворяющих заданной операцию. Из всех найденных гаджетов строится дерево, обход которого позволяет выявить подходящую заданной цепочку операций. Поддерживаются следующие расширения файлов: .exe, .scr, .drv, .cpl, .dll, .ocx, .sys, .efi, .acm, .ax, .mui, .tsp, .axf, .bin, .elf, .o, .out, .prx, .puff, .ko, .mod, .so. Виртуальный язык представлен следующими операциями: xor, and, or, not, sub, neg, add, mov, eqc, ltc, spa, sps, gcf, lsd, lc, ld, st.

Рассмотрены следующие системы: Windows 7 SP 1 Сборка 7601, Windows 10 Версия 22H Сборка 22621, Windows 11 Версия 23H2 Сборка 22635. Проанализирован процент найденных гаджетов среди DLL библиотек. Для моделирования машины Тьюринга произведён поиск каждой возможной операции. Исследовано распределение числа найденных гаджетов в зависимости от размера файлов.

Полученные экспериментальные результаты показывают, что злоумышленник сможет найти гаджет для любой произвольной операции, выполняя сложное связывание других операций, когда нужная операция не найдена напрямую, либо же имея данные достаточного объёма. Все самые распространённые по использованию в программах DLL библиотеки являются уязвимыми к ROP атакам, а значит разработанное с их помощью ПО, при отсутствии флага CFG, на этапе компиляции представляет угрозу пользователю.

Используя разработанное программное обеспечение можно найти как одиночные гаджеты в коде файлов, так и цепочки гаджетов. Пользователь может указать специфичные регистры и операции для более точного поиска.

Данный инструмент ориентирован на анализ разрабатываемого программного обеспечения на предмет его уязвимости к атакам и может быть интегрирован в плагины популярных сред разработки.

УДК 004.421.5

М.В. КОВТУН

Национальный исследовательский ядерный университет «МИФИ», Москва

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОДА РИДА-СОЛОМОНА

Аннотация. Целью работы является изучение эффективности помехоустойчивого кодирования кодом Рида-Соломона на языке Python. Применение схожих свойств БЧХ-кодов позволяет достичь лучшей производительности и простоты реализации (за счет синдромного декодирования). Эксперимент показал, что при увеличении числа проверочных символов возрастают требования к вычислительной мощности, а время декодирования значительно превышает время кодирования.

Современные системы передачи информации должны обеспечивать надежность передачи данных в условиях возникающих помех. Для обнаружения и исправления ошибок применяют методы помехоустойчивого кодирования с добавлением избыточной информации (проверочных символов).

В результате сравнения [1] двух классов помехоустойчивых кодов (блочных и непрерывных) по ряду характеристик нельзя однозначно определить оптимальный, так как, например, использование одних кодов приводит к меньшему расширению полосы пропускания, а других – позволит указывать на наличие неисправимых ошибок, поэтому на практике часто используется их комбинация.

Для исследования и демонстрации процессов кодирования и декодирования кодом Рида-Соломона была выполнена программная реализация на языке Python в конечном поле Галуа $GF(2^8)$.

Оригинальная реализация кода Рида-Соломона включает полиномиальную интерполяцию и может требовать выбора наиболее популярного декодирования из всех возможных, что делает алгоритм сложным и неэффективным, особенно для больших исходных сообщений.

Для кодирования и декодирования предлагается использовать алгоритмы, разработанные для кодов Боуза-Чоудхури-Хоквингема (БЧХ-кодов), поскольку коды Рида-Соломона и БЧХ-коды являются подклассами циклических кодов и имеют схожие математические основы [2].

Логика БЧХ-кода позволяет обнаруживать и исправлять ошибки, основываясь на вычисленных синдромах, что дает возможность быстро

определять ошибки и их позиции и делает кодирование и декодирование более практичными и простыми при реализации для реальных приложений.

В качестве входной информации задаём примитивный полином (чтобы определить операции в $GF(2^8)$), исходный текст сообщения, а также количество проверочных символов t и ошибки, которые вносятся в сообщение явно или случайным образом.

В качестве выходной информации получаем текст сообщения, который проверяется на идентичность исходному тексту.

К промежуточной информации относятся: закодированное исходное сообщение; вычисленный локатор ошибок и их позиции; признак корректности позиций ошибок; значения ошибок и синдромов.

Результат тестирования работы программы показывает, что сообщения восстанавливаются верно при наличии не более $t/2$ ошибок при количестве проверочных символов t.

При проведении тестирования, с целью анализа зависимости времени работы программы от числа проверочных символов при фиксированном количестве информационных символов, на 5000 запусков было получено, что среднее время декодирования одного сообщения превышает время кодирования от четырех (при малых t) до восьми раз (при больших t).

Объем вычислительной мощности, необходимой для кодирования и декодирования кодов Рида-Соломона при фиксированной длине сообщений, зависит от числа t (чем больше t, тем большее число ошибок может быть исправлено, но это потребует большей вычислительной мощности).

Таким образом, применение кодов Рида-Соломона для исправления ошибок делает задачу построения эффективных алгоритмов декодирования этих кодов весьма актуальной. В настоящее время реализуется множество различных алгоритмов декодирования кода Рида-Соломона, однако время декодирования все еще остается большим.

Список литературы

1. TM Synchronization and Channel Coding, Recommendation for Space Data System Standards CCSDS 131.0-B-1, Issue 1, Blue Book, Consultative Committee for Space Data Systems, September, 2023., 22 с. https://public.ccsds.org/Pubs/131x0b5.pdf (дата обращения: 08.08.2024).

2. Reed-Solomon Error Correction. https://sigh.github.io/reed-solomon/ (дата обращения: 08.08.2024).

УДК 004.056

К.В. АГИЕВЕЦ[2], М.А. ИВАНОВ[1, 2],
М.А. КОНДАХЧАН[2], А.В. СТАРИКОВСКИЙ[1]
[1]*Государственный университет управления», Москва*
[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

АЛГОРИТМИЧЕСКОЕ МЫШЛЕНИЕ В ЗАДАЧЕ НАДЕЖНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛУ СВЯЗИ

Рассматривается пример использования алгоритмического мышления, эвристических приемов разрешения технических противоречий и метода контрольных вопросов при решении задачи защиты информации, пересылаемой по каналу связи.

При передаче данных по каналам связи приходится решать три задачи: обнаружение и исправление ошибок, вызванных действием помех в каналах связи (обеспечение помехозащищенности); обеспечение секретности информации; защиту от навязывания ложных данных (имитозащиту).

Традиционно каждая из этих задач решается на основе использования отдельного механизма – соответственно помехоустойчивого кодирования, шифрования, формирования (на стороне отправителя) и проверки (на стороне получателя) контрольного кода целостности (имитовставки). В результате реальные системы передачи данных громоздкие и недостаточно эффективные.

Итак, у нас имеется *изобретательская задача*: необходимо найти единое техническое решение, обеспечивающее защиту от случайных искажений информации в канале связи с помехами; секретность информации; защиту от умышленных искажений информации (имитозащиту).

Применим *алгоритмическое мышление*, а также воспользуемся *эвристическими приемами* разрешения технических противоречий и *методом контрольных вопросов* [1]. Сформулируем *идеальный конечный результат*: требуется код, который решает все три упомянутые выше задачи защиты информации и при этом обеспечивает наперед заданную вероятность правильного приема информации при решении первой задачи.

Используем *посредника*, создадим виртуальный (преобразованный) канал связи с нужными нам свойствами, когда все вектора ошибок на выходе преобразованного канала связи будут равновероятны. Таким образом, на выходе реального канала связи нужен блок преобразования R (Random), на входе которого будет реальный вектор ошибок e, а на выходе – будет сформирован преобразованный вектор ошибок e' с вышеупомянутыми свойствами. В криптографии есть термин, близкий к термину вектор ошибок, а именно дифференциал (или разница) двух двоичных строк. Криптографические преобразования обладают свойством непредсказуемости, которое означает, что при любом входном дифференциале все выходные дифференциалы равновероятны. По этой причине блок R логично назвать блоком стохастического (т.е. непредсказуемого) преобразования.

Применим принцип *предварительного антидействия* и получим схему, показанную на рис. 1. Как показано на рис. 1, преобразованный дискретный канал работает не с битами, а с L-разрядными двоичными наборами данных. Если эти наборы назвать Q-ичными символами, принимающими значения от 0 до $2^L - 1$, полученный преобразованный дискретный канал с учетом свойств блока R^{-1}, можно с полным основанием назвать Q-ичным симметричным каналом. В случае ошибки каждый из $(2^L - 1)$ ненулевых векторов ошибки появляется на его выходе с вероятностью $p/(2^L - 1)$, где p – вероятность ошибки в канале связи.

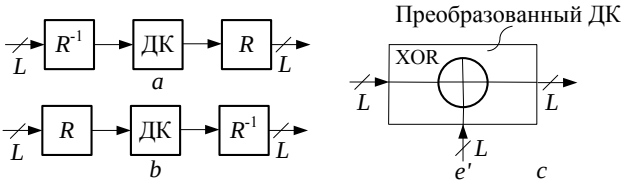


Рис. 1. Преобразованный дискретный канал: *a* – первоначальная схема; *b* – окончательная схема, предложенная автором стохастического кода [2]; *c* – преобразованный ДК, действия помех в котором, т.е. искажение Q-ичных символов, задается преобразованным вектором ошибок e'. ДК – реальный дискретный канал

Список литературы

1. Иванов М.А. Алгоритмическое мышление в задачах защиты информации. − Настоящий сборник.

2. Осмоловский С.А. Стохастические методы защиты информации. – М.: Радио и связь, 2003.

УДК 004.056

М.А. ИВАНОВ
Государственный университет управления», Москва
Национальный исследовательский ядерный университет «МИФИ», Москва

АЛГОРИТМИЧЕСКОЕ МЫШЛЕНИЕ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматриваются примеры использования алгоритмического мышления, эвристических приемов разрешения технических противоречий и метода контрольных вопросов при решении различных задач защиты информации.

В основе вычислительного мышления лежат способность мыслить логически и алгоритмически, не упуская никаких важных деталей, эффективные способы решения сложных проблем. Специальность «Информатика и вычислительная техника» уникальна тем, что она объединяет все эти разнообразные навыки. Как только удается получить алгоритмическое решение какой-либо задачи, эти задачи становится возможным решать даже не задумываясь, следуя актам алгоритма. При наличии алгоритма задачу решит кто угодно, в том числе ЭВМ. Сила вычислительного мышления заключается в том, что следование алгоритму обеспечивает решение не какой-то одной конкретной задачи, а большой группы часто вовсе не однотипных задач [1]. Существует множество определений и толкований термина Computational Thinking, который начал широко использоваться после публикации в 2006 г. одноименной работы Жаннетты Винг (Jeanette Wing) [2]. Можно, например, упомянуть иногда используемый термин «компьютерное мышление», который ввел специалист по искусственному интеллекту Сеймур Пайперт. Согласно [3] он определил его так: «компьютерное или вычислительное мышление – это мыслительные процессы, участвующие в постановке проблем и представлении их решения в форме, которая может быть эффективно реализована с помощью человека или компьютера».

Для поиска решений сложных (изобретательских) задач в свое время было предложено понятие *идеального конечного результата* (ИКР) [4]. Удивительно, но факт, при упорном движении к ИКР поразительно часто возникает одна из четырех ситуаций, показанных на рис. 1.

Рассматриваются примеры использования алгоритмического мышления, эвристических приемов разрешения технических

противоречий и метода контрольных вопросов при решении задач синтеза 2D и 3D криптоалгоритмов; построении генераторов псевдослучайных чисел, ориенти- рованных на решение различных задач защиты информации; обеспечении комплексной защиты информации, пересылаемой по каналам связи и ряда других.

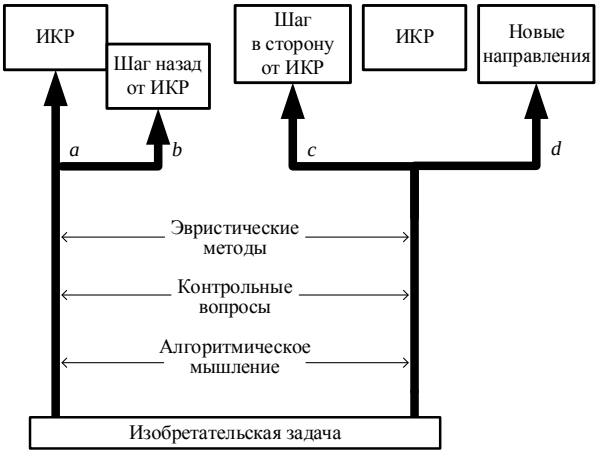


Рис. 1. Варианты исхода при движении к ИКР:
a – мы достигаем ИКР; *b* – мы достигаем результата, близкого к ИКР (шаг назад от ИКР); *c* – мы решаем задачу, отличную от исходной, о которой в начале пути даже не подозревали (шаг в сторону от ИКР); *d* – мы открываем новое направление развития технической системы, о котором в начале пути не подозревали

Список литературы

1. Керзон П., Макоун П. Вычислительное мышление. Новый способ решать сложные задачи. Пер. с англ. – М.: Альпина Паблишер, 2018. – 266 с.
2. Wing J. Computational Thinking // Communications of the ACM, 2006, Vol. 49, № 3, p. 33–35.
3. Эдвард де Боно. Латеральное мышление. Учебник. – Минск: Попурри, 2012 – 384 с.
4. Альтшуллер Г.С. Творчество как точная наука. – М.: Советское радио, 1979. – 105 с.

Направление

Интеллектуальное управление сетевой безопасностью

Руководитель секции – МИЛОСЛАВСКАЯ Н.Г.,
д.т.н., профессор

УДК 004.056.5

И.О. ЛАПШИН, И.С. СТРУЧКОВ
Московский университет МВД России им. В.Я. Кикотя

ТЕХНОЛОГИИ ВИРТУАЛЬНЫХ СЕТЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Рассматриваются задачи защиты сетевых структур с помощью технологий виртуальных частных сетей, реализуемых на базе отечественных программных продуктов «ViPNet» и «Континент». Особое внимание уделяется компонентам этих технологий, которые определяют архитектурную гибкость в сочетании с современными методами и средствами обеспечения кибербезопасности.

При анализе кибербезопасности распределённых информационных сетей следует учитывать не только угрозы со стороны внешних злоумышленников, но и потенциальные риски, исходящие от внутренней сети, доступ к которой зачастую бывает более уязвим для нарушений**.**

При этом важно создать такую интегрированную защищённую среду в телекоммуникационной инфраструктуре, чтобы обеспечить надёжную безопасность коммуникаций, технических средств и информационных ресурсов. Это требует учёта взаимодействия с внешними техническими средствами и ресурсами, способствуя формированию эффективной защиты от возможных угроз.

Задачи защиты сетевой структуры

С учетом актуальных требований, касающихся киберзащиты сетевой инфраструктуры и передачи сетевого трафика, возникает необходимость в решении следующих задач:

- обеспечение квалифицированными специалистами в области информационной безопасности;
- нормативно-правовое регулирование защищенного сетевого взаимодействия, в том числе – между ведомствами;
- оперативное реагирование на появление новых угроз кибербезопасности, что требует ее постоянного мониторинга и анализа;
- расширение инструментов комплексной защиты от угроз в области кибербезопасности;
- сокращение расходов на систему защиты информации, что требует оптимизации существующих подходов и технологий.

Новые решения

Одним из элементов системы киберзащиты является аппаратно-программный комплекс шифрования (АПКШ) «Континент» 3.М.3, для создания магистральных VPN-сетей повышенного уровня безопасности с использованием алгоритмов шифрования государственного стандарта.

Комплекс направлен на применение в трех направлениях:

– использование межсетевых экранов для защиты внутренних сетевых сегментов от несанкционированного доступа;

– осуществление криптографической защиты (согласно ГОСТ 28147–89) передаваемых данных;

– построение информационных подсистем с разграничением физического доступа.

Технологии «ViPNet» включены в Единый реестр российского программного обеспечения, полностью соответствуя требованиям государственной программы импортозамещения. «ViPNet» представляет комплексное решение, включающее разнообразные программные продукты и сетевые технологии для эффективного управления кибербезопасностью. Обеспечивает защиту рабочих станций от внешних и внутрисетевых угроз путём фильтрации трафика, а также безопасную работу удалённых сотрудников в корпоративных системах и сервисах.

Заключение и выводы

Технологические решения на базе программных комплексов «Континент» и «ViPNet» удовлетворяя современным практическим потребностям, обеспечивают надежную защиту данных, соответствуя высоким требованиям кибербезопасности. Этот процесс не ограничивается установлением обновлений, включая в себя комплекс мероприятий, направленных на постоянный мониторинг и оперативное внедрение усовершенствований в области кибербезопасности.

Список литературы

1. Гусев В. В., Чаплыгин В. Е. Администрирование системы защиты информации ViPNet (Windows & Linux). М.: Горячая линия – Телеком, 2018. – 366 с.

2. Прудников А.И., Шахов В.Г. Особенности использования технологии ViPNet для защиты информации в корпоративных сетях. URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniyatehnologii-ViPNet-dlya-zaschity-informatsii-v-korporativnyh-setyah. (Доступ 15.09.2024).

3. Акинина Л.Н., Попов В.Б., Перехрест Р.Д. Программно-аппаратные комплексы ViPNet и их использование в корпоративных сетях // Научный вестник Крыма. 2016. № 3. URL: https://cyberleninka.ru/article/n/ programmno-apparatnye-kompleksy-ViPNet-i-ih-ispolzovanie-v-korporativnyh-setyah. (Доступ 15.09.2024).

УДК 004.056

А.С. МИНЗОВ[1], А.Ю. НЕВСКИЙ[1], О.Р. БАРОНОВ[1], Н.А. ТОКАРЕВА[2]

[1]*Национальный исследовательский институт «МЭИ», Москва*

[2] *Государственный университет «Дубна», Московская обл.*

ОБРАБОТКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

В докладе рассматривается новый подход к обработке рисков информационной безопасности, позволяющий использовать его в автоматизированных системах управления СМИБ. В основе этого подхода положены идеи корреляции параметров рисков - угроз, уязвимостей и информационных активов, предложены способы агрегации рисков по их параметрам, обоснованы стратегии ранжирования рисков при ограничениях на общие затраты и сформулированы условия поиска условно-оптимальных решений при обосновании плана обработки рисков.

Введение

Существующие методики обработки рисков информационной безопасности (ИБ) основаны на рекомендациях стандарта [1], которые ориентированы на ручные методы оценки и обработки рисков. Это существенно ограничивает применение этих методик при автоматизированной обработке рисков (АОР) ИБ АСУ.

Постановка задачи

Целями проектирования АОР являются:

1. Разработка плана обработки рисков информационной безопасности на основе оценки их параметров, определения ущерба, способа обработки риска и мер защиты.
2. Проведение анализа рисков по его отдельным параметрам (угрозам, уязвимостям, активам, мерам защиты) и поиск условно-оптимального решения.

Решение

В качестве модели риска ИБ была принята расширенная модель плана обработки рисков на основе стандарта [1]. Исходные параметры и результаты оценки и принятия риска ($\boldsymbol{X}$) представлены в выражении (1), а результаты по условно-оптимальному решению в выражении (2):

$$\begin{cases} X = <Nt, Et, Nv, Ev, Na, Ea, M, V, C, Z, U> & (1) \\ Y = < s_z, s_u >, C_d & (2) \end{cases}$$

где ***Nt, Nv, Na –*** наименования (коды) угроз, уязвимостей, активов;

Et, Ev, Ea – значения возможностей появления угроз, величин уязвимостей и ценностей активов в числовых значениях лингвистических переменных;

M - метрики рисков;

V, C, Z, U – вариант обработки рисков, контрмеры по защите, затраты, ущерб (риск). Выбор защитных мер определяется анализом агрегатов рисков |***Nt*| : | *Nv*| : | *Na***|** [2].

U – возможные значения ущерба (риска), выраженные в абсолютных значениях, например в денежных эквивалентах. метод, основанный на имитационном моделировании значений рисков при заданных интервалах их значений. Применение этого подхода к оценке показателей ущерба основано на Центральной предельной теореме

s_z, s_u - суммарные значения затрат на принятие мер защиты и возможного ущерба;

C_d – функция цели управления рисками информационной безопасности, где индекс s определяет стратегию анализа риска по одному из параметров модели (1). В выражении (3) представлено одно из лучших решений, в котором значение предотвращенного ущерба является максимальным при ограничениях по затратам.

$$Cd = \max_s \left(\sum_{i=1}^{k} u_i^s \right), \left(\sum_{i=1}^{k} z_i^s < z_0 \right), i = \overline{1,k}, s = \overline{1,n}. \qquad (3)$$

Заключение

Рассмотренная модель реализована в прототипе задачи АОР и оценены погрешности определения предотвращенного ущерба методом имитационного моделирования [2].

Список литературы

1. Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности. ГОСТ Р ИСО/МЭК 27005-20012.

2. Минзов А.С., Невский А.Ю., Баронов О.Р. Управление рисками информационной безопасности: Монография/ Под редакцией А.С. Минзова. – М.: ВНИИгеосистем, 2019. – 110 с.

УДК 004.056

А.В. БАЛЫБЕРДИН

Финансовый университет при Правительстве Российской Федерации, Москва

ПРОБЛЕМЫ ВНЕДРЕНИЯ МЕТОДОВ ОБНАРУЖЕНИЯ АНОМАЛИЙ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Системы обнаружения вторжения (СОВ) выявляют несанкционированные действия злоумышленника в сети. В настоящее время активно ведутся исследования по разработке методов обнаружения аномалий на основе машинного обучения для СОВ. На основе анализа работ по методам обнаружения аномалий в докладе представлен ряд вопросов и проблем, возникающих при их внедрении.

Введение

Для выявления несанкционированных действий в сети применяют системы обнаружения вторжений (СОВ). В зависимости от способа детектирования кибератак СОВ бывают двух типов: системы на основе сигнатурного анализа и системы обнаружения аномалий. Системы обнаружения аномалий (СОА) выявляют новые и неизвестные кибератаки и аномалии на сеть. Для повышения точности выявления СОА активно применяют методы машинного обучения.

Постановка задачи

В настоящее время проводится значительное количество исследований по обнаружению сетевых аномалий [1]. Целью доклада является систематизация знаний и формализация проблем на основе анализа методов обнаружения аномалий.

Анализ методов обнаружения аномалий

В последнее время исследования по обнаружению сетевых аномалий направлены на использование алгоритмов машинного обучения. Особое внимание уделяется методам глубокого обучения [3] и гибридным методам [4]. Для повышения точности выявления сетевых аномалий применяют различные алгоритмы по предобработке и оптимизации признакового пространства наборов данных, проводят работы по усовершенствованию алгоритмов классификации и настройке оптимальных гиперпараметров в искусственных нейронных сетях (ИНС). Рассматриваются новые типы классификаций, такие как многозначные

классификации [5] и прогнозирование временных рядов [2]. Значительная часть исследований фокусируется на оценки точности методов как основной метрике классификации сетевых аномалий. В результате данные методы в лабораторных условиях показывают высокие показатели точности классификаций, но на практике данные показатели значительно снижаются, что приводит невозможности использовать СОА в реальной сети.

Проблемы внедрения СОА

Результатом анализа методов обнаружения аномалий СОА были выявлены следующие проблемы:

- Отсутствует единые подход к оценке методов обнаружения аномалий.
- Низкая точность обнаружение редких атак и аномалий.
- Для практического применения одной оценки точности метода недостаточно.
- Постоянное изменение параметров реальной среды снижает точность классификации.
- Отсутствие механизма, позволяющего выявлять и принимать решение по переобучению метода.

Заключение

В докладе представлен анализ методов обнаружения аномалий, показаны проблемы применения данных методов на практике.

Список литературы

1. Шелухин, О. И. Сетевые аномалии. Обнаружение, локализация, прогнозирование: [текст] / О. И. Шелухин. - Москва: Горячая линия-Телеком, 2019. – 447 с. ISBN 978-5-9912-0756-0.

2. Psychogyios, K.; Papadakis, A.; Bourou, S.; Nikolaou, N.; Maniatis, A.; Zahariadis, T. Deep Learning for Intrusion Detection Systems (IDSs) in Time Series Data. Future Internet 2024, 16, 73. https://doi.org/10.3390/ fi16030073.

3. Xinwei Yuan, Shu Han, Wei Huang, Hongliang Ye, Xianglong Kong, Fan Zhang, A simple framework to enhance the adversarial robustness of deep learning-based intrusion detection system, Computers & Security, Volume 137, 2024, 103644, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103644.

4. A. A. E. -B. Donkol, A. G. Hafez, A. I. Hussein and M. M. Mabrook, "Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks," in *IEEE Access*, vol. 11, p. 9469-9482, 2023, doi: 10.1109/ACCESS.2023.3240109.

5. Шелухин О.И., Раковский Д.И. Многозначная классификация компьютерных атак с использованием искусственных нейронных сетей с множественным выходом. Труды учебных заведений связи. 2023;9(4):97-113. https://doi.org/10.31854/1813-324X-2023-9-4-97-113.

УДК 004.056

А.Д. АБХАЗИ

Московский государственный лингвистический университет, Москва

КОРРЕЛЯЦИЯ И ИНТЕГРАЦИЯ СОВ И SIEM

В докладе рассматриваются возможности и проблемы интеграции и корреляции систем обнаружения вторжений (СОВ) с системами управления событиями и инцидентами информационной безопасности (SIEM). Подчёркивается важность правильной интерпретации сообщений, поступающих от СОВ в SIEM, и рассматриваются методы оптимизации взаимодействия этих систем.

Современные системы информационной безопасности требуют интеграции различных компонентов для обеспечения эффективного мониторинга и защиты. Одним из ключевых аспектов является корреляция сообщений от систем обнаружения вторжений (СОВ) и их интеграция с системами управления событиями и инцидентами информационной безопасности (SIEM).

Основная задача СОВ заключается в сигнатурном анализе сетевого трафика и генерации сообщений о возможных инцидентах. Эти сообщения должны быть корректно интерпретированы системой SIEM для дальнейшей корреляции и визуализации данных. Однако возникает проблема соответствия сигнатур СОВ и правил синтаксического анализатора SIEM, особенно в условиях частого обновления сигнатур.

Для решения данной проблемы предлагается методика оптимизации, которая заключается в исключении из набора правил SIEM тех, что соответствуют неактивным сигнатурам СОВ. Такой подход позволяет снизить нагрузку на вычислительные мощности SIEM. Важно отметить, что набор сигнатур СОВ может варьироваться в зависимости от настроек администратора, что требует постоянного обновления правил на стороне SIEM.

На рис. 1 представлена стандартизированная схема взаимодействия СОВ и SIEM, демонстрирующая ключевые этапы интеграции. Слева расположены основные компоненты СОВ, ответственные за обновление сигнатур и генерацию сообщений, а справа — компоненты SIEM, осуществляющие синтаксический анализ и оптимизацию правил. Такая структуризация позволяет визуально выделить зоны ответственности каждой системы и продемонстрировать их взаимосвязь.

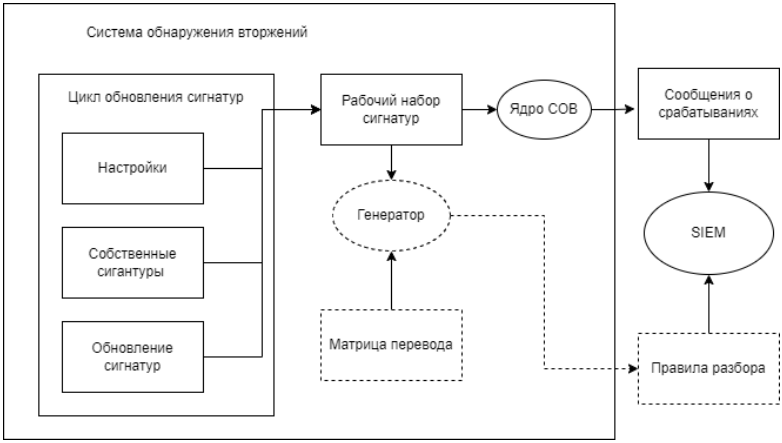


Рис. 1. Схема взаимодействия СОВ и SIEM.

На рынке также присутствуют комплексные интегрированные решения, включающие СОВ и SIEM. Однако их использование сопряжено с рядом трудностей, таких как высокая стоимость и сложности интеграции со сторонними устройствами. В качестве решения этих проблем предлагается внедрение модуля генерации правил синтаксического анализатора, который интегрируется в цикл обновления сигнатурных баз СОВ. Этот подход позволяет синхронизировать работу СОВ и SIEM, обеспечивая актуальность и полноту обрабатываемых данных.

Таким образом, представленный метод интеграции и корреляции СОВ и SIEM позволяет улучшить эффективность мониторинга информационной безопасности и снизить риски, связанные с некорректной интерпретацией данных.

Список литературы

1. Бородавкин Д.А., Почурицин А.В., Потуремский И.В. Метод интеграции систем обнаружения вторжений, совместимых с сигнатурами формата Snort, с системами управления событиями и инцидентами информационной безопасности // Решетневские чтения. 2014. №18. URL: https://cyberleninka.ru/article/n/metod-integratsii-sistem-obnaruzheniya-vtorzheniy-sovmestimyh-s-signaturami-formata-snort-s-sistemami-upravleniya-sobytiyami-i (дата обращения: 09.09.2024).

УДК 004.89

В.Ю. СТЕПАНЬКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ЦИФРОВЫЕ ДВОЙНИКИ ДЛЯ КИБЕРЗАЩИТЫ: МОДЕЛИРОВАНИЕ И УПРАВЛЕНИЕ СЕТЕВЫМИ УГРОЗАМИ С ИСПОЛЬЗОВАНИЕМ МНОГОАГЕНТНЫХ СИСТЕМ

С увеличением количества и сложности кибератак традиционные методы защиты сетевой инфраструктуры становятся недостаточно эффективными. В условиях быстрого развития цифровых технологий появляется необходимость в более гибких и адаптивных системах киберзащиты. Одним из перспективных подходов является использование цифровых двойников и многоагентных систем (MAS) для моделирования сетевых угроз и управления ими в реальном времени. Целью данного доклада является исследование возможностей интеграции цифровых двойников и многоагентных систем для построения интеллектуальной системы киберзащиты, способной предсказывать угрозы и принимать меры по их нейтрализации.

Цифровой двойник — это виртуальная модель реальной сети, которая позволяет отслеживать ее текущее состояние, прогнозировать поведение и моделировать различные сценарии. В контексте кибербезопасности цифровой двойник может использоваться для динамического мониторинга сетевого трафика, обнаружения аномалий и симуляции атак. Он предоставляет возможность предсказывать угрозы и оценивать эффективность защитных мер до их реального применения.

Многоагентные системы (MAS) представляют собой распределенную систему автономных программных агентов, каждый из которых выполняет конкретные функции, такие как сбор данных, анализ трафика, обнаружение атак и реагирование на инциденты. Эти агенты могут взаимодействовать друг с другом, делясь информацией и координируя свои действия для обеспечения безопасности всей системы.

В результате интеграции MAS с цифровым двойником возникает система, способная в реальном времени: моделировать различные типы угроз (например, DDoS, атаки на уязвимости); эффективно предсказывать новые угрозы на основе собранных данных; адаптировать защитные механизмы под динамически меняющиеся условия сети.

Методы имитационного моделирования играют ключевую роль в разработке и тестировании систем киберзащиты. Цифровой двойник

позволяет проводить эксперименты с симуляцией различных типов атак без угрозы для реальной сети. Многоагентная система взаимодействует с цифровым двойником для сбора данных, анализа сценариев атак и разработки стратегии защиты.

Использование имитационного моделирования в сочетании с MAS позволяет: воспроизводить реальные сетевые атаки для оценки их влияния на инфраструктуру; тестировать реакцию системы на различные типы угроз, включая новые и неизвестные атаки; оценивать эффективность предложенных защитных мер в условиях, приближенных к реальным.

Архитектура разрабатываемой системы включает в себя следующие ключевые компоненты: цифровой двойник сети; агенты; центр управления.

Агенты работают на основе данных, собранных цифровым двойником, и могут самостоятельно адаптироваться к изменяющимся условиям. Например, при обнаружении подозрительной активности агенты могут инициировать симуляцию атаки для проверки, является ли это реальной угрозой, и предложить меры по предотвращению атаки.

Для оценки эффективности предложенной системы было проведено имитационное моделирование нескольких сценариев атак (DDoS, SQL-инъекции, распространение вредоносного ПО). Результаты показали, что использование MAS в сочетании с цифровым двойником позволяет значительно снизить время обнаружения угроз и повысить точность предсказания атак. Система показала высокую адаптивность к новым типам угроз благодаря способности агентов быстро обмениваться данными и изменять стратегии защиты.

Перспективы дальнейшего развития данной технологии включают внедрение методов глубокого обучения для автоматического улучшения поведения агентов и усиление координации между агентами для еще более точного прогнозирования и нейтрализации сложных киберугроз.

Список литературы

1. Rybina, G.V., Stepankov, V.Y. (2023). Features of the Use of Multiagent Technology in the Management of Urban Parking Space. In: Kovalev, S., Kotenko, I., Sukhanov, A. (eds) Proceedings of the Seventh International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’23). IITI 2023. Lecture Notes in Networks and Systems, vol 776. Springer, Cham. https://doi.org/10.1007/978-3-031-43789-2_34

2. Путято, М.М., Макарян, А.С., Черкасов, А.Н., and Кучер, В.А., 2024. Разработка имитационной модели в области защиты информации с использованием программного обеспечения AnyLogic. Bulletin of Adyghe State University. Series: Natural-Mathematical and Technical Sciences, (1), p. 336.

УДК 004.056

Н.В. ЛИНЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ВЕБ-ИЗОЛЯЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СЕТЕЙ ОТ ИНТЕРНЕТ-УГРОЗ

В работе проведено обоснование использования технологии веб-изоляции для повышения эффективности сетевой безопасности на объектах. Дана характеристика технологии по решению ряда задач, связанных с защищенностью информации на объектах. Приведен ряд решений российского и иностранного производства, рассмотренных по цене и функционалу.

Введение

При наличии необходимости использования сети Интернет в различных организациях и распространения в этой сети ценной информации, одним из основных видов деятельности является сетевая безопасность. Злоумышленники используют данный канал для попытки получения несанкционированного доступа к информации. Из этого следует, что количество инцидентов, а также их разновидности в сети Интернет с каждым годом стремительно растут [1]. Для защиты от подобного рода угроз и повышения защищенности информации в организациях внедряют технологии веб-изоляции.

Постановка задачи

Задачей технологии веб-изоляции является повышение уровня защищенности за счет исключения возможности получения вредоносной информации по сети Интернет на стороне пользователя. Достигается это путем предотвращения прямого контакта интернет-трафика с системой пользователя. Данная специфика отличает это средство защиты информации от других и решает вопрос обеспечения производительности системы.

Так как на сегодняшний день человеческий фактор остается основным источником формирования инцидентов информационной безопасности, данная технология должна решать следующие задачи [2]:

Обеспечение большей безопасности. В случае возникновения инцидента информационной безопасности локальный компьютер пользователя должен оставаться в безопасности, но локальные системы

организации могут быть скомпрометированы. В этом случае требуется наличие стороннего веб-облака.

Упрощение IT-контроля. IT-специалистам может быть проще внедрить политики безопасности и настроить изоляцию браузера.

Повышение производительности. Система должна обеспечивать максимальную защищенность при минимизации нагрузки на неё и на всю систему.

Пути решения задачи

Обозначенные выше задачи решаются внедрением технологии веб-изоляции. Российские компании на данный момент не так активно разрабатывают продукт данного класса. Один из примеров российской разработки – DIY-веб-изоляция «IronBRO» (Isolated Remote BROwser).

После анализа технологий веб-изоляции иностранного производства, были определены следующие решения, отобранные на основе стоимости и по их функционалу:

– Cigloo Browser Isolation Management.

– Citrix Secure Browser.

– Ericom Remote Browser Isolation.

Заключение

Технологии веб-изоляции играют ключевую роль в формировании защищенности информации в организации, ввиду повышения производительности информационной системы и увеличения уровня эффективности безопасности информации в организации. Стоит острый вопрос в создании отечественных продуктов данного класса, один из которых «IronBRO».

Список литературы

1. Максим О. Таныгин, Юлия А. Будникова, Андрей С. Булгаков, Михаил А. Марченко. Модель оценки ущерба от инцидентов информационной безопасности. Безопасность информационных технологий = IT Security, Т. 28, № 2, 2021. С. 98–106. DOI: http://dx.doi.org/10.26583/bit.2021.2.09.

2. Ремесник Е.С., Муратов Д.И. Роль человеческого фактора в обеспечении информационной безопасности ИТ-инфраструктуры. Применение SIEM-систем: XIX Международная научно-практическая конференция «Теория и практика экономики и предпринимательства», 2022. С. 258–259.

УДК 004.056

Н. АЛДАБЕРГЕНОВ[1], А.С. ВОРОБЬЕВ[1]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

УЯЗВИМОСТИ ТИПА МЕЖСАЙТОВЫЙ СКРИПТИНГ В SWAGGER UI:

В работе рассматривается проблема уязвимости DOM XSS в Swagger UI, которая возникает из-за недостаточной фильтрации данных и устаревшей версии библиотеки DomPurify. Задача исследования — найти способы эксплуатации уязвимости, способной привести к захвату учетных записей. Для её решения проведён анализ инструментов и предложены методы защиты, включая обновление Swagger UI и библиотек. В результате экспериментов было реализовано ПО для поиска данных уязвимостей в интернете или охраняемой инфрастуктуры..

Введение

Swagger UI — это популярный инструмент для визуализации и взаимодействия с API, который широко используется разработчиками для тестирования и демонстрации API-интерфейсов (ссылка на survey любой). Однако, как и любое программное обеспечение, оно подвержено уязвимостям, которые могут представлять угрозу безопасности. Одной из таких уязвимостей является DOM XSS (Cross-Site Scripting), позволяющая злоумышленникам внедрять вредоносные скрипты через параметры запросов. Данная статья посвящена исследованию данной уязвимости, её потенциальным последствиям и способам предотвращения таких атак для обеспечения безопасности API-интерфейсов. Дополнительно было реализовано ПО для автоматического поиска данного типа уязвимостей в защитном контуре охраняемых объектов или в сети интернет.

Постановка задачи

Перед нами были поставлены следующие задачи. Провести анализ уязвимости и проверить ее с представленной в банках CVE:

1. Воспроизвести уязвимость в тестовом окружении с целью выявления особенностей исполнения и возможных расширениях вектора атаки.
2. Разработать ПО для автоматического поиска уязвимости в сети Интернет.
3. Проверить надежность в глобальной сети Интернет.

Данные шаги смогут обосновать важность проведения мероприятий по защите от данных видов уязвимостей.

Основная часть

В рамках анализа уязвимости были проанализированы действительные веб-сайты. Во избежание эксплуатации и потенциальных последствий компрометации, для выявления уязвимости был составлен список признаков: названия узлов, GET параметров и версий ПО Swagger. Поиск осуществлялся с помощью общедоступных инструментов типа Shodan, Google и т.д.

Уязвимость позволяет выполнять несанкционированный клиентский код злоумышленника в рамках сессии пользователя, что, в зависимости от существа веб-приложения, может как минимум привести к подмене контента, взаимодействия с веб-приложением от лица жертвы, а как максимум привести к захвату аккаунта жертвы.

Для оценки уязвимости мы использовали базовые метрики CVSS v3.1 и соответствующий вектор по оценке уровня опасности уязвимости. Калькулятор балла, обозначающего уровень опасности, доступен по ссылке https://www.first.org/cvss/calculator/3.1.

Реализованная ПО для поиска уязвимостей в инфраструктуре или в сети интернет расположено на интернет-ресурсе GitHub и реализовано на ЯП Python. Данный ЯП был использован с целью оптимизации затрат времени на реализацию ПО, а также за понятный синтаксис и хорошую поддержку со стороны других разработчиков ПО.

Заключение

Исследование показало тривиальность эксплуатации и простоту нахождения уязвимости с помощью автоматизированных инструментов на основе информации из открытых источников. Совокупность этих особенностей уязвимости демонстрируют её актуальность среди злоумышленников. Однако, разработанное решение и используемые признаки могут также быть использованы специалистами по информационной безопасности для выявления уязвимостей на веб-приложениях вендоров.

Список литературы

1. Марков А.С. Важная веха в безопасности открытого программного обеспечения. Вопросы кибербезопасности. 2023, № 1(53), с. 2–12. DOI: http://dx.doi.org/10.21681/2311-3456-2023-1-2-12.

2. Милославская Н.Г., Толстой А.И. Управление информационной безопасностью. М.: НИЯУ МИФИ, 2020. – 536 с.

3. Когос К.Г., Финошин М.А. Перспективные подходы к обнаружению сетевых скрытых каналов. Безопасность информационных технологий, [S.l.], т. 28, № 2, с. 45–61, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.2.05. – EDN: QESDBW

КИБ-2024
КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Информационная безопасность социотехнических систем

Руководители секции:

ДВОРЯНКИН С.В. – д.т.н., начальник НОЦ «БИКС»

ВАНИЧКИНА А.С. – к.филол.н., и.о. директора ИИН МГЛУ

УДК 347

В.А. МИНАЕВ

Московский университет МВД России им. В.Я. Кикотя

КИБЕРБЕЗОПАСНОСТЬ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ В СОВРЕМЕННОМ МИРЕ

Рассмотрены базовые направления и основные принципы формирования единого киберсообщества, особенности технологического «очищения» киберпространства от деструктивного контента. Сформулированы подходы России по системному созданию безопасного киберпространства.

Руководствуясь концепцией своего развития, Россия формирует архитектонику Интернет-державы, пересаживаясь на трех цивилизационных коней: стимулирование цифровой экономики, формирование чистой и надежной онлайн-среды, обеспечение безопасности киберпространства [1].

Страна повышает охват широкополосным доступом в Интернет все свои регионы, включая территории с низкой плотностью населения. Россия готова сотрудничать с другими странами при создании безопасного и устойчивого киберпространства. В этой связи Президент Российской Федерации В.В. Путин неоднократно призывал мировое сообщество к сотрудничеству в сфере Интернета и цифровой экономики. Создается «цифровая» Россия, нацеленная на глубокое слияние Интернета, технологий Big Data, искусственного интеллекта и реального сектора экономики. Перспективы реализации таких планов – это начало развития территорий, поселений и отдельных индивидов, по сути дела, с нового «нуля», означающего, что на современном этапе ни один человек в стране уже не сможет обходиться в своей жизнедеятельности без сетевого пространства, которое предстоит строить совместно. По отдельности – не получится, поскольку масштабы, которые несет новая техническая революция, превышает все аналоги прошлого.

Характерно на этот счет мнение руководителя компании «Лаборатория Касперского» [2], который сказал, что человечество живёт в очень опасном мире, и оно сегодня уязвимо, как никогда. Если в 1997 г., по его словам, существовало полтысячи вредоносных программ и вирусов, то сейчас их насчитывается более 20 млн. Появился даже новый тренд – многослойность и многоуровневость в разработке и реализации вредоносных программ.

Информационные войны, фейковая информация как их отражение, все более увеличивают свою масштабность на фоне разрастающихся конфликтов в разных регионах мира. Нестабильность обостряет глобальные проблемы, усиливает турбулентность в международных отношениях. Во многом это обострение и усиление связано с попытками кибергегемонизма в информационной сфере, информационного деструктивного воздействия на население, масштабных краж данных в цифровой сфере. Все это требует повышения эффективности управления киберпространством на основе сетецентрических технологий.

Базовые направления формирования единого киберсообщества:

• *активное содействие цифровой индустриализации и цифровой трансформации общества,* связанные с созданием глобальной информационной инфраструктуры, включая обеспечение всех регионов доступными Интернет-услугами;

• *развитие сообщества безопасности киберпространства* на основе соблюдения нейтрального характера информационных технологий, своевременного обмена данными о киберугрозах, трансграничной координации по противодействию кибертерроризму;

• *построение коллективной кибероответственности*, позволяющей органам власти, силовым структурам, Интернет-компаниям, бизнес-сообществам, общественным-организациям способствовать созданию норм управления киберпространством страны;

• *достижение общих киберинтересов государства, регионов и социальных групп.* Это означает создание киберпространства, в котором на первом месте стоит человек с его цифровыми интересами и Интернет-культурой.

Рассмотрим **четыре основных принципа**, которым необходимо следовать при создании единого киберпространства:

• *соблюдение цифрового суверенитета,* постулирующего право государств выбирать собственные пути развития Сети и модели равного участия в международном управлении киберпространством;

• *сохранение стабильности и безопасности киберпространства* как фактора предотвращения в нем криминальных действий и агрессии, экстремизма и терроризма, незаконного оборота наркотиков;

• *содействие открытости и сотрудничеству* как предпосылок проведения транспарентной политики в киберпространстве, создания платформ эффективного сотрудничества в нем, координации инноваций;

• *поддержание киберпорядка*, выражающегося в руководящей роли нравственного воспитания и достижений человеческой цивилизации.

Очищение цифрового контента

Российское общество следит, чтобы в Интернете обеспечивалась безопасность, выступающая многомерным объектом, которому присущи:

• *позитивная энергия в Интернете*, где растет масса позитивного и здорового контента, передовые культурные элементы;

• *разнообразие цифровой культуры*, представленной онлайн-видео и аудио, литературой, музыкой, электронными библиотеками, музеями в «облачных» хранилищах, онлайн-театры, выставки и концерты;

• *передовые средства онлайн-коммуникации и обработки данных*, включающие методы искусственного интеллекта, технологии больших данных, облачные вычисления, виртуальную и дополненную реальность;

• *киберэкосистемные представления об Интернете*, направленные на обеспечение чистой и здоровой киберсреды, очищаемой от противоправного и аморального контента;

• *продвижение Интернет-цивилизации*, включающего создание здорового сообщества в Сети, формирование праведной Интернет-культуры;

• *развитие работы онлайн-платформ*, содействующих качественному социально-экономическому развитию и устремлениям людей к лучшим образцам жизни. С целью укрепления рубежей своего киберпространства в России создается фундаментальная правовая основа, включающая, в первую очередь, законодательство о кибербезопасности, безопасности данных и защите персональных данных.

В частности, в стране разработана нормативная база о безопасности и защите критической информационной инфраструктуры (КИИ), усилена работа в области оценки рисков, надзора и раннего предупреждения чрезвычайных ситуаций.

Огромное влияние на комплексное обеспечение безопасности киберпространства России оказывает обучение в десятках ее учебных заведений кибербезопасности как основной дисциплине. Поощряются инновационные структуры в области кибербезопасности, создаются национальные парки и пилотные зоны кибербезопасности.

Заключение и выводы

Чтобы в целом охарактеризовать подход Российской Федерации к системному созданию единого киберпространств, кратко охарактеризуем ее усилия в этой сфере, выделив, десять направлений.

1. *Цифровой суверенитет*, смысл которого состоит в праве каждой страны самостоятельно выбирать свой путь цифрового развития, модель и государственную политику управления Сетью при равных его возможностях.

2. *Поддержание безопасности и стабильности*, содержание которых состоит в интеграции интересов всех стран и устранении ситуаций, когда безопасность одних обеспечивается за счет других.

3. *Создание недискриминационной цифровой среды*, означающей устранение политизации технологических процессов, поддержание безопасных и стабильных цепочек поставок ИТ-продуктов и услуг, а также разработку международных правил управления цифровыми технологиями.

4. *Укрепление защиты КИИ* как основы нормального функционирования экономики и общества путем взаимного раннего предупреждения о чрезвычайных ситуациях в информационной сфере.

5. *Безопасность и стабильность системы управления ресурсами Интернета*, гарантирующих их доступность и надежность.

6. *Противодействие киберпреступности и кибертерроризму* как глобальному бедствию [3, 4].

7. *Безопасность, развитие и использование данных* как основы цифровых, Интернет- и смарт-технологий [5].

8. *Справедливая и рациональная система управления киберпространством*, направленного на достижение сбалансированного отражения интересов всех стран-участников.

9. *Создание Интернет-цивилизации* как ключевого объекта в системе прогрессивного развития человечества.

10. *Совместное построение и развитие инфраструктуры Интернета* для цифрового разрыва между странами и различными социальными группами населения, усиление цифровой помощи его уязвимым слоям.

Список литературы

1. Минаев В.А., Поликарпов Е.С. Китайский взгляд на развитие и безопасность киберпространства // Информация и безопасность. 2023. Т. 26. Вып. 4. – С. 535–542.

2. Касперский заявил о появлении 90 млн новых вирусов за год. URL: https://www.rbc.ru/technology_and_media/ 03/12/2017/5a2405079a7947213b28 a893 (дата обращения: 21.07. 2024).

3. Минаев В.А., Поликарпов Е.С., Симонов А.В. Методы снижения шумовых факторов при выявлении контента экстремистского характера в социальных медиа // Информация и безопасность. 2022. Т. 25. Вып. 2. – С. 179–186.

4. Минаев В.А., Симонов А.В. Сравнение моделей-трансформеров BERT при выявлении деструктивного контента в социальных медиа // Информация и безопасность. 2022. Т. 25. Вып. 3. – С. 341–348.

5. Минаев В.А. Поликарпов Е.С., Еременко В.Т., Рытов М.Ю. Управление информационной безопасностью: Учебное пособие. М.: МосУ МВД России им. В.Я. Кикотя, 2022. – 310 с.

УДК 004.056

В.Г. ГРИБУНИН

АНО «Институт инженерной физики», Серпухов

АНОМАЛИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. КЛАССИФИКАЦИЯ И СОВРЕМЕННЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ

В докладе показана роль обнаружения аномалий в информационной безопасности. Представлены подходы к классификации аномалий и их обнаружению.

Понятие «аномалии» является трудно определимым формально, хотя и интуитивно понятным. Словарь дает толкование: «аномалия - отклонение от нормы, от общей закономерности». Для изучения того, что же является нормой в той или иной области и обнаружения отклонения от нее могут применяться различные статистические методы, а также машинное обучение – с учителем и без учителя, поверхностное и глубокое. В последние годы для обнаружения аномалий предложено использовать большие языковые модели (БЯМ) [1].

Обнаружение аномалий имеет решающее значение в области информационной безопасности. Приведем лишь некоторые примеры аномалий:

аномалии поведения пользователей информационных систем, характеризующие злоумышленников;

аномалии поведения программных процессов, характеризующие вредоносное программное обеспечение;

аномалии сетевого трафика, характеризующие компьютерные атаки;

аномалии шифрованного материала, характеризующие слабость или неверное применение алгоритмов шифрования;

аномалии мультимедийной информации, характеризующие наличие стеганографических вложений;

аномалии датасета, характеризующие его отравление;

аномалии поведения нейронов в глубокой сети, характеризующие отравление модели и т.д., и т.п.

Для каждой упомянутой подобласти информационной безопасности можно разработать свои классификационные признаки и классификацию аномалий. Например, для сетевого трафика такими признаками могут быть источник, причина и область возникновения, способ проявления, характер изменений трафика и т.п. [2].

Предложим наиболее общую, непривязанную к конкретным приложениям, классификацию аномалий.

1) В зависимости от условий проявления аномалии могут быть контекстуальными и бесконтекстными. Например, температура +20° является нормальной в летний период и аномальной – в зимний (для умеренного климата).

2) В зависимости от характера проявления аномалии могут быть точечными или быть представленными некоторым рядом, кривой. Например, аномалией может быть, как единичный выброс значения, так и тренд или же некоторая область значений.

3) В зависимости от порядка обработки аномалии после ее обнаружения можно выделить: собственно, аномалию, выброс и новизну. Выброс необходимо удалить, так как это мешающий решению задачи «шум». Аномалию можно в дальнейшем исследовать отдельно. Новизну можно включить позднее в обновленный датасет, в том числе, как отдельный класс.

4) В зависимости от типа можно рассматривать сенсорные и семантические аномалии. При сенсорной аномалии предполагается, что образцы «нормальности» исходят из одного и того же ковариантного распределения. При этом необходим выбор методики определения характеристик распределения примеров и порога, позволяющего относить примеры к нормальному и аномальному классу. При семантической аномалии считается, что образцы «нормальности» происходят из одного и того же семантического распределения (категории), т.е. нормальности должны принадлежать только одному классу.

Таким образом, при сенсорной аномалии образцы «нормальности» поступают из распределения P(X), тогда как аномалии – из распределения $P`(X) \neq P(X)$. Семантического сдвига нет, то есть, $P`(Y) = P(Y)$ (класс один и тот же). Для семантической аномалии, напротив, $P`(Y) \neq P(Y)$. Конечно, здесь также и $P`(X) \neq P(X)$.

В работе [1] показано, что БЯМ может обнаруживать аномальные области, содержащие всего 2% данных, с точностью 96,7%.

Список литературы

1. Jason Lopatecki. A Novel Approach for Anomaly Detection Using Large Language Models / URL: https://arize.com/blog-course/anomaly-detection-using-large-language-models/

2. Артамонов В.А. Обнаружение сетевых аномалий через реконструкцию сетевого трафика // Известия Южного федерального университета. Технические науки. – 2007. – № 1. – Т. 76. – С. 127–130.

УДК 004.056

А.В. КУЗНЕЦОВ

Финансовый университет при Правительстве Российской Федерации, Москва

КОНВЕЙЕР ДАННЫХ ДЛЯ АВТОМАТИЧЕСКОЙ ЛОКАЛИЗАЦИИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

Исследование направлено на сокращение времени локализации компьютерных инцидентов, возникающих в территориально распределенных информационных инфраструктурах. По результатам исследования определены шаги по обработке данных, в т. ч. данных о событиях безопасности, которые в отличии от известных учитывают состав необходимых атрибутов данных и необходимость альтернативной проверки результатов выполнения технического действия по локализации компьютерного инцидента.

Введение

Субъекты критической информационной инфраструктуры, операторы, организующие и/или осуществляющие обработку персональных данных, должны осуществлять реагирование на возникающие компьютерные инциденты. В рамках реагирования одной их первоочередных задач является локализация обнаруженного компьютерного инцидента в информационной инфраструктуре субъекта (оператора). Принимая во внимание, что время активного проникновения составляет минуты [1], время локализации должно так же измеряться в минутах – десятках минут.

Но в территориально распределенных инфраструктурах, где часть специалистов, вовлекаемых в процесс реагирования, может находиться в других часовых поясах (быть временно недоступной) или обладать недостаточной квалификацией, реагирование требует гораздо большего времени. Таким образом, сокращение времени локализации компьютерных инцидентов путем автоматизации, базирующейся на обработке данных (data driven approach), является актуальной задачей [2].

Постановка задачи

Определить состав атрибутов данных и последовательность шагов по их обработке, в т. ч. данных о событиях безопасности, для автоматической локализации компьютерных инцидентов.

Конвейер данных

На практике уже есть отдельные примеры автоматизации процедур реагирования [3], но они не учитывают состав необходимых атрибутов данных и необходимость альтернативной проверки результатов

выполнения технического действия.

Предлагаемая последовательность шагов для обработки данных, в т. ч. данных о событиях безопасности (data pipeline), с указанием необходимых атрибутов данных, включает в себя:

1. Получение данных о подозрении на инцидент (атрибуты: дата и время обнаружения, источник, цель, категория инцидента).
2. Нормализация формата полученных данных и формирование карточки компьютерного инцидента (дополнительные атрибуты: ответственный за устранение, приоритет инцидента, статус инцидента).
3. Подтверждение инцидента (обновление значения для атрибута: статус инцидента; дополнительный атрибут: комментарий).
4. Подтверждение необходимости локализации инцидента (обновление значений для атрибутов: статус инцидента, комментарий).
5. Выбор технического действия по локализации инцидента (дополнительные атрибуты: статус покрытия средством(ами) защиты информации источника и/или цели, реквизиты доступа к средству(ам), мандат на действие по локализации).
6. Выполнение технического действия по локализации (дополнительный атрибут: запрос (команда) к средству защиты информации; обновление значения для атрибута: статус инцидента).
7. Проверка результатов выполнения технического действия по локализации альтернативным способом согласно п. 5–6 (обновление значения для атрибута: статус инцидента).

Заключение

По результатам исследования предложен конвейер данных, позволяющий проводить автоматическую локализацию обнаруживаемых компьютерных инцидентов, который в отличии от известных учитывает состав необходимых атрибутов данных и необходимость альтернативной проверки результатов выполнения технического действия по локализации.

Список литературы

1. Беспалова Н.В., Корчагин С.А., Сердечный Д.В., Селиверстов В.В. Анализ зарубежного опыта применения интеллектуальных методов в задачах защиты объектов критической информационной инфраструктуры финансового сектора. Инженерный вестник Дона. 2024, № 5 (113), с. 76–91.

2. Шананин В.А. Применение систем искусственного интеллекта в защите информации. Инновации и инвестиции. 2022, № 11, с. 201-205.

3. Yu Nong, Haoran Yang. Automated Software Vulnerability Patching using Large Language Models. August, 2024. URL: https://arxiv.org/html/2408.13597v1 (Дата обращения 30.09.2024) DOI:10.48550/arXiv.2408.13597.

УДК 004.056

А.М. КУЧИНА, Е.Н. КЛОЧКОВА

Московский университет МВД России им. В.Я. Кикотя

ОПАСНОСТЬ РАСПРОСТРАНЕНИЯ ФЕЙКОВЫХ НОВОСТЕЙ

Фейковые новости представляют собой угрозу в информационной среде, потому применение способов выявления ложной информации является актуальной задачей в нынешнее время. В статье рассматриваются возможные грозы на сферы общественной жизни человека. Анализ этих возможных последствий, наносимых фейковыми новостями, позволяет наметить основные подходы к выявлению и борьбе с ложными сведениями.

В настоящий момент люди получают немыслимое количество информации в день и, закономерно, среди всего этого пласта данных появляются лживые новости.

Обретая очередные сведения и неоднократно сталкиваясь с опровержением недавно прочитанных, подрывается доверие не только к источнику ошибочной информации, но и ко всей получаемой в целом.

Фейковые новости – неправдивые и неподтвержденные данные о предметах, субъектах или ситуации, создающие искаженное представление о действительности.

Существует ряд угроз, которые могут являться следствием распространения фейковых новостей.

1. Подрыв доверия к СМИ. Основным источником новостей являются средства массовой информации, которые предоставляют проверенные известные им данные, однако бывают и те, что не утруждают себя проверкой транслируемого ими. Действия последних вызывают сомнительное представление о источниках информации в целом.

2. Угроза терроризма. Распространение недостоверной или лживой информации о несуществующих угрозах терроризма может стать последствием немалых волнений не только среди граждан, но и правоохранительных органов. Последние, усилив охрану общественного порядка на той территории, в которой была ложная угроза терроризма, могут упустить действительную угрозу.

3. Угроза политической обстановки. Доверие своим лидерам и их решениям являются основой силы всей страны, однако при подрыве

доверия к ним, могут начаться общественные волнения вплоть до государственного переворота.

4. Информационная настороженность. Нередко получая ложные сведения, люди начинают к ним относиться скептически, вследствие чего могут упустить важную информацию, считав ее ложной.

5. Угроза экономической ситуации. При получении неверной информации об экономической обстановке, люди могут принять то решение, которое бы никогда не приняли, зная правдивую ситуацию.

6. Угроза здоровью. Зачастую, люди, сталкивающиеся с вопросами здоровья, обращаются за помощью в сеть «Интернет», однако получают противоречивую, а иногда и деструктивную информацию, которая при применении может навредить здоровью.

Вышеперечисленные угрозы в совокупности представляют опасность во всех сферах жизни общества, потому приоритет в их разрешении имеет особую важность.

Во избежание последствий возникновения угроз, необходимо проверять достоверность информации, анализировать источники, проверять факты и опираться на ведомственные сайты.

Подведя итоги вышесказанного, появляется понимание угроз, которые могут наступить в последствии распространения фейковых новостей. Необходимо быть бдительным, получая информацию из непроверенных ресурсов, сверять ее с достоверными источниками на ведомственных сайтах. Также, важно не только проверять данные, но и размышлять самому, задумываться об их правдивости.

Список литературы

1. Защитные решения кибербезопасности для дома и бизнеса / Лаборатория Касперского / Kaspersky DOI: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-identify-fake-news, 2022.

2. Максименков М. И. Фейковые новости: актуализация проблемы в РОССИИ / Коммуникология: электронный научный журнал, 2020, № 5. С. 56–67.

3. Третьяков А.О., Филатова О.Г., Жук Д.В., Горлушкина Н.Н., Пучковская А.А. Метод определения русскоязычных фейковых новостей с использованием элементов искусственного интеллекта / International Journal of Open Information Technologies., 2018, № 6. С. 99–105.

4. Курбанов Т.К., Качаева Г.И., Малаев А.Х., Качаев З.К., Саадуев О.С. Угрозы распространения и методы ограничения фейковых новостей / Образование и право, 2022, № 6, С. 16–19.

УДК 004.056

В.М. ШИКАЛОВА, Е.А. ПОЛЯНСКАЯ

Московский университет МВД России им. В.Я. Кикотя

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГРАЖДАН: РОЛЬ ГОСУДАРСТВА И ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Данная статья рассматривает роль государства и правоохранительных органов в обеспечении информационной безопасности граждан в контексте современных вызовов и угроз в киберпространстве, анализирует перспективы дальнейшего развития механизмов защиты информации, включая развитие законодательства, применение новых технологий и обучение граждан.

Информационная безопасность имеет огромное значение для человека в цифровом мире. Одним из главных ее аспектов является обеспечение защиты личных данных от несанкционированного доступа, что может привести к финансовым потерям или нанести ущерб репутации человека. Также важным аспектом информационной безопасности выступает противодействие киберпреступлениям, обеспечивающее стабильность и безопасность информационной инфраструктуры общества в целом.

Государство играет важную роль в обеспечении информационной безопасности граждан путем разработки и реализации законодательства о защите персональных данных, создания и поддержки инфраструктуры для безопасности информационных систем и организации обучения и осведомления граждан о методах защиты информации. Эти меры помогают обеспечить сохранность личных данных, защитить информационные системы и повысить осведомленность граждан о безопасном использовании информации.

Правоохранительные органы в свою очередь занимаются выявлением и пресечением деятельности хакеров, мошенников и шпионов, включающим в себя сбор доказательств, проведение оперативных мероприятий и сотрудничество с другими правоохранительными органами и специалистами в области информационной безопасности. Активно взаимодействуют с государственными службами безопасности, специализированными информационными службами, что позволяет более эффективно бороться с угрозами информационной безопасности и разрабатывать новые методы защиты.

Обеспечение информационной безопасности граждан включает в себя использование следующих механизмов и инструментов:

A. Развитие методов обнаружения и предотвращения киберугроз.

B. Создание системы мониторинга и обнаружения инцидентов информационной безопасности.

C. Усиление защиты персональных данных и критической информационной инфраструктуры.

Однако быстрое развитие технологий создает новые угрозы и вызовы для обеспечения информационной безопасности. Киберпреступники постоянно совершенствуют техники и методы, используемые для атак на информационные системы, что создает сложности для выявления и пресечения новых угроз, требует постоянного мониторинга и обновления систем безопасности.

Таким образом, можно рассмотреть перспективы дальнейшего развития и совершенствования роли государства и правоохранительных органов в обеспечении информационной безопасности граждан. Постоянное развитие законодательства в данной области позволит адаптировать правовые нормы к появлению новых технологий и угроз. Важной перспективой является улучшение сотрудничества между организациями и странами, что позволит обмениваться информацией о киберугрозах, координировать действия по предотвращению и реагированию на инциденты информационной безопасности, и разрабатывать совместные стратегии по защите граждан. Также важной перспективой является проведение программ обучения и осведомления граждан о методах защиты информации и безопасном поведении в киберпространстве.

Каждая из этих перспектив играет важную роль в укреплении системы информационной безопасности и защите интересов граждан в контексте модернизации технологий и появления новых киберугроз, а их реализация может обеспечить более эффективную защиту информации и повысить безопасность граждан в цифровой среде.

Список литературы

1. Развитие понятия «Информационная безопасность» в научно-правовом поле России URL: https://cyberleninka.ru/article/n/razvitie-ponyatiya-informatsionnaya-bezopasnost-v-nauchno-pravovom-pole-rossii (дата обращения 10.09.2024).

2. Доктрина информационной безопасности Российской Федерации URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 10.09.2024).

УДК 004.056

В.М. ШИКАЛОВА, Е.А. ПОЛЯНСКАЯ

Московский университет МВД России им. В.Я. Кикотя

МЕТОДЫ И ПОДХОДЫ ОПТИМИЗАЦИИ РАБОЧЕГО ПРОЦЕССА ПРИ АНАЛИЗЕ УЯЗВИМОСТЕЙ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ

Аннотация: данная статья рассматривает методы и подходы для оптимизации рабочих процессов, анализируя их в контексте современных вызовов и угроз в киберпространстве.

Социотехнические системы являются подходом к проектированию рабочих процессов взаимодействия человека и технико-технических продуктов. Для уменьшения количества уязвимостей данной системы требуется комплексный подход, который учитывает, как технические аспекты, так и социальные.

Анализ уязвимостей в социотехнических системах – многогранный процесс. Методы анализа могут затрагивать не только традиционные способы обнаружения и борьбы с угрозами, но и более сложные подходы, учитывающие моделирование поведения пользователей.

В качестве основных методов и подходов можно выделить:

1 Комплексный анализ, включающий в себя метод HAZOP (Hazard and Operability Study), а иначе говоря системный подход, дающий возможность изучить производственное оборудование; метод FTA (Fault Tree Analysis), представляющий собой анализ дерева неисправностей - метод обнаружения и анализа факторов, которые способствуют возникновению исследуемого нежелательного события (конечного события); метод ETA (Event Tree Analysis), являющийся графическим методом представления взаимоисключающих последовательностей событий, следующих за появлением исходного события, в соответствии с функционированием и нефункционированием систем, разработанных для смягчения последствий опасного события.

2. Анализ человеческого фактора в виде SWAT (Social, Technological, Organisational, and Physical) – анализа, охватывающего социальные, технологические, организационные и физические аспекты системы; HRA (Human Reliability Analysis) – метода, применяющегося для оценки влияния действий человека, в том числе ошибок оператора, на работу системы; HFMEA (Human Factors Failure Mode and Effects Analysis) –

анализа, фокусирующегося на поиске потенциальных ошибок человека и их последствий; TEG (Task Error Grid) – графического метода, который даёт возможность оценить вероятность ошибки человека и выполнения определённой задачи.

3. Анализ социальных факторов, состоящий из STPA (System Theoretic Process Analysis) – анализа, который фокусируется на выявлении потенциальных рисков, которые связаны с взаимодействием человека и системы; Socio-Technical Risk Assessment – анализа, который учитывает социальные факторы, такие как организационная структура, мотивация персонала, коммуникационные процессы; Ethnographic Research – метода, выявляющего риски и позволяющего изучить культуру и поведение пользователей.

4. Инструменты для анализа, куда входят: программное обеспечение, используемое для моделирования систем (например, Simulink или Arena); инструменты, предназначенные для анализа рисков - RiskVision, BowTie, а также инструменты для анализа данных – SPSS и инструменты для проведения исследований – Qualtrics, SurveyMonkey.

Выбор отдельных методов и подходов зависят от характера социотехнических систем, целей анализа и доступных ресурсов. Важно использовать комплексный подход, а результаты анализа применять для разработки мер по предотвращению уязвимостей и повышения безопасности системы. Также стоит внедрить механизм обратной связи, позволяющий быстро реагировать на новые угрозы и корректировать методы анализа.

Список литературы

1. Белов А.В. Введение в социотехнические системы: анализ и управление. – М.: Наука, 2020.

2. Васильев П.А. Методы оценки безопасности социотехнических систем. – СПб.: Питер, 2019.

УДК 004.056

Е.Н. БАХАНОВА, Е.П. ПОЛЯНСКАЯ

Московский университет МВД России им. В.Я. Кикотя

НЕКОТОРЫЕ АСПЕКТЫ ОРГАНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЕ ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

В статье рассматривается процесс организации защиты данных в информационной системе органов внутренних дел Российской Федерации. Анализируются аспекты комплексной защиты информации, а также методы и средства, используемые для построения функционального информационного ресурса по обработке данных.

Для достижения беспрепятственного, эффективного функционирования органов внутренних дел Российской Федерации используется информационно-аналитическая система обеспечения деятельности ОВД, которая была создана на базе интегрированной мультисервисной телекоммуникационной сети.

ИСОД, как и любая другая информационная среда, нуждается в организации системы защиты данных. Для системы разработана многоуровневая защита, которая включает в себя набор современных методов и средств по реализации мер и принципов обеспечения информационной безопасности. Но не стоит забывать, что вопрос соблюдения требований информационной безопасности при работе с информационными системами всегда остается зависим и от человеческого фактора [1, с. 249].

Наиболее эффективным подходом в организации защиты сведений является системный подход, который содержит в себе оптимальное сочетание различных средств для создания многофункционального механизма защиты данных. Рассмотрим основные методы и элементы реализации комплексной защиты информации.

Для качественной защиты сведений в ИСОД используется принцип *разграничения и управления доступом*, который позволяет установить правила идентификации и аутентификации пользователей строго в рамках делегированных прав доступа [2, с. 34–36].

Аутентификация подразумевает под собой процесс сверки введенных в форму данных с данными сотрудников, согласно специально созданным спискам. Путем управления привилегиями пользователя создается дополнительный аспект обеспечения безопасности информационной системы, так как недостаток или избыток полномочий способствует нарушению нормального функционирования ресурса. А с помощью механизма реагирования выполняется функция защиты от несанкционированного доступа путем использования различных средств блокирования нормального взаимодействия системы с пользователем.

Физические средства защиты позволяют ограничить круг лиц, имеющих возможность беспрепятственного использования ИСОД. Это достигается в связи с использованием системы контроля и управления доступом (СКУД) на этапе входа в режимное помещение.

С помощью *программно-аппаратных средств* защиты выполняются функции идентификации пользователей, шифрования информации, воспрепятствования несанкционированной работе системы, аудита событий безопасности, которые в большинстве случаев используются для предотвращения внешних угроз безопасности путем установления антивирусной и антиспамовой системы защиты. Антивирусная защита является одним из элементов системы безопасности, целью которой выступает недопущение воздействия вредоносного программного обеспечения на информационную систему. Для нормального функционирования ИСОД наиболее эффективно использование многовендорного варианта защиты. Это позволяет всесторонне охватить попытки внешних угроз и повысить уровень обнаружения и обезвреживания вредоносных программ [3, с. 79–83].

Средствами *организационной защиты* служат регламентация деятельности подразделения с помощью разработки и утверждения должностных инструкций, управление работой личного состава, требование соблюдения должностных полномочий, предоставление возможностей для переподготовки и повышения квалификации в условиях информатизации общества.

Список литературы

1. Гафнер В.В. Информационная безопасность: учебное пособие. Ростов-на-Дону – 2020. – 249 с.

2. Кемпф В.А. Обеспечение информационной безопасности в ОВД: учебное пособие. – Барнаул: Барнаульский юридический институт МВД России – 2022. С. 34–36.

3. Григорьев А.Н., Мускатиньев А.Ю., Иванов П.Ю. Организация антивирусной защиты автоматизированных информационных систем органов внутренних дел: учебное пособие. – Калининград: Калининградский филиал СПбУ МВД России, 2023. С. 79–83.

УДК 004.056

А.С. ЭРДНИЕВ

Московский университет МВД России им. В.Я. Кикотя

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СОЦИОТЕХНИЧЕСКОЙ СИСТЕМЫ ОВД

Цель данной работы – обоснование потребности в системном подходе к обеспечению безопасности социотехнической системы органов внутренних дел (ОВД). По итогам исследования формулируются общие векторы обеспечения безопасности.

Значительный объем научных исследований посвящен участию органов внутренних дел в вопросах обеспечения информационной защищенности граждан Российской Федерации. Существуют как организационно-правовые [1], так и технические [2] подходы к информационной безопасности ОВД. Однако, большинство исследований детализирует сущность участия ОВД в реализации Стратегии национальной безопасности, но не раскрывает сущностное наполнение социотехнической системы ОВД, а вместе с ней и проблемы обеспечения собственной безопасности рассматриваемой системы.

Сущность и система организации собственной безопасности определена приказом МВД России от 2 января 2013 года № 1 [3], в котором формулируются, как характеристики внешних и внутренних угроз, так и направления по обеспечению безопасности.

Регулятор предусмотрел ряд отдельных направлений по обеспечению защищенности технологических ресурсов и информационных систем, но в контексте обеспечения защиты сведений, составляющих государственную тайну. Правовые нормы не предусматривают потенциальную возможность информационного воздействия на личный состав с точки зрения внедрения деструктивных сущностей в профессиональное мировоззрение квалифицированного специалиста.

Выделяя такой аспект, как низкую социальную защищенность сотрудника органов внутренних дел, нормативное регулирование не рассматривает способы и механизмы защиты личного состава в контексте не профессиональной, а социальной реальности. Вместе с тем, социальная коммуникация профессионального сообщества не может быть искусственно отделена от остальных форм коммуникации. При этом следует учитывать и общедоступные технологические достижения, которые так или иначе выступают основой для функционирования

технических систем правоохранительных органов. Связь информационной безопасности с противодействием информационно-психологическому воздействию в отношении сотрудников полиции [4] не в полной мере отражает проблематику. В качестве ориентирующей рамки по-прежнему выступают коррупционные риски и формирование облика сотрудника в медиапространстве.

Однако, допустимо более детально проанализировать динамику нарушений служебной дисциплины, а также причины оттока кадров, выделив на основании полученной информации модель угроз информационного воздействия на сотрудников. Результаты анализа позволят определить не только явные технологии воздействия, но и отдельные латентные механизмы и инструментарии. Систематизация используемых технологий на примерах обеспечит возможность для проработки форм и методов противодействия деструктивным намерениям.

Таким образом эффективная организация обеспечения информационной безопасности органов внутренних дел должна включать: представления о системе технологий, используемых для деструктивного воздействия на социальную среду ОВД; структуру и содержание технологического контента, используемого для воздействия; модель социально-технологического воздействия; инструментарий противодействия деструктивным влияниям. Системный подход к обеспечению безопасности социотехнической системы органов внутренних дел, должен включать не только техническую составляющую, но и немаловажный социальный аспект.

Список литературы

1. Баторов Б.О. Некоторые проблемы нормативно-правового регулирования защиты информации в органах внутренних дел Российской Федерации и пути их разрешения / Б.О. Баторов // Труды Академии управления МВД России. – 2022. – № 2(62). – С. 121–127. – DOI 10.24412/2072-9391-2022-262-121-127. – EDN EOCSJV.

2. Богданова К.Н. Использование искусственного интеллекта для оптимизации процессов обеспечения информационной безопасности в автоматизированных системах / К.Н. Богданова // Охрана, безопасность, связь. – 2024. – № 9-2. – С. 83–89. – EDN VKQVQL.

3. Приказ МВД России от 2 января 2013 г. № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»

4. Курдюкова В. Ю. Информационная безопасность сотрудников органов внутренних дел и защита от информационно-психологического воздействия / В.Ю. Курдюкова // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований: Материалы всероссийской научно-практической конференции, Санкт-Петербург, 17 декабря 2021 г. / Санкт-Петербургский университет МВД России. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2022. – С. 127–133. – EDN JDBBLD.

УДК 004.89

В.А. МИНАЕВ[1], К.М. БОНДАРЬ[2], В.С. ДУНИН[2]

[1]*Московский университет МВД России им. В.Я. Кикотя*

[2]*Дальневосточный юридический институт МВД России им. И.Ф. Шилова, Хабаровск*

ОРГАНИЗАЦИЯ РАДИОСВЯЗИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ НА БАЗЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

Рассмотрены концептуальные и технологические особенности разработки и внедрения систем машинного обучения (МО) в радиосвязи органов внутренних дел (ОВД). Предлагается расширение функционала радиосвязи на основе самоорганизации сети в условиях адаптации к помеховым воздействиям и противодействию со стороны противника.

Постановка задачи

Современные условия управления ОВД связаны с тем, что физическая передача командных указаний и исполнительских сообщений сопряжена с развитием новых проблем. В частности, организация радиосвязи ОВД сопряжена с необходимостью учета противодействия (со стороны криминальных элементов, в том числе - экстремистов, противника в условиях боестолкновений).

Совокупность новых явлений и значимость возникающих сегодня киберпроблем, способных в целом ряде случаев даже прерывать существующие управленческие циклы в ОВД, требуют развития концепции системы цифровой радиосвязи [1], которая позволит создать защищенную сеть на основе современных информационных технологий, обеспечивающую предоставление необходимого комплекса услуг связи и передачи данных подразделениям ОВД Российской Федерации. Они должны быть расширены путем самоорганизации сети радиосвязи в условиях адаптации к помеховым воздействия и противодействию со стороны противника [2]. Такой способ может быть реализован с помощью технологических преобразований передатчиков и приемников средств радиосвязи на базе псевдослучайной перестройкой рабочей частоты (ППРЧ). Данный способ требует, как минимум, повышения помехоустойчивости передачи данных в системах радиосвязи [3]. Решением может стать все более активное внедрение технологий МО [4].

Построение радиосвязи на основе МО потенциально способствует практическому совершенствованию следующих направлений:

1. *Автоматизация и совершенствование оперативной связи* по ряду характеристик (маршрутизация вызовов, анализ и фильтрация информации, работы с базами данных).

2. *Выявление, анализ и прогнозирование преступлений*. МО может быть использовано при обработке и анализе данных о преступлениях, включая сведения из радиосетей. Применение алгоритмов машинного обучения и нейронных технологий помогает выявлять закономерности и предсказывать криминальные события на основе анализа больших данных.

3. *Улучшение безопасности и обеспечение связности*. Включение в функционал мониторинга и анализа состояния сетей связи алгоритмов МО способно обеспечить эффективное обнаружение возможных угроз, сбоев связи, а также поддержать ее безопасность, быстрое восстановление при сбоях.

4. *Управление ресурсами радиосети*, направленное на оптимизацию частотного спектра и пропускной способности. Алгоритмы МО могут адаптироваться к изменяющимся условиям и динамически распределять ресурсы для обеспечения надежной связи и минимизации перегрузок сети.

Заключение и выводы

Основные концептуальные и технологические особенности, рассматриваемые авторами, требуется учитывать при разработке и внедрении методов МО в радиосетях ОВД. Следуя Концепции [1], изучение конкретных сценариев внедрения МО раскрывает дополнительные проблемы развития радиосвязи ОВД (инновационные меры безопасности, надежности, гибкости), а также пути и способы их преодоления.

Список литературы

1. Об утверждении Концепции развития цифровой радиосвязи органов внутренних дел Российской Федерации до 2024 года: Приказ МВД России от 28 ноября 2019 г. № 892 // СТРАС «Юрист».

2. Липатников В.А., Петренко М.И. Модель самоорганизующейся сети радиосвязи, функционирующей в сложной сигнально-помеховой обстановке // Труды учебных заведений связи. 2023. Т. 9. № 2. С. 72–80.

3. Филатов В.И., Сухов А.В., Зайцев М.А., Генов А.А. Комплексная оценка показателей помехоустойчивости современных и перспективных систем передачи информации и связи. Журнал радиоэлектроники [электронный журнал]. 2020. № 9. https://doi.org/10.30898/1684-1719.2020.9.13.

4. Артемов М.Л. Применение технологий искусственного интеллекта в автоматизированных системах управления и радиосвязи // Теория и техника радиосвязи. 2021. № 4. С. 5–17.

УДК 004.056

А.И. ВАСИЛЬЯНОВ[1], Б.С. ЛЕЩИНСКИЙ[2]

[1]*Донецкий государственный университет*

[2]*Донской государственный технический университет*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ: ТЕХНОЛОГИИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

В эпоху цифровизации и развития технологий социотехнические системы (СТС) становятся все более сложными и взаимосвязанными. Эти системы включают в себя как технические компоненты, так и человеческие факторы. Обеспечение информационной безопасности таких систем является критически важной задачей, так как атаки могут затрагивать как технологические, так и социальные аспекты. В статье рассматриваются ключевые вызовы информационной безопасности СТС, предлагаются пути решения этих задач и обсуждаются новые подходы и результаты экспериментов в данной области.

Социотехнические системы охватывают широкий спектр применения: от систем управления на предприятиях до глобальных сетей взаимодействия в государственном управлении и критической инфраструктуре. Одним из ключевых аспектов функционирования СТС является информационная безопасность, которая обеспечивает сохранность и конфиденциальность данных, а также защиту от несанкционированного доступа и сбоев [1].

Основные угрозы безопасности социотехнических систем можно разделить на две категории: технические угрозы, социальные угрозы.

Таким образом, главная задача – разработать комплексный подход к обеспечению безопасности, который учитывал, как технические, так и человеческие аспекты функционирования СТС.

Рассмотрим основные проблемы с информационной безопасностью:

Угрозы кибератак: проникновение в системы через уязвимости программного обеспечения или сетевой инфраструктуры.

Человеческий фактор: ошибки пользователей, неосознанное раскрытие конфиденциальной информации, использование слабых паролей.

Социальная инженерия: злоумышленники используют психологические манипуляции для получения доступа к закрытым системам.

Для эффективного решения задач информационной безопасности социотехнических систем необходим комплексный подход, который охватывает технические, организационные и социальные меры [2].

В последние годы в области обеспечения безопасности социотехнических систем были предложены и исследованы несколько новых подходов. Одним из них является использование искусственного интеллекта (ИИ) и машинного обучения для анализа больших объемов данных и обнаружения аномалий в поведении систем и пользователей.

ИИ позволяет автоматизировать процессы анализа данных, что значительно повышает эффективность обнаружения угроз. Например, системы на основе машинного обучения способны анализировать сетевой трафик в реальном времени, выявлять аномалии и прогнозировать возможные атаки на основе предыдущих инцидентов.

Большое внимание следует уделять изучению поведения пользователей в СТС, чтобы лучше понять, какие действия могут привести к угрозам безопасности. Эксперименты показали, что персонализированные тренинги по кибер-гигиене значительно уменьшают количество ошибок пользователей и снижают риск успешных атак через социальную инженерию.

Другой перспективной областью является использование симуляционных платформ для создания сценариев атак и их последующего анализа. Такие системы позволяют тестировать различные методы защиты и оценивать их эффективность.

Использование современных технологий, таких как искусственный интеллект и машинное обучение, открывает новые возможности для защиты социотехнических систем. Однако этот процесс должен сопровождаться тщательным анализом и интеграцией подходов к улучшению безопасности на всех уровнях [3].

Для улучшения информационной безопасности в социотехнических системах рекомендуем интеграцию технических и поведенческих мер, проведение обучения и повышения осведомленности сотрудников, а также внедрение новых технологий.

Список литературы

1. Герасимов Ю.В., Герасимова Н.В. Информационная безопасность: учебник для вузов. – М.: Юрайт, 2020. – 512 с.

2. Греков И.Н. Информационная безопасность и защита информации: учебное пособие. – М.: ИНФРА-М, 2021. – 360 с.

3. Кирьянов Д.В. Информационные технологии и информационная безопасность: учебное пособие. – СПб.: Питер, 2019. – 256 с.

УДК 004.056

А.Ж. НИЗАМОВ

Финансовый университет при Правительстве Российской Федерации, Москва

ИСПОЛЬЗОВАНИЕ НЕОДНОРОДНОСТИ СКОРОСТИ РАСПРОСТРАНЕНИЯ АКУСТИЧЕСКИХ ВОЛН ДЛЯ ЗАЩИТЫ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

В докладе рассматривается процесс поворота волнового фронта акустической волны за счет изменения скорости распространения акустических волн вблизи стен помещения для частот до 3 кГц, Исследование проводилось с целью показать перспективность применения метода для широкого диапазона частот сигнала. Приведены результаты расчета двумерной задачи в ограниченном пространстве, подтверждающие возможность развернуть акустическую волну до момента её воздействия на стену помещения.

Введение

В настоящее время используется множество средств защиты информации по акустическому каналу. Это свидетельствует о том, что, во-первых, в различных условиях возможно применение только некоторых из этих средств и, во-вторых, что ни одно из средств защиты акустической информации не решает полностью задачу защиты. В этих условиях целесообразно искать новые технические средства защиты акустической информации, расширяя возможности средств защиты [1].

Концептуальна модель

В процессе исследования решалась задача распространения акустической волны в двумерном приближении, моделируя распространение в помещении от точечного источника в условиях полного отражения волны от стен помещения. При этом, вблизи одной из стен скорость звука изменялась (возрастала) по различным законам (линейная зависимость и степенная).

В настоящее время разработано большое количество численно-аналитических методов и вычислительных алгоритмов для решения волновых задач.

Решение волнового уравнения строилось в лучевом приближении. Это позволило построить траектории лучей и увидеть, как они поворачиваются из области с увеличенной скоростью звука.

Задача исследования акустического зеркала, поворачивающего лучи за счет изменения скорости звука по направлению нормали к поверхности зеркала, сводится к решению волнового уравнения с растущей скоростью звука в слое некоторой толщины по одной из переменных.

Результаты моделирования показали, что при достаточно малом относительном изменении скорости звука (порядка 0,2 при наибольшем значении) возникает область тени, мало зависящая от частоты акустического сигнала в диапазоне частот от 100 Гц до 3 кГц. Таким образом, удалось погасить акустический сигнал практически полностью в наиболее значимой энергетической области речи, на которую приходиться максимум энергии.

Разворот фронта звуковой волны позволяет решить задачу защиты акустической информации при ведении переговоров, в том числе в финансовой сфере, когда в ходе устного общения может произойти утечка конфиденциальной информации по акустическому каналу.

Полученный результат требует экспериментального подтверждения, но он показывает возможность поворота волнового фронта акустического сигнала для предотвращения его измерения и записи по колебаниям с различных поверхностей.

Заключение

Проведенный расчет показал:

- достаточно тонкий слой воздуха с повышенной скоростью звука способен повернуть фронт акустической волны;
- изменение скорости акустической волны позволяет повернуть фронт волны акустического речевого сигнала в широком диапазоне частот.

Список литературы

1. Хорев А.А. Способы защиты выделенных помещений от утечки речевой (акустической) информации по техническим каналам: системы виброакустической защиты / А.А. Хорев // Специальная техника. – М.: 2013. – № 4. – С. 31–63.

2. Сагдеев К.М., Оленев А.А. Математическая модель акустического канала утечки речевой информации, научная статья, журнал Фундаментальные исследования, № 6 (часть 3), 2012. – С. 668–673 (URL: https://fundamental-research.ru/ru/article/view?id=30098).

УДК 001.2; 001.53; 004.056; 32.321; 340.01

А.П. ФИСУН[1], Ю.А. БЕЛЕВСКАЯ[2], Р.А. ФИСУН[3]

[1]*Орловский государственный университет им. И.С. Тургенева,*

[2]*Мезенский педагогический колледж, Орёл,*

[3]*Отделение по Смоленской области Главного управления ЦБ РФ по ЦФО*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЭВОЛЮЦИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Развитие теоретико-методологических основ информационной, правовой, технической, экономической, политической, других наук, как основного инструмента решения актуальных прикладных задач современного информационного общества (ИО) и его сфер (ИСф) в условиях глобального и непрерывного воздействия на ИО угроз, неразрывно связано с развитием теоретических и прикладных основ обеспечения информационной безопасности (ИБ) социотехнических систем (СТС) ИО.

В основе исследования эволюции ИО в условиях глобальных и непрерывных угроз ИБ ИО, ИБ СТС, лежит системный анализ, информационно-деятельностный комплексный подход исследования эволюции, ИО через содержание и формы политико-правовых, общественных отношений, являющихся «концентрированным выражением экономики», основанных на реализации информационных процессов во всех материально-энергетических и ИСф, направленных на удовлетворение определенных целей человека, общества, государства. Основными результатами решения искомой проблемы является системное представление взглядов, подходов, концепций и принципов формирования понятийного базиса, информационной, правовой, технической, экономической, политической, и других наук современного ИО, их центральных понятий: «информация», «ИО», «ИБ ИО», «ИБ СТС».

Уточнено, что ИО – это и общество, в котором все правовые, политические, экономические и другие общественные отношения во всех сферах и видах деятельность имеют информационный характер, определяются основным объектом этих отношений – информацией, удовлетворяющей требованиям безопасности, достоверности, своевременности и требующее регулярного и непрерывного обеспечения ИБ СТС.

Рассмотрение искомой проблемы развития ИО основано на исследовании известных подходов, концепций, взглядов и традиций, в том числе политико-правового анализа и методологии греко-римской философии, взглядов известных учёных [1–13] на содержание и

эволюцию ИО. Это позволило заключить: значительные, несопоставимые скорости создания и распространения информации в современном мире, влекут реальные последствия изменения общества и потенциальные угрозы, обусловленные несоответствием требований к её свойствам своевременности, достоверности, безопасности, полноты, релевантности, пертинентности и другим. Такие нарушения, оказывает разрушающее воздействие на человека, общество, государство, на развитие его политической, экономической и других сфер и видов деятельности, что подтверждает значимость качественной информации, как основного объекта, для эффективного развития всех сфер ИО и обеспечения ИБ.

Исходя из этого, были уточнены и сформулированы утверждения, гипотезы зарождения, существования и развития ИО на всех исторических этапах формирования социума, развития человечества, где его основной объект «информация», существует вне зависимости от нашего к ней отношения и не связано с конкретным историческим этапом развития человека, общества, государства. А основной шкалой оценки эффективности информации, являются её свойства (своевременность, достоверность, безопасность и другие), выступающие критериями оценки развития ИО, его СТС и обеспечения их ИБ.

Список литературы

1. Гоббс Т. Ливиафан. Т. 2. 97 с.
2. Соловьев Э.Г. Новая философская энциклопедия Институт философии Российской Академии Наук. URL: http://iph.ras.ru/elib/1265.html.
3. Бутенко Е.В. Эволюция теорий информационного общества: дис. канд. философ. наук: 09.00.11/ – Томск, 2004 – 130 с.
4. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере / Н.Н. Куняев. – М.: Логос, 2010. – С. 176–185.
5. Сляднева Н.А. Социально-информационные технологии как синергетический фактор социального управления// Социально-информационные технологии: проблема двойного назначения. Аналитико-прогностические исследования. Ч. 1. М.: МГУКИ, 2004. С. 13–34.
6. Смолян Г.Л. Некоторые ключевые понятия информатизации: категориальный статус и предметная область. // ИО. - № 1. – С.7–17.
7. Стратегия развития ИО в Российской Федерации [Электронный ресурс]: [Утверждена Президентом Российской Федерации 7 мая 2017 г. № Пр.-203.]. – URL: http://www.kremlin.ru/acts/bank/41919/
8. Караваев Н.Л. ИО: попытка осмысления сущности понятия. //НТИ. – 2014. - №6. – С. 1–6.
9. Фролова Е.А., Рыжкова М.В., Кашапова Э.Р. Социальное и экономическое благополучие современного информационного общества// ИО. – 2015. - № 5. – С. 3–7.
10. Баева Л.В. Исследовательские мегатренды в условиях ИО и проблемы социокультурной безопасности. //ИО. – 2015. - № 2–3. – С. 13–24
11. Ракитов А.И. Философия компьютерной революции. М.: Политиздат, 1991. – 91 с.
12. Ракитов А.И. Наш путь к информационному обществу // Теория и практика общественно-научной информации. М.: ИНИОН, 1989.
13. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М.: Издательский дом «Парад», 2005.

УДК 004.056

Л.О. МИШИНА, В.Н. ТАРАН

Крымский федеральный университет им. В.И. Вернадского,
Гуманитарно-педагогическая академия (филиал), Ялта

БУДУЩЕЕ КВАНТОВОЙ КРИПТОГРАФИИ: ВЫЗОВЫ И ВОЗМОЖНОСТИ

В статье предлагается новый вид защиты информации с помощью квантовой криптографии. Рассмотрено текущее состояние квантовой криптографии, сделана попытка выявить ключевые проблемы и предложить пути их решения, т.к. классические методы криптографии, основанные на алгоритмах математики, становятся уязвимыми к атакам квантовых компьютеров.

Введение

В современном мире возникает необходимость в надежных методах защиты и шифрования информации. Квантовая криптография предлагает новые подходы к обеспечению безопасности данных.

Цель исследования – рассмотреть текущее состояние квантовой криптографии, выявить ключевые проблемы и предложить пути решения.

Квантовая криптография – это метод защиты коммуникаций, основанный на принципах квантовой физики. Квантовые компьютеры способны решать определенные задачи намного быстрее, чем обычные машины. Однако, внедрение такого типа криптографии сталкивается с рядом вызовов, включая необходимость создания инфраструктуры, разработки новых протоколов и подготовки специалистов.

При использовании квантовой криптографии, процесс отправки и получения информации всегда осуществляется физическими средствами, например, с помощью электронов в электрическом токе или фотонов в волоконно-оптических линиях связи. Используя квантовые явления, можно спроектировать и воссоздать систему связи, которая всегда способна обнаружить прослушивание. Это обеспечивается тем фактом, что попытка измерить взаимосвязанные параметры в квантовой системе вносит в нее изменения, уничтожая исходные сигналы, а это означает, что законные пользователи могут распознавать степень активности перехватчика по уровню шума в канале.

Квантовые вычисления представляют серьезную угрозу для существующих методов криптографии. Например, алгоритм Шора может эффективно факторизовать большие числа, что дает возможность разрушить системы шифрования, основанные на сложности факторизации. Алгоритм Гровера, способен находить ключи существенно быстрее, чем классические алгоритмы, что делает симметричные шифры

менее надежными. В ответ на эти вызовы и угрозы, разрабатываются квантово-устойчивые методы шифрования и квантовая криптография.

К основным проблемам квантовой криптографии относятся:

– технические ограничения: сложность реализации и потери квантовых состояний, что влечет за собой потерю информации;

– инфраструктурные проблемы: отсутствие стандартов квантовой криптографии и высокая стоимость разработки и внедрения;

– проблема безопасности и уязвимости информации: существуют потенциальные риски за счет физических атак на устройства;

– проблема правовых и этических аспектов: недостаток правовых норм и стандартов для использования квантовой криптографии, конфиденциальность данных, использование и защита личных данных.

Рассматривая пути решения, для развития квантовой криптографии, можно предложить разработку новых протоколов, например, квантовая распределенная передача ключей и протоколы (BB84, E91), разработку стандартов для интеграции квантовых технологий с существующими системами связи, необходима подготовка специалистов, способных работать с новыми технологиями, а также научные исследования и эксперименты, для выявления новых методов и алгоритмов.

Заключение

Таким образом, квантовая криптография обладает значительным потенциалом для обеспечения безопасности данных, но при этом, необходима разработка новых стандартов и подготовка кадров в области квантовых технологий. Это обеспечит повышение качества и безопасности российских технологий, в том числе за счет разработки и использования российских стандартов, что имеет более системный и конкретный характер [3].

Список литературы

1. Авдонина М.В. Квантовые технологии на службе криптографии будущего / М.В. Авдонина // Научные исследования студентов и учащихся: сборник статей VII Международной научно-практической конференции, Пенза, 27 октября 2022 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 9–12. – EDN XQSRVS.

2. Базаев М.А. Квантовые вычисления и их будущее в компьютерной науке / М.А. Базаев, Л.К. Хаджиева, Д.Т. Борщигов // Молодежь, наука, инновации: Сборник статей XII Всероссийской научно-практической конференции, Грозный, 18 октября 2023 года. – Грозный: Грозненский государственный нефтяной технический университет им. М.Д. Миллионщикова, 2023. – С. 36–39. – DOI 10.26200/GSTOU.2023.88.17.005. – EDN ROZMJL.

3. Арустамян, С. С. Методические и реализационные аспекты внедрения процессов разработки безопасного программного обеспечения / С. С. Арустамян, В. В. Вареница, А. С. Марков // Безопасность информационных технологий. – 2023. – Т. 30, № 2. – С. 23–37. – DOI 10.26583/bit.2023.2.01. – EDN AXVLZO.

УДК 349:681

А.В. БЕЛЯКОВА
Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации», Москва

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ В ОБЛАСТИ КИБЕРНЕТИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стремительное развитие информационных технологий во всех областях и сферах жизнедеятельности приводит к тому, что правовое регулирование не успевает адаптироваться к новейшим технологиям. В настоящее время правовое регулирование в рассматриваемой сфере крайне разрозненно и фрагментарно, что приводит к необходимости переосмысления действующего законодательства. Предлагается проанализировать имеющиеся пробелы в данной области и сформулировать ряд предложений по дальнейшему развитию направления, с учетом междисциплинарного подхода.

Введение

Разобщенность правового регулирования, отсутствие единого логико-структурированного современного понятийного и категориального аппарата приводит не только к проблемам в реализации общественных отношений в рассматриваемой области, но и создает существенные проблемы в правоприменительной практике. Смысловая и терминологическая разобщенность в понятиях, используемых в юридической практике и применяемых техническими специалистами, приводит впоследствии к проблемам в реализации технических заданий, проектов, исполнении договорных обязательств.

Постановка проблемы

Сформировавшийся массив нормативно-правовых актов и локальных актов, содержащих нормы об исследуемой области, имеет фрагментарную регламентацию данного рода общественных отношений в большинстве кодифицированных источников права России.. При этом в науке и правовой доктрине уже многие годы идут обсуждения по вопросу о необходимости кодификации и систематизации правовых норм данной сферы[1]. Обсуждаются вопросы о «цифровом кодексе» [1–3],

[1] Например, актуальная дискуссия по данному вопросу развернулась на XII Петербургском международном юридическом форуме, подробнее см.: URL: https://legalforum.info/programme/business-programme/5371/.

«информационном кодексе» [2] и т.п. При этом единого мнения по данному аспекту среди правоведов до настоящего времени не сформировалось. Автор полагает, что это связано, в первую очередь, с тем, что отсутствует междисциплинарный подход к развитию данной отрасли. Обновление правовой составляющей данной области возможно с учетом синтеза знаний в области права, кибернетики и информационной безопасности. Было бы целесообразно для начала рассмотреть возможность создания обновленного словаря терминов изучаемой сферы, как одного из первых этапов формирования унифицированного понятийного аппарата, с привлечением специалистов, как в области юриспруденции, так и в информационных технологиях.

Заключение

Таким образом, можно выделить ряд проблем:

– отсутствие специалистов, обладающих междисциплинарными знаниями в области права и информационных технологий, кибернетики и информационной безопасности и, как следствие, проблемы формирования эффективной информационной инфраструктуры в России;

– отсутствие междисциплинарного взаимодействия при реализации проектов, технических заданий и т. п., что создает также ряд проблем в достижении поставленных целей, а впоследствии — в правоприменении;

– разобщенность правового регулирования, являющаяся следствием вышеизложенных пунктов;

– ускоренное развитие информационных технологий, которое приводит к тому, что базовое законодательство устаревает и требует обновления и конкретизации.

В связи с этим автор полагает, что необходимо разработать единую национальную концепцию развития кибернетики и информационной безопасности с учетом мнения не только правоведов, но и непосредственно технических специалистов.

Список литературы

1. Вайпан В.А. Источники цифрового права. Вестник арбитражной практики. 2024, № 1, с. 3–29.

2. Жарич А.В. Национальные и международные предпосылки создания Цифрового кодекса РФ. Цивилист. 2023, № 4, с. 5–9.

3. Рожкова М.А. Является ли цифровое право отраслью права и ожидать ли появления цифрового кодекса? Хозяйство и право. 2020, № 4 (519), с. 7.

УДК 004.056

Д.В. ЛЕМЕШКО

РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва

НЕКОТОРЫЕ ВОПРОСЫ, СВЯЗАННЫЕ С ПРИМЕНЕНИЕМ МАШИНОЧИТАЕМЫХ ДОВЕРЕННОСТЕЙ НА ПРАКТИКЕ

В работе рассмотрены вопросы перехода на использование усиленных квалифицированных электронных подписей физических лиц (УКЭП ФЛ) с предъявлением машиночитаемых доверенностей (МЧД). Рассмотрены возможные риски, связанные с МЧД. Проведена оценка актуальных рисков применения МЧД.

Введение

С 1 сентября 2023 года в Федеральный закон №63-ФЗ «Об электронной подписи» вступили в силу новеллы, связанные с внедрением электронных доверенностей – МЧД. К 1 сентября 2024 года государственные информационные системы (ГИС) ведомств должны были перейти на использование УКЭП ФЛ с предъявлением МЧД. Однако, некоторые ведомства оказались технически не готовы к данному переходу, и, как выяснилось, возникают некоторые проблемы и риски, связанные с МЧД и персональными данными (ПДн).

Практические проблемы использования МЧД

На текущий момент существует несколько практических проблем использования МЧД, а именно:

1. Не все информационные системы (ИС) смогли перейти на МЧД.
2. Отсутствует унифицированный формат МЧД.
3. Необходимость периодической сверки полномочий из классификатора полномочий, так как могут изменятся уникальные идентификационные номера полномочий.
4. Бывают проблемы в регистрации МЧД на узле оператора (ФНС России).
5. Если МЧД заполняется в свободной форме, то присутствует ограничение по количеству вводимых символов.

Актуальные риски МЧД и их оценка

Актуальными рисками являются:

1. Не совсем безопасное хранение МЧД.
2. Возможная утечка ПДн, которые указываются в XML-файле МЧД.

Для оценки рисков использовались F-N диаграммы. F-N диаграмма является частным случаем матрицы количественных последствий/вероятности. Частный случай количественной диаграммы вероятности и последствий, применяемый для рассмотрения допустимости риска [1]. В таблице 1 представлены вероятные опасные события (ВОС).

Таблица 1. ВОС

№ВОС	ВОС	Вероятность наступления ВОС	Частота, f	Количество событий
1.	Небезопасное хранение МЧД	Вероятное	10^{-4} … 10^{-3}	1 … 10000
2.	Утечка ПДн из МЧД	Частое	10^{-3} … 10^{-2}	1 … 10000

Согласно программной реализации, были получены результаты, показанные на рис. 1.

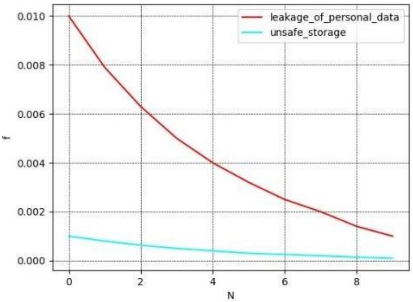


Рис. 1. F-N диаграмма

При большем количестве случаев в год вероятность возникновения ВОС, а именно: небезопасного хранения МЧД и утечки ПДн из МЧД, снижается.

По итогу, для снижения рисков потребуется разработать безопасное хранилище МЧД, а также усовершенствовать законодательство в области защиты ПДн и выстраивать грамотные защитные механизмы, чтобы исключить утечки ПДн.

Список литературы

1. ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска.

УДК 004.056

К.Ю. РЮМШИН[1], С.Ю. КАПИЦЫН[2]

[1]*Московский технический университет связи и информатики*

[2]*Санкт-Петербургский политехнический университет*

ВТОРЖЕНИЯ В СОЗНАНИЕ ЦЕЛЕВОГО ОБЪЕКТА ВОЗДЕЙСТВИЯ КАК ЭЛЕМЕНТ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

В статье представлен системный анализ подходов к представлению целостности семантики знаний информационной потребности целевого объекта воздействия и разработке логико-лингвистического метода формирования «бумажных» пуль на основе фразово-структурной грамматики.

Исходя из анализа и прогнозирования развития обстановки сформированной вокруг Российской Федерации, особенностей социального поведения целевого объекта воздействия (далее – ЦОВ) в кризисных ситуациях, их ИП с достаточной определенностью поддается структуризации. При этом в предлагаемом подходе на основе ЗСЦО, к целостности естественно-языкового описания семантических структур требуемой информационной потребности (далее – ИП), представленном на рис. 1, учитываются следующие закономерности:

−закономерности построения смысловых структур естественно-языкового текста (информационной потребности, «бумажных» пуль);

−закономерности построения объектов различной физической природы, в частности, описание требуемой ИП ЦОВ.

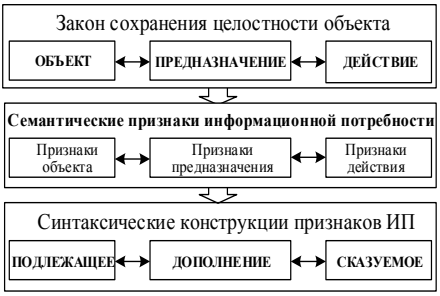


Рис.1. Схема подхода к представлению целостности естественно-языкового описания

В рамках выбранного подхода к целостности семантического описания ИП ЦОВ в виде лексических единиц и их синтактико-семантического взаимодействия, необходимо:

– сформировать словарь семантических признаков, определяющих ИП ЦОВ, т.е. представление смысла в виде устойчивой зависимости свойств (признаков) объекта от свойств (признаков) действия при фиксированном предназначении;

– сформировать словарь синтаксических конструкций признаков ИП, определяющих принадлежность семантических признаков к частям речи и предложения в текстовых структурах естественного языка.

Модель представления «бумажных» пуль краткими семантико-синтаксическими конструкциями в виде фразово-структурной грамматики базируется на формировании грамматических правил синтактико-семантическое взаимодействие признаков (идентификаторов) текстовых структур с элементами, играющих роль членов предложения или частей речи [1].

Логико-лингвистическая модель представления множества требуемых смысловых выводов целевого объекта воздействия базируется на формальной фразово-структурной грамматики аналогична текстовым структурам и представляет собой априорный словарь смысловых выводов, соответствующих конкретной ССК признаков смысловых выводов. Сформированный априорный словарь смысловых выводов в виде синтаксических конструкций, позволяет представить знания ЦОВ в структурированном виде, что фактически обеспечивает представление семантики входных текстовых структур естественного языка [1].

Контекстно-свободная грамматика информационной потребности ЦОВ задаётся фразово-структурной грамматикой, которая выступает в качестве адекватного средства представления ИП ЦОВ и начального этапа формализации семантики текстовых структур с заданными признаками.

Список литературы

1. Рюмшин К.Ю., Капицын С.Ю., Вареница В.В. Логико-лингвистический механизм формирования «бумажных» пуль при информационном противоборстве. Вопросы кибербезопасности. 2023, № 1, с. 93–99.

УДК 004.056

К.Ю. РЮМШИН[1], С.Ю. КАПИЦЫН[2]

[1]*Московский технический университет связи и информатики*

[2]*Санкт-Петербургский политехнический университет*

РЕАЛИЗАЦИИ НАУЧНЫХ ПОЛОЖЕНИЙ МЕТОДОЛОГИИ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ ВОЙНЫ

Базовым требованием к решению задач информационной войны целесообразно считать – получение условия существования процесса подготовки и ведения информационной войны с требуемым уровнем эффективности боевого применения (далее – ЭБП) специальных информационных формирований (далее – СИФ), т.е. получение условия «ПОБЕДЫ», в интересах обеспечения реализации гарантированного военно-политического превосходства (в частности, стратегического сдерживания).

1. Требование к разработке информационного оружия.

Использовать естественнонаучный подход для разработки системы оружия на основе структурно-функционального синтеза (далее – ЗСЦО). Зная ЗСЦО получаем условия существования процесса ведения действий СИФ с заданным показателем ЭБП. Исходя из военно-политической обстановки (далее – ВПО), поставленных руководством задач, мы формируем адекватные характеристики информационного оружия для оснащения СИФ.

2. Требование к адекватной интерпретации ведения действий СИФ.

При ведении действий, специальные информационные формирования в первом приближении работают с четырьмя процессами [1]:

2.1 Процесс целевой деятельности – вторжение в сознание способом подмены информационной потребности для формирования у противника (целевого объекта воздействия) требуемой модели социального поведения – модели социального поведения «побеждённого»;

2.2 Процесс проявления опасности (угрозы), характеризуется λ – величиной, обратной среднему времени проявления;

2.3 Процесс идентификации опасности (угрозы), характеризуется ν_1 – величиной, обратной среднему времени идентификации;

2.4 Процесс нейтрализации опасности (угрозы) – разрушение у ЦОВ целевой деятельности, характеризуется ν_2 – величиной, обратной среднему времени нейтрализации.

3. Требования к подготовке специалистов для решения задач информационной войны в условиях гибридных действий противника.

Для адекватного военно-политической обстановки решения, военному руководству (лицу принимающему решение) всех звеньев управления целесообразно руководствоваться тремя базовыми принципами, представленными в структурной схеме формирования модели решения на рис. 1.

3.1 Принцип трехкомпонентности познания (для формирования пространственного мышления).

3.2 Принцип целостности. Базируется на ЗСЦО и позволяет описать физический смысл процессов решения задач информационной войны [1].

3.3 Принцип познания. Основу принципа составляют методы: декомпозиции, абстрагирования, агрегирования. Что является фундаментальной составляющей для *интеллектуального развития профильных специалистов*.

Рис. 1. Структурная схема формирования модели решения

К базовым дисциплинам обучения целесообразно отнести:

1. Методология подготовки и ведения информационной войны.
2. Методы и модели действий СИФ в интересах обеспечения превосходства (стратегического сдерживания).
3. Технологии решения задач информационной войны.

Список литературы

1. Рюмшин К.Ю., Капицын С.Ю., Вареница В.В. Логико-лингвистический механизм формирования «бумажных» пуль при информационном противоборстве. Вопросы кибербезопасности. 2023, № 1, с. 93–99.

УДК 004.056

В.Б. ПРАХОВ

Московский государственный лингвистический университет

ИССЛЕДОВАНИЕ ВЛИЯНИЯ АКУСТИЧЕСКИХ ПОМЕХ НА ЗАЩИЩЕННОСТЬ РЕЧЕВОЙ ИНФОРМАЦИИ

Рассматривается возможность создания речеподобной помехи для средств виброакустической защиты речевой информации. Обосновывается выбор помехи типа «речевой хор», на основании проведения артикуляционных испытаний. Обсуждается направление дальнейших исследований по повышению эффективности алгоритмов формирования речеподобных помех.

Известно, что информация, получаемая в момент её озвучивания или демонстрации, является самой оперативной, ёмкой и готовой к немедленному использованию злоумышленником. Вот почему интерес злоумышленников обращен к непосредственному прослушиванию речи в том числе с помощью специальных технических средств [1].

Для защиты речевой информации от утечки по техническим каналам широко применяются активные средства защиты – генераторы акустического и виброакустического шума. Такие генераторы построены в основном с использованием в качестве задающего белого шума с нормальным законом распределения вероятности значений. Естественно, что встает вопрос о выборе такой помехи, которая при обеспечении требуемого показателя защищенности (в общем случае – это коэффициент словесной разборчивости речи W) дает минимальное значение интегрального уровня помехи, то есть вносит минимальные дискомфорт и демаскирующие признаки при проведении переговоров. Так, доказано, что для шумовых помех такими являются формантоподобные, то есть помехи, имеющие огибающую спектра, подобную спектру формант [1].

В качестве активных средств защиты речи от утечки по техническим каналам используются генераторы на основе белого, розового шума и речеподобной помехи. Однако ряд исследователей смогли «вычистить», например, белый шум из конечного аудиосигнала, что ставит вопрос о дополнительной оценке эффективности разного рода помех.

Для оценки эффективности каждой помехи были проведены их генерация, внедрение в исходный аудиосигнал, а также расчет словесной разборчивости речи W путем проведения артикуляционных испытаний в

соответствии с ГОСТ 16600-72 «Требования к разборчивости речи и методы артикуляционных измерений».

После проведения соответствующих испытаний [3] удалось установить следующее:

1) При использовании помехи типа белый шум при отношениях сигнал/шум 0дБ, 5дБ, 10 дБ уровень разборчивости речи *W* соответствует 9,6%, 18%, 41,8%;

2) При использовании помехи типа розовый шум при отношениях сигнал/шум 0дБ, 5дБ, 10 дБ уровень разборчивости речи *W* соответствует 2,6%, 11,7%, 26,5%;

3) При использовании помехи типа «речевой хор» при отношениях сигнал/шум 0дБ, 5дБ, 10 дБ уровень разборчивости речи *W* соответствует 0,2%, 10,4%, 20,6%.

Практический опыт показывает, что составление подробной справки о содержании перехваченного разговора невозможно при словесной разборчивости менее 70–80%, а краткой справки аннотации – при словесной разборчивости менее 40–60% [4].

Таким образом, по анализу полученных данных речеподобная помеха при одинаковых соотношениях сигнал/шум снижает разборчивость речи эффективнее других видов помех, а значит ее можно использовать в качестве средства активной защиты речевого сигнала.

В качестве направления для дальнейшего исследования можно рассмотреть обоснование выбора помехи, а именно: речевой хор, метод скремблирования и т.д.

Список литературы

1. Дворянкин С.В., Дворянкин Н.С., Устинов Р.А. Речеподобная помеха, стойкая к шумоочистке, как результат скремблрованя защищаемой речи – Вопросы кибербезопасности 2022, № 5 (51). С. 14–27.

2. Авдеев В.Б., Трушин В.А., Кунгуров М.А. Унифицированная речеподобная помеха для средств активной защиты речевой информации, Тр. СПИИРАН, 2020, выпуск 19, том 5. С. 991–1017 DOI: 10.15622/ia.2020.19.5.4

3. ГОСТ 16600-72 Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений

4. Хорев А.А., Оценка эффективности защиты речевой информации от утечки по техническим каналам Телекоммуникационные устройства и системы. 2015. Т. 5. № 4. С. 449–453.

УДК 004.056

Р.Т. БАТИСТА

Московский государственный лингвистический университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗЛОНАМЕРЕННОЕ ИСПОЛЬЗОВАНИЕ ИИ

Цель данной работы - представить подход к проблеме информационной безопасности и использования искусственного интеллекта с социокультурной точки зрения. Полученные результаты указывают на то, что поведение человека и конфиденциальность данных в большей степени зависят от культуры по сравнению с другими психологическими, демографическими и технологическими переменными. Кроме того, выявлен риск дестабилизации политических систем в результате целенаправленных кибератак, а также роль культуры информационной безопасности в противодействии этим угрозам.

Культуры определяют технологическое развитие, а технологии проникают в жизнь людей, влияя на их культуру и образ жизни. Однако восприятие и понимание информационной безопасности и ИИ, скорее всего, будет сильно зависеть от местных культурных и социальных условий. Критическая роль культуры в цифровой трансформации позволяет понять, как информационная безопасность и технологии, основанные на ИИ, используются в качестве геополитического оружия, направленного на культуру, чтобы повлиять на политическую стабильность в регионе [1].

Культурные данные питают ИИ, то есть алгоритмы обучаются на культурных выражениях с содержанием, связанным с изображениями, музыкой, текстами и видео. Однако те же возможности для развития производительности, персонализации продуктов или контента, создания квалифицированных рабочих мест, становятся такими же целенаправленными кибератаками на основе ИИ [2].

Развитие генеративного ИИ, глубокого машинного обучения, сетей IoT подталкивает информационное общество к новой когнитивной эре цивилизации. Поэтому вызовы информационной безопасности также связаны с тем, что эти технологии взаимодействуют с когнитивными представлениями людей и предоставляют любому человеку, группе, организации или национальному государству возможность влиять на общественное сознание в качестве нового вида оружия в мировой системе. Эволюция данных подтверждает, что конфликты остаются культурными, а значит, и ответные меры должны быть культурными.

Данные как ценность: Интернет, социальные сети и Большие Данные создали новые бизнес-модели, основанные на поведенческих данных. Корпорации берут под контроль своих пользователей.

Данные как оружие атаки: Кибератаки и киберпреступления направлены против отдельных лиц, организаций и правительств с помощью гибридных методов ведения войны. Конфликты переносятся в сознание.

Данные как культурная гегемония: Масштабная электронная слежка и автоматизированная пропагандистская техника с помощью кибератак на основе ИИ представляют собой метод символического насилия, позволяющий эмоционально манипулировать общественным мнением, формировать поведение людей и навязывать им видение, которое является общепринятым, доминирующим, действительным и универсальным.

Таблица 1. Основные тактики ЗИИИ и информационной безопасности

Данные как ценность	Данные как оружие атаки	Данные как культурная гегемония
Автоматизация рекламы и практики социальной инженерии	Автоматизация хакинга	Манипулирование информацией
	Фейковые новости с технологией DeepFake	Автоматизированные операции влияния с использованием методов прокси-войны
Пользователи-роботы или поддельные люди	Автоматические акции по дезинформации	

Такие тактики уже были опробованы в различных регионах Европы и Латинской Америки в рамках стратегий гибридной войны. Интересно, что инциденты в странах-членах БРИКС совпали в течение последних трех лет. Также недавно, в конце сентября 2024 г., Израиль осуществил гибридную кибер-атаку против «Хезболлы» в Ливане с помощью дистанционного и радио-взрыва пейджеров и раций.

Защита от этих угроз носит не только кибернетический, правовой, политический, но и культурный характер. Культура информационной безопасности позволяет не только сочетать технические средства контроля и человеческие риски в организациях, но и интерпретировать реальность в соответствии с ценностями и убеждениями, национальной идентичностью, поэтому реагировать в оборонительном ключе, повышая восприятие риска.

Список литературы

1. Базаркина Д.Ю., Пашенцев Е.Н. 2021. Стратегическая коммуникация БРИКС: Настоящее и будущее. Россия в глобальных делах, 19(3), с. 64–93. doi: 10.31278/1810-6374-2021-19-3-64-93.

2. Ваничкина А.С. Концептуальная парадигма дискурса информационной безопасности. Германистика 2021: Nove et Nova, с. 209–213, Московский государственный лингвистический университет, 2021.

УДК 004.056

Р.Т. БАТИСТА

Московский государственный лингвистический университет

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ ЧЕЛОВЕЧЕСКОЙ НАДЕЖНОСТИ

В последнее время предпринимаются попытки разработать измерения когнитивных способностей, которые можно было бы применить к более широкому спектру систем обработки информации, связанных с информационной безопасностью. Цель доклада - представить подход к проблеме информационной безопасности на основе анализа векторов атак. Анализ отражает не только угрозы и уязвимости информационных систем, но и то, как человеческая надежность может стать эффективной стратегией защиты стоимости активов организации, а следовательно, и цифрового суверенитета.

Развитие цифровых технологий приводит к изменениям в способах распространения информации, а для обработки естественного языка в последнее время используются глубокое обучение и нейронные сети. Поэтому автономные системы предоставляют новые векторы для кибератак, более точную и эффективную обработку, основанную на человеческих эмоциях [1].

Интернет поведения (Internet of Behaviors, IoB) заставляет переосмыслить стратегическую автономию, основанную на информационной безопасности. Цифровые технологии все еще, но не только, являются важнейшей способностью для обеспечения конкурентоспособности, защиты ценностей общества и, более того, суверенитета. Однако стратегическая автономия и суверенитет - это не одно и то же. Скорее, стратегическая автономия - это средство реализации суверенитета [2].

Глобальный ландшафт угроз в период с 2023 по 2024 год показывает, что фишинговые атаки остаются наиболее распространенной кибератакой и ответственны за 90% утечек данных. Интересно, что социальная сеть LinkedIn была связана с 52% фишинговых атак по всему миру. В то же время 92% вредоносных программ распространяются через электронную почту. Криптоджекинг и вредоносное ПО для IoT значительно выросли по мере развития сети взаимосвязанных устройств. Киберпреступность наносит огромный экономический ущерб организациям и создала рынок объемом 2 триллиона долларов. Полученные данные, несомненно, отражают, что большинство векторов атак направлены на компрометацию

пользователей, что также влияет на организации. Киберпреступность стала инструментом социального контроля, позволяющим осуществлять власть, контролируя информационные активы.

Таким образом, культура информационной безопасности является стратегическим фактором устойчивости организаций, а ее влияние способствует предотвращению инцидентов безопасности. Однако культура безопасности должна быть направлена на обеспечение баланса между социально-психологическими и человеческими потребностями и целями организации посредством управления человеческой надежностью. Речь идет не только об оценке человеческих неудач, ошибок, причиненного ущерба, последующем исправлении и обучении людей, но и о предвидении пробелов, которые позволяют людям терпеть неудачи.

Модели организационного управления обычно учитывают три основные подсистемы: техническую или подсистему задач, управленческую или административную подсистему и социальную подсистему. Анализ векторов атак показывает, почему социальная подсистема подвергается более легкому взлому. Многие организации разрабатывают стратегию информационной безопасности, ориентированную на технические и административные аспекты. Организационная культура, коллективные нормы и ценности, уровень мотивации, личные потребности могут оказаться несовместимыми с возможностями системы по реагированию и, следовательно, привести к сбоям. В отличие от этого, человеческая надежность - это превентивная стратегия, которая приносит ценность активам организации, стратегической автономии и суверенитету.

Основные аспекты, рекомендуемые для повышения надежности человека в культуре информационной безопасности: организация, ориентированная на процессы и риски, организация и разделение труда, иерархия и контроль на рабочем месте, график работы, размер компании, зарплата, рабочие группы, обучение по компетенциям, горизонты личного развития, уровни коммуникации, технологические условия труда, рабочая среда, рабочие процедуры, мотивация, продвижение по службе.

Список литературы

1. Ваничкина А.С. Концептуальная парадигма дискурса информационной безопасности. Германистика 2021: Nove et Nova, с. 209–213, Московский государственный лингвистический университет, 2021.

2. Пашенцев Е.Н. The Palgrave Handbook of Malicious Use of AI and Psychological Security. Palgrave McMillan, Springer Nature. с. 47–80, 2023 https://doi.org/10.1007/978-3-031-22552-9.

УДК 004.056, 008

П.Г. БЫЛЕВСКИЙ

Московский государственный лингвистический университет

АКТУАЛЬНОСТЬ ОБЩЕГРАЖДАНСКОЙ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В условиях разрушения однополярного глобализма, выработки новых форматов многополярного равноправного международного сотрудничества реализуются всё новые риски трансграничного характера интернет-коммуникаций в отношении российских граждан, превращённых цифровой трансформацией в пользователей компьютерно-сетевых технологий и объекты генерации данных. Расширение информационной безопасности от специализированных профессиональных компетенций до общегражданской культуры является актуальной задачей, направленной на достижение и обеспечение полноценного цифрового технологического и социально-культурного суверенитета.

«Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации», утверждённая распоряжением Правительством России 22 декабря 2022 года, подтверждает актуальность расширения прежде узкой профессии до развёрнутой общегражданской культуры, включающей профессиональное, специализированное и массовое направления. В современных условиях формирование и развитие такой общегражданской культуры является необходимым фактором достижения и обеспечения цифрового технологического и социально-культурного суверенитета [1].

История формирования общегражданской культуры информационной безопасности, занявшая около тридцати лет (с 1990-х годов), характеризовалась быстрыми скачкообразными переменами, появлением новых технологий, решений, массовых сервисов и радикальными социально-культурными переменами. Компьютерно-сетевые технологии из узкопрофессиональной сферы распространились на всё отрасли и профессии, напрямую или косвенно охватив важнейшие области повседневной жизни всего человечества. Цифровые сервисы и интернет-коммуникации стали влиятельнейшим организационно-техническим фактором личной жизни, национального развития и безопасности. Окружающая среда всё больше превращается в цифровую техносферу, а люди — в постоянных беспрерывных пользователей интернет-сервисов, напрямую и косвенно вовлечённых, активных и пассивных.

В то же самое время мир сильно изменился, в том числе при помощи тех же самых компьютерно-сетевых технологий, и не во всём в лучшую сторону. Цифровые технологии способны объединить все производительные силы в единое автоматизированное предприятие, рассредоточенное по странам и континентам, а человечество в «совокупного рабочего», пользователей. Новый, мировой (транснациональный) уровень обобществления производительных сил пришёл в противоречие со старым мироустройством однополярного глобализма; переформатирование международных отношений в новые, равноправные и многополярные, сопровождается драматическими конфликтами [2]. Производительные и деструктивные возможности трансграничных цифровых сервисов, сочетания эффективности и безопасности переплетаются в изменчивых причудливых комбинациях, конфликтах антагонистических интересов [3]. Можно прогнозировать дальнейшее расширение перечня угроз, связанных с компьютерно-сетевыми технологиями и трансграничным характером интернет-коммуникаций, уже пополнившегося «культурой отмены», фальсификацией природы и истории, дезинформацией, «высокотехнологичными» антироссийскими санкциями недружественных стран и организаций.

Развитие технологий и социально-культурных реалий изменяет и терминологию: безопасность, прежде компьютерная, превратилась в информационную, далее трансформируется в цифровую, с возможным дальнейшим продолжением. Всё более явное проявление и усиление социально-культурного характера разработок, применения и последствий компьютерно-сетевых технологий даёт основания предполагать, что технологические аспекты безопасности со временем окажутся на заднем плане, станут специализированными, малозаметными. Тогда, возможно, устареет и само прилагательное «информационная», а общие вопросы безопасности будут по умолчанию предполагать фоновое применение компьютерно-сетевых технологий.

Список литературы

1. Былевский П.Г. Феноменология культуры информационной безопасности. М.: Московский государственный лингвистический университет, 2024. 240 с. ISBN 978-5-907899-09-4

2. Былевский П.Г. Разработка культурологической парадигмы информационной безопасности в контексте разрушения цифрового глобализма // Вестник Кемеровского государственного университета культуры и искусств. 2023. № 4(65). С. 54–65. DOI: 10.31773/2078-1768-2023-65-54-65 EDN: BLNCWN.

3. Былевский П.Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. № 8. С. 46–56. DOI: 10.7256/2454-0757.2023.8.43909.

УДК 004.056

В.Д. САЛЬНИКОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью статьи является обзор существующих автоматизированных решений, направленных на автоматизацию процесса повышения осведомленности работников в области информационной безопасности с учетом особенностей каждого решения.

Введение

По данным российской компании BI.ZONE с начала 2024 года общее количество фишинга выросло в 2,5 раза: как показывает опыт киберразведки BI.ZONE с электронного письма начинается 68% целевых атак [1]. На этом фоне эксперты считают особенно важным обучать персонал базовым принципам цифровой гигиены. Помимо этого, низкая стоимость и доступность инструментов организации фишинговых атак делает данный метод самым популярным у киберпреступников. Стоимость готовых фишинговых наборов в даркнете (DarkNet) варьируется от 30 до 1000 долл [2].

Постановка задачи

Для минимизации возникновения инцидентов и рисков, вызванных низкой осведомленностью, необходимо внедрять и оптимизировать процесс повышения осведомленности работников по вопросам информационной безопасности [3]. Оптимизация процессов возможна с помощью их автоматизации. Ниже представлен перечень отечественных и зарубежных решений для автоматизации процесса повышения осведомленности работников в вопросах информационной безопасности.

Для данного исследования были выбраны 6 решений (отечественных и зарубежных), на основе анализа открытых источников:

1. Kaspersky ASAP
2. МегаФон Security Awareness
3. Антифишинг
4. Phishman
5. Deteact Awareness
6. Syssoft Security Awareness

Пути решения проблемы

Для выбора оптимального автоматизированного средства повышения осведомленности, были определены следующие блок-факторы: облачное иностранное решение; отсутствие возможности легальной покупки лицензионного решения на территории РФ; возможность прохождения обучения менее, чем за год; продукт находится на рынке более 3-х лет; отсутствие возможности имитации фишинговых рассылок.

По итогу отбора из вышеуказанных решений с применением блок-факторов, были определены «лидирующие» решения:

1. Антифишинг 0 блок-факторов
2. Phishman 0 блок-факторов

Наиболее оптимальное решение под конкретную организацию определяется при детальном расчете KPI для каждого решения.

Заключение

В исследовании рассмотрены 6 комплексных решений автоматизации процесса повышения осведомленности работников в вопросах информационной безопасности. По итогам были определены два оптимальных решения, но выбор единственного сервиса возможен только при детальном исследовании каждой системы и определения KPI по конкретным запросам организаций.

Список литературы

1. BI.ZONE: общее количество фишинговых писем выросло в 2,5 раза с начала года // habr.com [Электронный ресурс] – Режим доступа: https://habr.com/ru/news/750234/ (дата обращения: 10.12.2023).

2. Сколько стоит организовать целевую кибератаку (Advanced Persistent Threat, APT) // www.anti-malware.ru [Электронный ресурс] – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/How-much-does-it-cost-to-organize-APT#part23 (дата обращения: 12.11.2023).

3. Корпоративный фишинг и спам в 2022 году: всё чаще атакуют HR-специалистов и бухгалтеров // www.kaspersky.ru [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/about/press-releases/2022_korporativnyj-fishing-i-spam-v-2022-godu-vsyo-chashe-atakuyut-hr-specialistov-i-buhgalterov (дата обращения: 30.11.2023).

УДК 004.056

К.Г. ДЕМКИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ТРАНСФОРМАЦИЯ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Исследование посвящено анализу изменений в методах кибератак, связанных с использованием социальных инженерий, на фоне активного развития современных технологий. Основное внимание уделено тому, как искусственный интеллект способствуют появлению более изощренных и персонализированных атак. Предложены подходы для защиты социума от эволюционирующих угроз социальной инженерии в цифровую эпоху.

Введение

Масштабы лжи каждый год практически удваиваются. В четвертом квартале 2023 года Facebook принял меры в отношении 691 млн поддельных аккаунтов. Также интенсивно растет сегмент клонирования голоса [1]. Социальная инженерия, как одна из ключевых угроз информационной безопасности, также трансформируется, используя в своих атаках новые технологии и подходы [2].

Постановка задачи

Главная задача исследования – определение влияния современных технологий, таких как искусственный интеллект, на эволюцию методов социальной инженерии и составление списка рекомендаций по защите социума от новых форм кибератак, возникающих в результате этой трансформации.

Решение поставленной задачи

Традиционные методы социальной инженерии, такие как фишинг, всегда строились на манипуляции доверием человека. Однако с внедрением технологий, основанных на использовании искусственного интеллекта, эти атаки стали значительно более эффективными и сложными для выявления [2]. С развитием AI опасной тенденцией стало появление deepfake-атак, позволяющих создавать поддельные видео- и аудиозаписи, где «говорят» известные личности или руководители компаний [3]. По данным Verizon в отчете за 2023 г., более 85% всех успешных нарушений безопасности связаны с человеческим фактором, что делает методы социальной инженерии основным вектором атак.

Для успешного снижения риска реализации атак, связанных с социальной инженерией, включая те, которые используют deepfake, необходимо адаптировать и расширять существующие стратегии информационной безопасности:

- Многофакторная аутентификация (MFA) значительно снижает риски, связанные с атаками на основе deepfake. Она затрудняет злоумышленникам завершение атаки, требуя от них совершить дополнительные шаги для получения

доступа, например, одноразовый код на другое авторизированное устройство. Данная процедура может помочь практически нейтрализовать атаку.

- Ограничение доступа к конфиденциальной информации усложнит процесс создания реалистичной подделки. Конфиденциальную информацию, находящуюся под строгим контролем, злоумышленники не смогут использовать для целевых атак с помощью spear phishing (персонализированные фишинговые атаки), потому что они зависят от информации, позволяющей злоумышленникам маскировать свои запросы под легитимные. Исследование Ponemon Institute показало, что ограничение доступа к данным позволяет снизить вероятность утечки информации в при использования средств социальной инженерии на 40%.
- Цифровые подписи и верификация документов обеспечат проверку подлинности документов. Это позволяет убедиться, что документ или приказ действительно исходит от того лица, за которое он себя выдает. Люди, которым пришла фальшивая инструкция не будут ей следовать, если они легко смогут проверить подлинность сообщения или документа. По данным исследования Gartner, использование цифровых подписей для подтверждения подлинности снижает риск мошенничества на 60%, особенно эта цифра играет роль в финансовых и юридических сферах.
- Разработка и внедрение политик безопасности внутри компании, направленных ограничение доступности данных сотрудников в открытых источниках, а также о рисках, связанных с размещением личной информации в публичных источниках, таких как, социальные сети и т.п.

Заключение

Методы социальной инженерии эволюционируют, адаптируясь к изменениям в цифровом пространстве. Только комплексный подход, включающий в себя многоуровневую аутентификацию, цифровые подписи и верификацию, а также повышение осведомленности, позволяет эффективно противостоять новым формам кибератак в условиях цифровизации социума.

Список литературы

1. Фалалеев М.А. Ситдикова Н.А. Нечай Е.Е. Дипфейк как феномен политической коммуникации // Вестник Забайкальского государственного университета. – 2021 (дата обращения: 15.09.2024).

2. Репенко В.А., Резниченко С.А. Защита от атак с применением средств и методов социальной инженерии. Вестник Дагестанского государственного технического университета. 2022: с. 85–96 (дата обращения: 15.09.2024).

3. Аррыкова Г.К. Чуриев М.М. Чарыев Д.Г. Социальная инженерия в кибербезопасности: исследование методов социальной инженерии как угрозы для организаций и разработка стратегий обучения и защиты персонала // Всемирный ученый. – 2024 (дата обращения: 15.09.2024).

УДК 004.056

В.Л. ЕВСЕЕВ, В.А. ПЕЧЕРСКИЙ

Национальный исследовательский ядерный университет «МИФИ», Москва

ЦЕЛЕСООБРАЗНА ЛИ ВИЗУАЛИЗАЦИЯ БЛОКИРОВОК СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ?

В докладе сделан акцент на анализ необходимости формирования уведомлений пользователям при блокировке их действий средствами защиты информации. Основное внимание уделено вопросам значительного снижения объема передаваемой информации об элементах защиты и дифференцированию событий безопасности по критичности.

Введение

В современных информационных системах (ИС) средства защиты информации (СЗИ) способны полностью блокировать действия клиента в случае обнаружения угроз. В таких ситуациях возникает вопрос о целесообразности информирования пользователей о блокировке по средствам соответствующих окон и создания событий безопасности в СЗИ. В связи со значительным потоком информации об инцидентах, которые требуется решить специалистам по информационной безопасности [1], в докладе проанализирован процесс информирования пользователей, а также детально рассмотрены возникающие при этом последствия.

Постановка задачи

Задача состоит в повышении эффективности работы администраторов СЗИ и уменьшении количества открытых данных об элементах защиты ИС путем определения инцидентов, в которых уведомления о блокировках пользователям избыточны.

Пути решения задачи

В ходе исследования был проведен анализ порядка 100 инцидентов информационной безопасности, зарегистрированных в течение 30 дней. Рассмотрены такие параметры, как тип инцидента, последствия и вероятность его возникновения. Для обработки данных использовался метод кластерного анализа, позволяющий разделить инциденты на группы по критичности. В частности, применен метод k-средних, который позволил выделить кластеры малокритичных и критичных инцидентов. Для подтверждения устойчивости кластеров применялись различные

методы валидации, включая «статистику Хопкинса», что позволило оценить тенденцию данных к группировке [2]. В вычислениях использовались инструменты на языке программирования R.

В результате проведенного исследования 12% событий были отнесены к группе малокритичных инцидентов, характеризующихся высокой вероятностью возникновения и низкими последствиями для ИС. Для событий данного типа предложена скрытая блокировка без отображения уведомлений, при которой действия пользователя прерываются без оповещения специалистов по ИБ. Данный фактор позволяет снизить нагрузку на администраторов безопасности и минимизировать риск утечек информации о работе СЗИ, что особенно актуально с учетом последних тенденций [3]. Напротив, для инцидентов с более серьезными последствиями, которые определены в 23% случаев, уведомления для пользователей и администраторов наиболее существенны, так как позволяют ускорить процесс реагирования на угрозы и минимизировать возможные негативные последствия для информационной системы.

Заключение

Исследование показало, что информирование пользователей о блокировках СЗИ должно носить дифференцированный характер в зависимости от критичности инцидента. Внедрение данного подхода может существенно повысить эффективность работы администраторов СЗИ, минимизировать количество открытой информации об используемых средствах защиты в ИС, а также улучшить пользовательский опыт. Разделение инцидентов по критичности позволяет снизить нагрузку на специалистов по ИБ, автоматизировать обработку некритичных инцидентов, и одновременно обеспечить оперативное реагирование на серьёзные угрозы, что в конечном итоге значительно повысит безопасность ИС.

Список литературы

1. Селютина А.А. Реагирование на инциденты информационной безопасности: научная статья / Селютина А.А. – СПб.: Изд-во СПбГЭУ, 2023. – 72 с.

2. Шитиков В.К., Мастицкий С.Э. Классификация, регрессия, алгоритмы Data Mining с использованием R [Электронный ресурс]. Режим доступа: https://github.com/ranalytics/data-mining, свободный (дата обращения 14.09.2024).

3. Стоделов Д.Н. Вопросы поиска информации об организациях по открытым источникам / Д.Н. Стоделов, Н.Г. Милославская // Кибернетика и информационная безопасность «КИБ-2023»: Сборник научных трудов Всероссийской научно-технической конференции, Москва, 18–19 октября 2023 года. – М.: НИЯУ МИФИ, 2023. – С. 82–83. – EDN IBCWQR.

УДК 004.056

А.А. ХОРЕВ

Национальный исследовательский университет «МИЭТ», Москва

ВЕРОЯТНОСТНЫЙ МЕТОД ОБОСНОВАНИЯ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ЭФФЕКТИВНОСТИ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

В статье предложено в качестве показателей оценки эффективности защиты речевой информации использовать вероятности вскрытия тематики перехваченного разговора и вероятности составления его аннотации. Получены аналитические соотношения по расчету этих вероятностей в зависимости от словесной и фразовой разборчивости речи, а также от количества ключевых слов и ключевых фраз, необходимых для определения тематики разговора и составления его аннотации.

В качестве показателя эффективности защиты речевой информации от ее утечки по техническим каналам наиболее часто используется словесная разборчивость речи (W), отображающая качественную область понятности перехваченного разговора, под которой понимается отношение количества правильно распознанных слов к общему количеству слов в перехваченном разговоре.

Критерии эффективности защиты речевой информации во многом зависят от целей, преследуемых при защите информации, например, скрыть тематику ведущегося разговора или скрыть его смысловое содержание. Следовательно, для оценки эффективности защиты речевой информации необходимо не только рассчитать словесную разборчивость речи, но и оценить количество ключевых слов и фраз, требуемых для определения тематики разговора или составления ее аннотации.

Будем полагать, что тематика разговора вскрыта, если количество распознанных ключевых слов $N_{сл.кл.р}$ будет не менее установленного порогового значения $N_{сл.кл.min.}$ Тогда, вероятность вскрытия тематики разговора P_m можно рассчитать по формуле [1]:

$$P_m(N_{сл.кл.р} \geq N_{сл.кл.min}) = \sum_{i=N_{сл.кл.min}}^{N_{сл.кл.р}} P_m(N_{сл.кл.р.i}), \qquad (1)$$

где $P_m(N_{сл.кл.р.i})$ – вероятность правильного распознавания i-го количества ключевых слов.

Вероятность $P_m(N_{сл.кл.р.i})$ можно рассчитать с использованием формулы комбинаторики, определяющую количество сочетаний без повторений [2]:

$$P_m(N_{сл.кл.р.i}) = \frac{\prod_{j=N_{сл.кл.р.i}+1}^{N_{сл.кл.}} j \cdot \prod_{j=N_{сл.кл.}-N_{сл.кл.р.i}+1}^{N_{сл..}-N_{сл.кл.}} j \cdot \prod_{j=1}^{N_{сл..}-N_{сл.кл.}} j}{\prod_{j=1}^{N_{сл.кл.}-N_{сл.кл.р.i}} j \cdot \prod_{j=N_{сл.кл.}-N_{сл.кл.р.i}+1}^{(N_{сл..}-N_{сл.кл.})-(N_{сл.кл.}-N_{сл.кл.р.i.})} j \cdot \prod_{j=N_{сл.кл.}+1}^{N_{сл..}} j}, \quad (2)$$

где $N_{сл}$ – количество слов в перехваченном разговоре;

$N_{сл.кл}$ – количество ключевых слов в перехваченном разговоре;

$N_{сл.р}$ – количество распознанных слов в перехваченном разговоре;

$N_{сл.кл.р}$ – количество распознанных ключевых слов в перехваченном разговоре;

$N_{сл.кл.min}$ – минимальное количество ключевых слов, необходимых для вскрытия тематики перехваченного разговора.

Среднее количество ключевых слов зависит от тематики разговора. Минимальное количество ключевых слов, необходимых для вскрытия тематики перехваченного разговора ($N_{сл.кл.min}$), и пороговая вероятность вскрытия тематики разговора ($P_{т.п}(N_{сл.кл.р.i})$) определяются экспертным методом.

Допустим при перехвате разговора, состоящего из 1300 слов (2,5% из которых ключевые) словесная разборчивость речи составила 20% и $N_{сл.кл.min} = 7$.

Тогда вероятность вскрытия тематики разговора, рассчитанная по формуле (1), будет равна $P_т = 0{,}4$ [1].

Аналогичным образом может быть рассчитана и вероятность составления аннотации разговора $P_{ан.}$

Следовательно, в качестве показателей эффективности защиты речевой информации от ее утечки по техническим каналам целесообразно использовать не словесную разборчивость речи, а вероятности вскрытия тематики разговора $P_т$ или составления его аннотации $P_{ан}$, а в качестве критериев эффективности – их пороговые значения, определяемые на основе экспертных оценок.

Список литературы

1. Хорев А.А., Порсев И.С. Вероятностный метод обоснования показателей и критериев эффективности защиты речевой информации от ее утечки по техническим каналам// Вестник УрФО «Безопасность в информационной сфере». – Челябинск, УрФО. – 2024. – № 2(52) – С. 27–36.

2. Яремко Н. Н. Краткий курс комбинаторики, теории вероятностей и математической статистики: учеб. пособие / Н. Н. Яремко, О. Г. Никитина. – Пенза: Изд-во ПГУ, 2017. – 134 с.

УДК 004.056

А.М. АЛЮШИН[1, 2], С.В. ДВОРЯНКИН[1, 2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Московский государственный лингвистический университет*

МЕТОДЫ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА РЕЧЕВЫЕ АУДИОЗАПИСИ

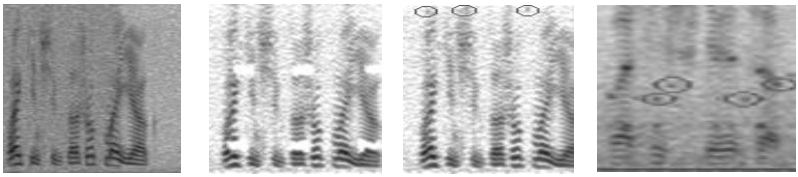
В работе проанализированы существующие методы защиты авторских прав цифрового контента посредством внедрения цифровых меток в речевые сигналы. Разработаны эффективные методы внедрения меток во временной и спектральной областях, показаны их преимущества и недостатки. Проанализирована работоспособность созданных методов защиты при детектировании меток с помощью повторной микрофонной аудиозаписи.

Актуальность защиты авторских прав в речевых сигналах обусловлена быстрым развитием технологий, позволяющих легко копировать и распространять аудиоматериалы без разрешения правообладателей. Отсутствие должной защиты может привести к распространению недостоверной информации и дезинформации, что негативно скажется на безопасности, общественном сознании и культуре. Таким образом, разработка эффективных механизмов защиты авторских прав является необходимым условием для поддержания справедливого баланса между интересами создателей и потребителей аудиоконтента.

В работе проанализированы существующие методы маркирования аудиосигналов [1–3], показаны их преимущества и недостатки. Среди основных недостатков следует выделить низкую эффективность методов обнаружения встроенных меток после повторной записи сигналов, например, через микрофон. Для решения этой задачи, а также для повышения уровня скрытности были разработаны следующие методы встраивания меток в речевые сигналы, учитывающие их специфику:

- Маркирование методом размножения шумовой составляющей (МРШС).
- Маркирование методом удаления спектральной составляющей (МУСС).
- Маркирование методом вставкой информации на локальных максимумах (МВИЛМ).
- Маркирование методом внедрения контрольной информации посредством модификации фаз (МВИПМФ).

Спектрограммы данных методов маркирования приведены на рис. 1.



а) б) в) г)

Рис. 1. Примеры спектрограмм со встроенными метками:
а) метод МРШС; б) метод МУСС; в) метод МВИЛМ; г) метод МВИПМФ.

Сравнительные характеристики описанных выше методов встраивания меток в речевые сигналы представлены в табл. 1.

Таблица 1. Сравнение различных методов аудиомаркирования

Методы маркирования	МРШС	МУСС	МВИЛМ	МВИПМФ
Среднее значение параметра ODG (мера близости) анализируемых сигналов при сравнении с исходным	-1.7143	-0.5363	-0.8436	-1.8327
Мера близости спектрограммы эталонного сигнала и маркированного (по Минковскому)	60%	84%	92%	98%
Вероятность обнаружения меток в повторно записанном сигнале на расстоянии 5 м от источника	< 0.1	< 0.1	0.6	0.5

Из анализа результатов экспериментов можно сделать вывод, что метод МВИЛМ и метод МВИПМФ имеют наилучшие характеристики при детектировании меток после перезаписи. Однако метод МВИПМФ более скрытен для распознавания при анализе спектрограммы.

Список литературы

1. Hua G., J.Huang Twenty years of digital audio watermarking - a comprehensive review. Signal Processing. - 2016. – Vol. 128. – P. 222–242.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2020. – 262 с.

3. Гофман М.В., Корниенко, А.А. Мирончинков Е.Т. Методы цифрового маркирования аудиосигналов для скрытой акустической связи через воздушный аудиоканал. Труды СПИИРАН, 2017, выпуск 55, с. 185–215DOI: https://doi.org/10.15622/sp.55.8.

4. Минаев В.А., Дворянкин С.В., Алюшин А.М. Методы биомаркирования защищаемых объектов. Информация и безопасность. 2023. Т. 26. № 3. С. 321–328.

УДК 004.056

С.В. ДВОРЯНКИН[1, 2], Н.С, ДВОРЯНКИН[1], А.Е. ЗЕНОВ[2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Московский государственный лингвистический университет*

О ПРИВАТНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ В РЕЧЕВЫХ ТЕХНОЛОГИЯХ

Приведена классификация угроз, связанных с конфиденциальностью и приватностью в речевых технологиях. Показана разница между этими понятиями. Рассмотрены подходы к их обеспечению на практике. Обоснована необходимость регулирования доступа к речевой коммуникации в зависимости от потребностей пользователя. Установлено пересечение проблем конфиденциальности и этики.

Речь – естественный способ коммуникации, содержащий большое количество информации не только смыслового содержания. Так она содержит приватную информацию о состоянии здоровья, эмоциях, физической, психологической, социальной идентичности и др., раскрытие которой может привести к серьезным последствиям (табл. 1).

Понятия конфиденциальности (К) и приватности (П) проявляются во всех областях применения речевых технологий (РТ). Их не следует отождествлять. К – это требование не разглашать информацию третьим лицам, а П – это право на неприкосновенность частной жизни и личной информации (см. табл. 1).

Базовая классификация угроз К и П приведена в [1]. Общий подход к противодействию - минимизировать передачу и хранение, а также доступ к конфиденциальной и приватной информации в речевом сообщении (РС), которая не имеет в данный момент коммуникации отношения к выбранным пользователем услугам. Понять, какая информация является релевантной. Определить, что нужно пользователю: предоставить информацию и-или обеспечить контроль над услугами и угрозами.

Для защиты смыслового содержания используются криптоалгоритмы шифрования речевого потока. Что касается П в РС то основной подход заключается в удалении из РС как можно больше и как можно раньше «побочной» частной информации, т.е. «выхолостить» РС.

Однако подобное удаление надо проводить с большой осторожностью. Например, паралингвистическая информация, такая как стиль речи, часто бывает полезной в передаче намеченного сообщения. То есть, не всегда ясно, что представляет собой очищенное от частных характеристик РС.

Таким образом, необходимо динамически регулировать доступ к речевой коммуникации в зависимости от потребностей пользователя.

Также сами системы с РТ должны активно отслеживать состояние К и П, чтобы определять соответствующие действия по их защите.

Кроме того, установлено, что этические ценности определяют предпочтения в отношении К и П. Большинство потенциальных нарушений этики в речевых технологиях связано с их нарушением.

Имеются и другие вопросы, требующие решения, такие как: согласие на использование речевых данных; метрики для потоковой передачи речи; модели нарушителя К и П; многопользовательское взаимодействие.

Таблица 1. Выбор категорий частной информации, потенциально идентифицируемой по речевым сигналам, и степень, в которой они сохраняются с течением времени.

Категории	**Примеры**	**Характер**	**Контроль**
Биологические	Характеристики организма	Устойчивые	Нет
	Состояние здоровья	Переменное	Нет
Психологические	Эмоции	Переменная	Частично
	Интеллект	Устойчивый	Нет
	Образование, навыки	Поддерживается	Да
	Гендерная идентичность	Поддерживается	Нет
Сообщение	Текст, акцент, стиль, выражение	Переменная	Да
	Манерность, контекст	Переменная	Частично
	Выбор языка и навыки	Частично	Частично
Принадлежность	Этническая, национальная, культурная, религиозная	Устойчивая	Нет
Характер отношений	Иерархия, знакомство, влечение, близость	Устойчивый	Частично
	Частость встреч с человеком	Переменная	Да
Физическое окружение	Фоновые звуки, расстояние до датчика, расстояние передачи, реверберация	Переменная	Да
Используемое оборудование	Тип и производитель сенсора	Переменная	Да

Ожидается, что дальнейшее совершенствование интеллектуальных РТ повысит их полезность. Но при этом, при появлении новых угроз частной жизни, роль обеспечения К и П в РТ будет постоянно возрастать.

Список литературы

1. Tom Backstrom, Senior Member, IEEE. Privacy in Speech Technology. arXiv:2305.05227v1 [eess.AS] 9 May 2023.

УДК 81.22

А.С. ВАНИЧКИНА

Московский государственный лингвистический университет

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ

Исследование анализирует влияние цифровой трансформации на взаимодействие человека с технологиями, подчеркивая уязвимость, связанную с социальной инженерией. Целью работы является изучение человеческого фактора в контексте безопасности и использование лингвистических и когнитивных методов для противодействия угрозам. Работа акцентирует внимание на необходимости комплексного подхода к безопасности, учитывая информационную перегрузку и снижение критического мышления, чтобы повысить устойчивость современных социотехнических систем.

Современное общество представляет собой сложную социотехническую систему, в которой взаимодействие человека и различных технических приборах происходит не только в рамках организационных производственных процессов и отношений, но и в повседневной жизни. Этому способствует постоянное развитие технологий, таких как Интернет вещей, мобильных устройств и так далее. Если раньше в доцифровую эпоху использование технологий носило ограниченный характер, то в настоящий момент не существует ни одной сферы, в которой бы не использовались цифровые технологии. Особенно актуально это стало заметно в эпоху пандемии, когда все организационные процессы и бытовые вопросы были переведены в цифровой формат, то есть произошла цифровая трансформация на уровне государств. Безусловно, в таком переходе было много позитивных изменений, которые были отмечены обществом немедленно, но с течением времени стало очевидны негативные последствия такого резкого трансформационного перехода.

Следует обратить внимание на то, что при оценке цифровой трансформации нередко из поля зрения выпадает такой важный фактор, как человек и то воздействие, которое может быть на него оказано. С развитием технологий понятие периметра безопасности трансформировалось и на данный момент фактор «человека как уязвимости» стал одной из основных проблем, стоящих перед профессиональным сообществом. И здесь важен не только так называемый «человеческий фактор», который криптограф и специалист в области компьютерной безопасности Брюс Шнайер описал следующим

образом: «Я говорю потенциальным клиентам, что математика непогрешима, компьютеры могут быть взломаны, как и сети, а люди ужасны своей непредсказуемостью. Я долго занимался решением проблем защиты компьютеров и сетей, но это не приблизило меня ни на дюйм к решению проблемы человека» [1, С.149]. Ряд исследователей подчеркивает подверженность человека методам социальной инженерии [2]. При этом, если мы ранее говорили о факторе наивности, неподготовленности людей к такой угрозе, то сейчас как отдельные организации, так и государство в целом развертывают масштабные кампании с целью проинформировать людей о подобных угрозах. Организации проводят тренинги и обучения, тестируют сотрудников, что безусловно, приносит свои плоды, но этого мало, так как не учитываются иные факторы, такие как перегруженность современного человека информацией, что приводит к снижению критического мышления

Однако, все эти институты оказываются на шаг позади злоумышленников, которые постоянно совершенствуют свои подходы и изобретают все новые методы оказания воздействия на людей, используя различные манипулятивные методы воздействия.

В настоящее время перспективными представляются подходы и методики борьбы с преступлениями, основанными на применении методов лингвистической прагматики и когнитивной лингвистики для изучения и анализа воздействия на потенциальную жертву. Лингвистическая прагматика, изучающая использование языка с целью оказания воздействия, позволяет выявлять скрытые намерения и манипулятивные стратегии в коммуникации. Анализ речевых актов помогает распознавать потенциально опасные запросы, апеллирующие к доверию и срочности, часто использующихся мошенниками. Когнитивная лингвистика, в свою очередь, фокусируется на том, как язык отражает ментальные процессы и может использоваться для создания более безопасных информационных сред.

В условиях стремительной цифровой трансформации современного общества, где технологии пронизывают каждую сферу, от профессиональной до личной, для повышения устойчивости социотехнических систем требуется комплексный подход, который учитывает лингвистические и когнитивные факторы, что станет важным шагом на пути к созданию более надежного цифрового будущего.

Список литературы

1. Schneier B. Secrets and lies: digital security in a networked world. Wiley, 2015.
2. Lineberry S. The human element: the weakest link in information security. JOFA, 2007, vol. 204, no. 5, p. 44.

КИБ-2024
КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Разработка безопасного программного обеспечения

Руководитель секции – ЗАГРЕБАЕВ А.М., д.ф.-м.н.,
заведующий кафедрой №22

УДК 004.056+004.85

АРУСТАМЯН С.С.[1], АНТИПОВ И.С.[2], МАГАКЕЛОВА Н.А.[3]

[1]*Научно-производственное объединение «Эшелон», Москва*

[2]*Московский государственный технический университет им. Н.Э. Баумана*

[3]*Финансовый университет при Правительстве Российской Федерации*

ПОДХОД К ФАЗЗИНГ-ТЕСТИРОВАНИЮ ПРОГРАММ В РАМКАХ ЦИКЛА БЕЗОПАСНОЙ РАЗРАБОТКИ

В данной статье рассматривается альтернативный подход к фаззинг-тестирование в рамках цикла безопасной разработки программ, путем применения алгоритмов машинного обучения для оценивания результатов предыдущей итерации. Данный метод основан на обучении модели прямого прогнозирования, которая сопоставляет входные данные программы с результатами выполнения. Затем обученная модель применяется для оценки входных данных, повышая эффективность проведения фаззинг-тестирования в несколько раз.

Введение

Цель фаззинг-тестирования состоит в том, чтобы обнаружить набор тестовых входных данных, который максимизирует охват кода в целевом программном комплексе в надежде, что это позволит найти ошибки или уязвимости [1-7]. В ходе типичного запуска фаззинга генерируется сотни тысяч входных данных, и лишь малая часть фактически покрывает новые пути выполнения программы, что приводит к сотням минут ненужного времени выполнения. Цель исследования состояла исследовании и интеллектуального фаззинга.

Сравнение AK-VS 3 ModFuzz и AFL

В таблице Таблица 1 представлен сравнительный результат классического фаззинг-тестирования на примере AFL с интеллектуальным фаззинг-тестированием на примере AK-VS 3 ModFuzz. Сравнивалось количество новых ветвей, который обнаружил каждый из фаззеров за одинаковое количество времени. В итоге удалось выявить, что результаты AK-VS 3 ModFuzz превосходят результаты AFL. После 30 минут проведения фаззинг-тестирования результаты AK-VS 3 ModFuzz более чем в 2 раза превосходят результаты AFL за аналогичное время. После 7 часов фаззинг-тестирования AK-VS 3 ModFuzz показал эффективность почти в 1,5 выше по сравнению с AFL. Данные результаты позволяют сделать вывод, что метод, описанный в данной статье, является

эффективным и может применяться при проведении фаззинг-тестирования.

Таблица 1. Результаты сравнения

Время	AFL	AK-VS 3 ModFuzz
30 минут	81	163
1 час	144	203
3 часа	632	634
7 часов	842	1248

Заключение

Авторы отмечают, что основным недостатком классического фаззинг-тестирования является количество выполнений программных или программно-аппаратных комплексов, которые тратятся впустую на избыточные входные данные. Чтобы устранить эту проблему, авторы предложили новый подход, использующий методы машинного обучения. Он заключается в использовании нейронных сетей для генерации входных данных, которые с большей вероятностью приведут к нахождению новых путей работы программы. Для проверки приведенного метода был проведен эксперимент на тестовой программе. Его результаты показали, что интеллектуальное фаззинг-тестирование является более эффективным по сравнению с классическим фаззинг-тестированием.

Список литературы

1. Зегжда Д.П., Александрова Е.Б., Калинин М.О. и др. Кибербезопасность цифровой индустрии // Теория и практика функциональной устойчивости к кибератакам. М.: Горячая линия – Телеком, 2021. – 560 с.

2. 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.

3. Арустамян С.С., Антипов И.С. Интеллектуальные методы фаззинг-тестирования в рамках цикла безопасной разработки программ // В сборнике: Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. М.: МТГУ им. Н.Э. Баумана, 2023. С. 11–15.

4. Козачок А.В., Ерохина Н.С., Николаев Д.А. Способ обнаружения программных дефектов в Javascript-интерпретаторах методом фаззинг-тестирования // Вопросы кибербезопасности. 2024. № 2 (60). С. 74–80.

5. Козырский Б.Л., Комаров Т.И., Иванов М.А. Использование фаззинга для поиска уязвимостей в программном обеспечении // Безопасность информационных технологий. 2014. Т. 21. № 4. С. 33–43.

6. Теплюк П.А., Якунин А.Г. Модели и подходы к анализу поверхности атаки для фаззинг-тестирования ядра Linux // Безопасность информационных технологий. 2024. Т. 31. № 1. С. 135–145.

7. Барабанов А.В., Варенница В.В., Марков А.С. Аудит безопасности программ. Учебно-методическое пособие. – М.: МТГУ им. Н.Э. Баумана, 2021. – 56 с.

УДК 004.056

АНТИПОВ И.С.[1], АРУСТАМЯН С.С.[2], МАГАКЕЛОВА Н.А.[2, 3]

[1]*Московский государственный технический университет им. Н.Э. Баумана*

[2]*Научно-производственное объединение «Эшелон», Москва*

[3]*Финансовый университет при Правительстве Российской Федерации*

ВЫБОР СТАТИЧЕСКОГО АНАЛИЗАТОРА КОДА ПРИ СЕРТИФИКАЦИИ

В данной статье представлен подход сравнения статических анализаторов кода, который включает современную методологию тестирования. Сравнение статических анализаторов кода проводится по показателям эффективности, функциональности и удобства, представленных в российских нормативных документах. Для показателя эффективности и функциональности были подготовлены синтетические тестовые примеры с открытым исходным кодом, которые содержат в себе уязвимости. Критерии оценки качества были определены в соответствии с российскими документами.

Введение

Статический анализ исходного кода применятся как при сертификации программных средств защиты информации [1, 2], так и при сертификации процессов разработки безопасного программного обеспечения [3, 4].

Для получения достоверных результатов и минимизации ложноположительных срабатываний (false positive), необходимо использовать несколько независимых друг от друга инструментов. Данный доклад посвящена сравнению различных статических анализаторов [5, 6].

Исследование статических анализаторов

Было выбрано два коммерческих анализатора и три анализатора с открытым кодом: АК-ВС3, Cppcheck, Clang SA, Horusec и Svace. Для оценки использовались тестовые наборы с открытым исходным кодом. Результат исследования представлены в таблице. Можно заметить, что два анализатора (Svace и Clang SA) не поддерживают CWE, поэтому срабатывания нельзя однозначно классифицировать.

Таблица 2. Дефекты кода (CWE), обнаруженные статическими анализаторами

Продукт	АК-ВС3	Cppcheck	Horusec
FFmpeg	14, 114, 134, 259, 394, 398, 480, 511, 563, 569, 570, 571, 628, 665, 667, 672, 690, 758, 798	190, 398, 457, 476, 562, 682, 758, 775, 786, 788	2, 20, 12, 36, 37, 78, 119, 120, 126, 134, 190, 327, 352, 362, 367, 676, 798, 807, 82
firebird	378, 401, 465, 476, 563, 672	401, 415, 457, 562	312, 798
httpd	121, 188, 243, 259, 369, 416, 465, 467, 476, 561, 563, 587, 672, 676, 690, 704, 775, 788, 824, 1041	398, 457, 476, 758	489
librdkafka	14, 369, 398, 401, 416, 465, 476, 561, 563, 569, 570, 571, 670, 676, 761, 763, 770, 824	398, 401, 476, 628, 682, 685, 768	2, 12, 20, 36, 37, 78, 119, 120, 134, 190, 312, 327, 676, 704, 798, 807
ruby	14, 134, 401, 404, 480, 563, 570, 672, 676, 770	398, 401, 415, 457, 476, 562, 628, 682, 758	2, 12, 20, 22, 36, 37, 73, 78, 119, 120, 126, 134, 190, 250, 312, 352, 362, 327, 676, 785, 798, 807, 829
unit	401, 416, 465, 476, 561, 563, 570, 763, 824	398, 401, 457, 476, 562	2, 12, 20, 22, 36, 37, 73, 89, 119, 120, 134, 190, 209, 250, 327, 330, 362, 367, 539, 611, 676, 704, 785, 798, 807

Вывод

Наилучший эффект от статического анализа может быть достигнут только при использовании нескольких инструментов, что позволит более исчерпывающе классифицировать дефекты кода.

Список литературы

1. Барабанов А.В., Вареница В.В., Марков А.С. Аудит безопасности программ Учебно-методическое пособие. – М.: МТГУ им. Н.Э. Баумана, 2021. – 56 с.

2. Бударный Г.С., Пестов И.Е., Штеренберг И.Г. Сравнение методов статического анализа исходного кода программы // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 1. С. 5–12.

3. Арустамян С.С., Вареница В.В., Марков А.С. Методические и реализационные аспекты внедрения процессов разработки безопасного программного обеспечения // Безопасность информационных технологий. 2023. Т. 30. № 2. С. 23–37.

4. Markov A.S., Varenitca V.V., Arustamyan S.S. Topical Issues in The Implementation of Secure Software Development Processes // In Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance. IPSQDA-2023. 2023. P. 48–53.

5. Марков А.С., Фадин А.А., Швец В.В. Сравнение статических анализаторов безопасности программного кода // Защита информации. Инсайд. 2015. № 6 (66). С. 38–43.

6. Markov A., Fadin A., Shvets V., Tsirlov V. The Experience of Comparison of Static Security Code Analyzers // International Journal of Advanced Studies. 2015. Т. 5. № 3. С. 55–63.

УДК 004.056

С.К. МУРАВЬЁВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ООО «Научно-техническое предприятие «Криптософт», Пенза

УГРОЗЫ ВРЕДОНОСНОГО ВМЕШАТЕЛЬСТВА В ПРОЦЕССЫ ОПТИМИЗАЦИИ ИСХОДНОГО КОДА

С целью повышения безопасности разрабатываемого программного обеспечения в работе рассмотрена возможность вредоносного изменения конвейера оптимизации исходного кода через штатные интерфейсы компилятора, позволяющие принципиально изменить алгоритм работы компилируемого приложения, даны рекомендации по нейтрализации подобных угроз. Результаты работы могут быть использованы при разработке перспективных средств разработки безопасного программного обеспечения (РБПО).

В настоящее время уделяется особое внимание вопросам снижения числа уязвимостей в разрабатываемом программном обеспечении (ПО). При этом уязвимости в ПО могут быть следствием не только ошибок, допущенных на этапе подготовки исходного кода, но и появиться в результате процедур оптимизации кода и сборки программ, выполняемых компилятором [1]. Осуществление преднамеренных действий в отношении инструментальных средств, применяемых при разработке ПО, внутренними и внешними нарушителями способно привести к возникновению различных угроз безопасности информации [2], что делает актуальным исследование угроз вредоносного вмешательства в процессы оптимизации исходного кода.

Ключевым элементом современных средств разработки ПО являются оптимизирующие компиляторы, которые в процессе компиляции применяют к исходному коду конвейер оптимизации, включающий множество операций для его анализа и трансформации, называемых проходами. При этом наиболее известные компиляторы, входящие в состав LLVM [3] и GCC [4], предоставляют штатные программные интерфейсы для разработки и подключения расширений, способных кардинально изменить процесс оптимизации исходного кода.

Одна из самых типичных задач, решаемая оптимизаторами компиляторов, заключается в поиске таких участков исходного кода, результат выполнения которых не меняется в процессе выполнения целевого приложения, и их замена на соответствующие константные

значения. Используя штатные интерфейсы компилятора, злоумышленник может включить в состав конвейера оптимизации вредоносный проход, который способен заменить использование вычисляемого или получаемого значения, обрабатываемого целевым приложением и которое связано с обеспечением безопасности информации, на константу с требуемым злоумышленнику значением. Примером такой вредоносной оптимизации может выступать замена инициализирующего значения для генератора случайных чисел на значение, известное злоумышленнику. После такой замены злоумышленник сможет предсказывать все числовые последовательности, получаемые с помощью такого генератора, что создаёт серьёзные угрозы безопасности информации.

Для нейтрализации подобных угроз в первую очередь необходимо зафиксировать перечень разрешенных к применению проходов оптимизации и реализовать общие требования к безопасному компилятору языков C/C++ в части формирования и контроля базы данных компиляции [1]. Также потребуется разработка и внедрение новых средств контроля конфигурации среды разработки и системного окружения операционной системы. Интерфейсы для динамического подключения к компилятору внешних модулей расширения должны быть отключены или доработаны таким образом, чтобы осуществлялся надёжный контроль аутентичности таких модулей. Защиту от описанной угрозы также можно обеспечить за счёт использования защищённой операционной системы QP ОС [5] в качестве основы для платформы РБПО.

Представленные в статье сведения могут быть использованы при проектировании и реализации перспективных средств РБПО, а также при внедрении соответствующих процессов РБПО [6].

Список литературы

1. ГОСТ Р 71206-2024 Защита информации. Разработка безопасного программного обеспечения. Безопасный компилятор языков C/C++. Общие требования.

2. ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения.

3. Наке К., Кван Э. LLVM 17: Инфраструктура для разработки компиляторов / пер. с англ. А.А. Слинкина. – М.: ДМК Пресс, 2024. – 370 с.

4. Interacting with the pass manager. URL: https://gcc.gnu.org/onlinedocs/gccint/Plugins-pass.html (дата обращения: 18.09.2024).

5. Егоров В.Ю. Экосистема операционной системы QP ОС // Системы и средства защиты информации: сб. ст. 15-й межведомственной научно-практической конференции им. Е.А. Матвеева. – Пенза: Издательство ПГУ, 2024. – С. 29–36.

6. ГОСТ Р 56939 – 2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования.

УДК 528.71:004.512.4

В.А. МИНАЕВ[1], А.С. ТОЛПЫГИН[2]

[1]*Московский университет МВД России им. В.Я. Кикотя*

[2]*Московский государственный технический университет им. Н.Э. Баумана*

КИБЕРБЕЗОПАСНОСТЬ УПРАВЛЕНИЯ БЕСПИЛОТНЫМ ТРАНСПОРТОМ

Рассматриваются вопросы кибербезопасности беспилотного транспорта, проводится анализ угроз его системам управления, обсуждается подход к описанию угроз на этапах жизненного цикла – от формирования требований к ним до вывода из эксплуатации, предлагается иерархическая структура системы контроля и управления беспилотным транспортом и разработка системы моделей угроз кибербезопасности для беспилотного транспорта.

Проблемы и задачи

Беспилотный транспорт проникает во все сферы жизни общества и отрасли хозяйственного механизма страны. Активно развиваются автомобильный, авиационный, железнодорожный, морской виды беспилотников.

Беспилотные летательные аппараты (БПЛА) активно применяются для решения задач мониторинга объектов критически важной инфраструктуры городов (трубопроводы, линии электропередач и связи, дорожная инфраструктура, вокзалы, аэропорты); грузоперевозок; разведки в труднодоступных местах (геологоразведка, мониторинг водных объектов); обеспечения безопасности, борьбы с преступностью и охраны общественного порядка.

В России принимаются меры государственной поддержки развития беспилотного наземного и водного транспорта и авиационных систем (БАС). По оценкам, к 2027 г. производство БПЛА в России достигнет 2 млн шт. в год, а на дорогах будет функционировать не менее 100 тыс. беспилотных автомобилей [1].

Однако все более проявляются и негативные последствия применения беспилотных транспортных средств (БТС) [2]. Так, из-за слабого контроля БТС увеличивается вероятность террористических актов, шпионажа и других противоправных действий. Этому способствуют складывающаяся геополитическая обстановка, быстрое развитие перспективных технологий, цифровизация общества, недостатки государственного регулирования. Поэтому необходима система управления, обеспечивающая:

– полный контроль трафика в границах зон защищаемых объектов критической инфраструктуры;

– киберустойчивость БТС и их защиту от неправомерного применения;

– контроль выполнения маршрутных (полетных) заданий. Выявление и предотвращение аномалий в поведении БТС;

– соответствие БТС законодательству РФ и требованиям регуляторов по безопасности их применения.

Пути обеспечения кибербезопасности беспилотников

Реализация угроз кибербезопасности БТС, в первую очередь, связана с уязвимостями в системе управления БТС, которая представляет собой комплекс программно-аппаратных средств и каналов связи, обеспечивающих автономное управление БТС без участия человека.

По методике просеивания угроз из Банка данных угроз (БДУ) безопасности информации ФСТЭК авторами выявлены более 30 угроз, которые могут быть осуществлены с высокой вероятностью и иметь высокий уровень влияния. Выделены следующие группы угроз кибербезопасности для беспилотного транспорта – данных, связи, инфраструктуры, системы искусственного интеллекта.

С целью учета факторов и сфер проявления угроз безопасности системам управления БТС разработаны модели угроз безопасности (МУБ) для каждого конкретного вида и класса: базовая модель угроз (БМУ) безопасности беспилотного транспорта; частные (по видам БТС) модели угроз (ЧМУ); типовые МУ безопасности частей системы управления БТС [3].

Заключение и выводы

Принимая во внимание, что развитие беспилотного транспорта включено в приоритетные направления проектов технологического суверенитета Российской Федерации, и формирование отрасли носит стремительный характер, подчеркнем необходимость обеспечения полного контроля трафика БТС в границах зон защищаемых объектов критической инфраструктуры, киберустойчивости БТС.

Список литературы

1. Future Readiness Indicator. URL: https://www.imd.org/future-readiness-indicator/home/automotive-2023/ (дата обращения: 10.08.2024).

2. Соколов И.А. и др. Умные города, инфраструктуры и их антитеррористическая устойчивость. Опыт интеграции антитеррористических стандартов США и создания программного обеспечения для цифровой безопасности // International Journal of Open Information Technologies. 2017. Т. 5. №. 7. – С. 45–65.

УДК 004.056

В.В. ПЕРОВ
Научный руководитель – к.т.н., доцент А.П. ДУРАКОВСКИЙ
Национальный исследовательский ядерный университет «МИФИ», Москва

ИССЛЕДОВАНИЕ ФАКТОРОВ ВОЗНИКНОВЕНИЯ ЛОЖНОПОЛОЖИТЕЛЬНЫХ И ЛОЖНООТРИЦАТЕЛЬНЫХ РЕЗУЛЬТАТОВ СТАТИЧЕСКОГО АНАЛИЗА ИСХОДНОГО КОДА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель исследования – анализ основных причин возникновения ложноположительных и ложноотрицательных результатов статического анализа исходного кода программы и разработка рекомендаций по их снижению. В рамках работы выполнен обзор современных инструментов статического анализа и их особенностей, проведен анализ влияния специфических языковых конструкций, стандартов оформления кода и архитектурных паттернов на точность анализа.

Введение

В современном мире программное обеспечение (ПО) играет ключевую роль во всех сферах деятельности человека – от бизнеса и промышленности до образования и здравоохранения. Возрастает количество ПО, использующих в своем составе зависимости с открытым исходным кодом, которое несет в себе множество угроз уязвимостей [1]. Эффективным инструментом обеспечения требований по безопасному ПО является статический анализ исходного кода. Одним из основных препятствий на пути его эффективного использования являются ложноположительные и ложноотрицательные результаты.

Анализ факторов возникновения ложных результатов статического анализа кода

Ложноположительные результаты статического анализа ПО могут быть вызваны следующими факторами:

1) **Сложность языковых конструкций и особенностей языков программирования.** Современные языки, такие как JavaScript и Python, поддерживают динамическую типизацию, который усложняет статический анализ. Динамические языковые особенности могут привести к увеличению числа ложноположительных срабатываний из-за неопределенности типов и структур данных на этапе компиляции [2].

2) **Недостаточный контекстный анализ.** Инструменты статического анализа часто не учитывают весь контекст выполнения программы, что может приводить к ошибочным интерпретациям сложных конструкций.

3) **Ограничения алгоритмов и правил анализа.** Проблемы с точностью статического анализа часто возникают из-за использования упрощённых алгоритмов, которые ограничивают возможности инструмента.

Ложноотрицательные результаты статического анализа ПО могут быть вызваны следующими факторами:

1) скрытые или сложные уязвимости. Некоторые уязвимости остаются невыявленными при использовании стандартных инструментов, что связано с ограничениями в анализе потоков данных.

2) использование внешних библиотек и компонентов. Недостаточная информация о сторонних модулях может привести к тому, что уязвимости, связанные с их использованием, останутся незамеченными.

3) обфускация и некорректные практики написания кода. Использование нестандартных или запутанных методов программирования усложняет анализ и может приводить к пропуску ошибок.

Заключение

Ложноположительные результаты в статическом анализе исходного кода возникают, когда инструмент сообщает об ошибке, которой нет. Это может быть вызвано сложностью языковых конструкций, динамической типизацией, недостаточным контекстным анализом или ограничениями применяемых алгоритмов. Ложноотрицательные результаты возникают, когда реальные уязвимости остаются незамеченными, что может быть связано с использованием внешних библиотек, сложностью межпроцедурных взаимодействий и неэффективностью обработки обфусцированного кода. Эти проблемы затрудняют объективную оценку качества программного обеспечения и требуют улучшения подходов к анализу.

Список литературы

1. Марков А.С. Важная веха в безопасности открытого программного обеспечения / А.С. Марков // Вопросы кибербезопасности. – 2023. – № 1(53). – С. 2–12. – DOI 10.21681/2311-3456-2023-1-2-12. – EDN OHYLTR.

2. Tymchuk, Yuriy (June 2017). The False False Positives of Static Analysis. In: Seminar Series on Advanced Techniques and Tools for Software Evolution SATToSE 2017. Madrid, Spain. 07–09. Juni 2017.

УДК 004.056

О.Д. ПАНФЕРОВ

Калужский филиал
Московского государственного технического университета имени Н.Э. Баумана

ОРГАНИЗАЦИЯ ХРАНЕНИЯ И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В МОДЕЛЯХ ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ ЯЗЫКАХ ВЫСОКОГО УРОВНЯ

Доклад включает обзор принципов безопасного хранения и обработки данных на этапе проектирования программных систем. Представлен анализ, как объектно-ориентированные модели могут способствовать соблюдению требований безопасности, включая управление доступом, шифрование данных и анонимизацию. Особое внимание будет уделено практическим аспектам внедрения этих принципов в код на языках высокого уровня, таких как Java, C# и Python. Цель доклада – предоставить участникам конференции знания и инструменты, необходимые для создания надежных и безопасных программных систем, которые эффективно защищают персональные данные пользователей.

Обеспечение безопасности хранимых и обрабатываемых данных – одна из первоочередных задач при проектировании крупных компьютерных ресурсов [1]. От того, насколько удобно записываются, хранятся и извлекаются данных, зависит скорость разработки программного обеспечения. Поэтому в сложившейся обстановке информационных войн крайне важно быстро отвечать на изменения в политиках и процедурах обеспечения безопасности данных. В последние несколько лет все больше компьютерных систем переходит на объектно-ориентированные схемы организации данных [2]. Данный факт позволяет создавать универсальные решения для упрощения и ускорения разработки систем с высокой степенью защиты данных. Автор предлагает нестандартный, но эффективный подход, основанный на использовании встроенных в языки программирования высокого уровня средств аннотирования полей и их валидации. Раскрываемый в докладе метод хорошо зарекомендовал себя при командной разработке нескольких крупных информационных систем.

Предлагаемая схема организации хранения и обработки персональных данных включает в себя несколько инструментов: реляционная база данных, нереляционная база данных, шифратор, дешифратор и валидатор.

Для каждой используемой сущности в работе информационной системы определяются поля, содержащие персональные данные. Для пометки особым статусом необходимо создать специальный атрибут. Далее определенным полям присвоить данный атрибут.

Процесс записи данных включает в себя следующие этапы: валидация модели валидатором, получение случайных асимметричных ключей (открытого и закрытого), рекурсивное прохождение по всем полям модели и поиск по созданному специальному атрибуту, формирование словаря персональных данных типа «ключ-значение», его шифрование и запись в нереляционную базу данных с привязкой по идентификатору, запись остальных полей в реляционную базу данных с привязкой по идентификатору, сохранение открытого ключа в шифраторе, передача закрытого ключа для хранения в дешифраторе.

Процесс извлечения данных включает в себя следующие этапы: получение объекта модели из реляционной базы данных, получение закрытого ключа объекта модели, получение словаря шифрованных персональных данных типа «ключ-значение» из нереляционной базы данных, расшифровка его закрытым ключом, рекурсивное присваивание расшифрованных полей модели по ключам, валидация модели валидатором.

Данный подход позволяет также хранить и обрабатывать файловые структуры данных путем интеграции их в нереляционную базу данных, а также быстро отвечать на изменяющиеся политики в части обработки персональных данных.

Список литературы

1. «Концепция защиты персональных данных в информационных системах персональных данных оператора связи» от 28.04.2010 // Официальный интернет-портал правовой информации. – 2016.

УДК 004.056

В.Л. ЕВСЕЕВ[1], А.С. МАМОНТОВ[2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Общество с ограниченной ответственностью «СберТройка», Москва*

РОЛЬ SCA И OSA В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ: АУДИТ УЯЗВИМОСТЕЙ СТОРОННИХ БИБЛИОТЕК ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Целью работы является исследование инструментов SCA (Software Composition Analysis) и OSA (Open Source Analysis), обеспечивающих безопасность компонентов Open Source и приложений с открытыми компонентами [1] путем аудита уязвимостей сторонних библиотек, используемых при разработке программных продуктов. Выполнен анализ существующих уязвимостей и рисков, связанных с использованием компонентов с открытым исходным кодом, а также методов их выявления и устранения. Особое внимание уделено процессам интеграции SCA и OSA в цикл разработки программного обеспечения (ПО) для предотвращения возможных угроз безопасности.

Введение

Современная разработка (ПО) неразрывно связана с использованием сторонних библиотек, особенно компонентов с открытым исходным кодом [2]. Это значительно ускоряет процесс разработки, снижает затраты и позволяет разработчикам использовать проверенные и оптимизированные решения. Однако, использование сторонних библиотек влечет за собой и ряд рисков, и в первую очередь, связанных с безопасностью. Основные угрозы связаны с тем, что сторонние компоненты могут содержать уязвимости, которые могут быть использованы злоумышленниками для проведения кибератак.

Постановка задачи

Система аудита безопасности сторонних библиотек позволяет решать задачи:

– аудит уязвимостей в сторонних библиотеках: SCA и OSA инструменты автоматически выявляют уязвимости в используемых сторонних библиотеках, опираясь на базы данных известных уязвимостей. Это поможет снизить риски, связанные с использованием уязвимого код;

– регулярное обновление библиотек: важно проверять используемые библиотеки на предмет новых версий, содержащих исправления

уязвимостей. SCA и OSA обеспечивают мониторинг и уведомление о выходе обновлений для повышения безопасности приложений;

– оценка рисков использования уязвимых библиотек: SCA и OSA дают оценку критичности выявленных уязвимостей, что позволяет команде разработчиков оперативно реагировать на самые критичные угрозы. Это позволяет расставлять приоритеты при устранении уязвимостей;

– интеграция с CI/CD процессами: для обеспечения безопасности на всех этапах разработки требуется интегрировать SCA и OSA в процессы непрерывной интеграции и доставки (CI/CD).

Пути решения задачи

Для решения задач аудита уязвимостей сторонних библиотек при разработке ПО российские компании необходимо внедрят инструменты анализа безопасности, такие как SCA и OSA. После анализа существующих решений в области автоматизации процесса обнаружения уязвимостей были определены наиболее универсальные и эффективные инструменты. Основное внимание уделялось стоимости внедрения, функциональности и способности обнаруживать уязвимости в сторонних компонентах.

По итогам анализа предпочтение в использовании целесообразно отдать: 1. OWASP Dependency-Check; 2. CodeScoring; 3. Snyk.

Заключение

Системы аудита безопасности сторонних библиотек, такие как OWASP Dependency-Check, CodeScoring и Snyk, играют важную роль в обеспечении кибербезопасности российских компаний. Эти сканеры безопасности каталогизируют все используемые в приложении компоненты с открытым исходным кодом и показывают имеющиеся в них уязвимости. Это помогает принимать меры для их устранения.

Список литературы

1. Марков А.С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. – 2023. – № 1(53). DOI: 10.21681/2311-3456-2023-1-2-12. (дата обращения: 15.09.2024).

2. Шинкарев А.А. Роль программного обеспечения с открытым исходным кодом в современной разработке корпоративных информационных систем // Компьютерные и информационные науки. – 2021. – № 1. DOI: 10.14529/ctcr210202. (дата обращения: 15.09.2024).

УДК 004.056

А.М. РУСАКОВ
МИРЭА – Российский технологический университет, Москва

ИССЛЕДОВАНИЕ СЕРВИСА НА НАЛИЧИЕ ЭФФЕКТА ИНФРАСТРУКТУРНОГО ДЕСТРУКТИВИЗМА НА ПРИМЕРЕ ТЕСТОВОЙ БАЗЫ ДАННЫХ «DVD RENTAL» ДЛЯ БАЗЫ ДАННЫХ POSTGRESQL

В статье приводятся результаты экспериментального исследования времени ответов на последовательности запросов к базе данных и определении ситуаций, в которых сервис перестает выполнять свои функции. Вводится понятие инфраструктурного деструктивизма и проводится оценка его эффекта для разных версий PostgreSQL: 12.20, 13.16 и 14.12. В результате показано что эффект инфраструктурного деструктивизма имеется и наиболее

Введение

Стремительное применение цифровых технологий во всех сферах современной жизни сопровождается таким же стремительным и быстрым ростом компьютерных атак. Решение вопросов обеспечения безопасности объектов информатизации при этом сопровождается необходимостью учета постоянного усложнения и изменения архитектур информационных инфраструктур. Одной из важных задач при обеспечении безопасности информационных инфраструктур является оценка эффекта инфраструктурного деструктивизма. Суть данного эффекта состоит в неконтролируемом саморазрушении инфраструктуры при штатном режиме функционирования сервиса [1].

Постановка задачи

Пусть имеется 3 различные версии системы PostgreSQL: 12.20, 13.16 и 14.12. Для каждой этих версий на одном и том же аппаратном обеспечении восстанавливается тестовый набор данных «DVD RENTAL». Далее формируется 20 тестовых запросов (в данном исследовании запросы были только на чтение). С помощью скрипта на Python в базу данных отправляются разные последовательности запросов. Каждая такая последовательность запросов отправляется в базу данных 100 раз, а результат усредняется. Всего было выполнено 100000 разных последовательностей запросов, для каждой последовательности запросов рассчитано время её выполнения. Результаты оценки времени обработки запросов для PostgreSQL 14.12 представлены в табл. 1.

Таблица 1. Последовательность запросов и время ответа

№.	Последовательность запросов	Время выполнения, с.
1.	4, 3, 10, 5, 13, 6, 12, 7, 11, 9, 1, 14, 15, 0, 8, 2, 16, 17, 19, 18	0,72676
2.	14, 11, 0, 19, 7, 17, 13, 5, 6, 4, 2, 15, 9, 10, 12, 3, 8, 16, 1, 18	0,72991
3.	12, 5, 4, 16, 18, 10, 17, 7, 1, 0, 6, 8, 3, 2, 19, 9, 11, 13, 15, 14	0,74087
4.	2, 9, 17, 11, 3, 18, 6, 8, 0, 1, 4, 14, 5, 16, 15, 7, 12, 10, 13, 19	0,74111
5.	3, 1, 7, 13, 2, 15, 12, 6, 11, 19, 4, 0, 9, 17, 14, 5, 10, 18, 16, 8	0,74566
6.	11, 14, 10, 13, 17, 8, 0, 9, 16, 18, 6, 19, 12, 15, 4, 1, 5, 2, 3, 7	0,84975
7.	6, 10, 2, 18, 13, 15, 14, 12, 0, 17, 8, 5, 3, 1, 9, 7, 11, 19, 16, 4	0,85109
8.	4, 10, 16, 12, 3, 19, 9, 13, 7, 15, 17, 5, 18, 8, 6, 1, 14, 0, 2, 11	0,89897
9.	5, 18, 15, 17, 14, 1, 13, 11, 16, 7, 9, 3, 4, 8, 19, 0, 12, 6, 10, 2	0,92828
10.	5, 8, 13, 3, 9, 19, 4, 16, 17, 18, 11, 1, 12, 14, 6, 15, 7, 10, 0, 2	0,93549

В табл. 1 представлена пример выборки, состоящей из 10 последовательностей запросов и времени выполнения запросов, последовательности запросов отсортированы по времени выполнения, представлены 5 запросов от начала и 5 от конца. Проанализировав данные эксперимента, можно прейти к выводу, что разная последовательность запросов приводит к разному времени выполнению запросов. Таким образом, время выполнения запросов зависит от внутренних параметров инфраструктуры и постоянно для именно этого экземпляра работы сервиса, что подтверждается и в других исследованиях [2, 3].

Заключение

Проанализировав данные исследования, можно оценить степень инфраструктурного деструктивизма сервиса и благодаря этому можно оценить какая инфраструктура лучше и для какой инфраструктуры возможно возникновения эффекта инфраструктурного деструктивизма, а для какой нет.

Список литературы

1. Максимова Е.А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры. Информатизация и связь. 2022. № 1, с. 68–74. DOI http://dx.doi.org/10.34219/2078-8320-2022-13-1-68-74. – EDN^ ZMOPQB

2. Русаков А.М., Горин Д.С., Лисютенко А.С. Интеллектуальный анализ работы хранилища данных Greenplum на основе обработки лог-файлов. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2023. № 6, с. 142–149. DOI: http://dx.doi.org/10.37882/2223-2966.2023.06.31. – EDN: PIRKUE

3. Русаков, А. М. Анализ динамики рисков деструктивного воздействия инфраструктурного генеза. Кибербезопасность: технические и правовые аспекты защиты информации: Сборник научных трудов I Национальной научно-практической конференции, Москва, 24–26 мая 2023 года. М.: МИРЭА Российский технологический университет, 2023, с. 85–87. EDN: FWCTSV.

УДК 004.89

Е.А. КУЗИНА

Национальный исследовательский ядерный университет «МИФИ», Москва

МЕТОДЫ ПОВЫШЕНИЯ ДОВЕРИЯ К ТЕХНОЛОГИЯМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ АТОМНОЙ ЭНЕРГЕТИКИ

Естественным требованием к разрабатываемому ПО мониторинга и контроля состояния АЭС, осложняющим внедрение систем искусственного интеллекта, является безопасность, и, в частности, интерпретируемость, используемых технологий и моделей. Целью данной работы является анализ существующих подходов, способствующих повышению интерпретируемости моделей глубокого обучения. Рассмотрены три направления исследования данной проблемы, проанализированы их современное состояние и перспективы применения в компьютеризации оперативных процедур на АЭС.

Введение

Опыт внедрения систем искусственного интеллекта (ИИ) в атомной энергетике демонстрирует их применение, в основном, в качестве систем поддержки оператора (СПО) по оперативной диагностике оборудования [1–2], что фактически реализует вспомогательную упреждающую функцию. Таким образом, в ответственности оператора частично остается оценка ситуации и полностью – планирование ответных действий. В то же время существуют работы, доказывающие эффективность применения методов ИИ в решении более широкого класса задач [3–4], направленных в том числе на повышение автономности работы АЭС. Препятствием к внедрению таких систем, в частности основанных на глубоком обучении, является недостаточный уровень доверия к ним, одним из факторов которого является низкая интерпретируемость таких моделей.

В данной работе представлен анализ подходов, направленных на повышение интерпретируемости моделей глубокого обучения и применимых в решении задач атомной энергетики.

Подходы к повышению интерпретируемости моделей ИИ

Среди подходов, способствующих повышению интерпретируемости моделей глубокого обучения, можно выделить следующие: применение объяснимого искусственного интеллекта (англ. eXplainable Artificial Intelligence, XAI) [5]; использование гибридных моделей; переход на принципиально новые модели нейронных сетей.

Исследования в области объяснимого ИИ направлены на создание техник верификации «осмысленности» заключений модели, что фактически не совершенствует саму модель в вопросе интерпретируемости.

Гибридизация моделей позволяет вносить ограничения в закономерности, которым обучается модель ИИ. С одной стороны, такой подход позволяет сдерживать модель в рамках некоторой физически обоснованной теории, с другой – может привести к ограничению способности модели по выявлению скрытых признаков для объяснения изучаемых закономерностей, снизить качество модели.

Смена архитектуры или парадигмы обучения нейронных сетей также может стать ключом к обеспечению интерпретируемости моделей. Так, свойства сети Колмогорова-Арнольда (KAN) [6] позволяют решать вопрос интерпретируемости модели на уровне ее архитектуры. Однако обучение KAN на существующих вычислителях затруднено.

Заключение

Исследованы проблемы применения технологии ИИ в задачах атомной энергетики. Проанализированы особенности направлений ИИ, применение которых способно повысить интерпретируемость моделей, а следовательно, способствовать достижению требуемого уровня доверия к технологии для ее распространения в решении задач атомной энергетики.

Список литературы

1. Поваров В.П. Принципы разработки систем принятия решений в задачах управления ядерными блоками. Вестник Воронежского государственного технического университета. 2023, т. 14, № 2, с. 87–91.

2. Сборник «2020-2021 годы: краткие результаты научно-технической деятельности АО «ВНИИАЭС». URL: https://vniiaes.ru/upload/Сборник_ОР_ВНИИАЭС_2020_2021.pdf (дата обращения 14.09.2024).

3. Николаева А.В., Увакин М.А., Пантюшин С.И., Сотсков Е.В., Антипов М.В., Николаев А.Л., Литышев А.В., Безруков Ю.А., Кавун О.Ю., Быков М.А. (АО ОКБ «ГИДРОПРЕСС») Искусственный интеллект в области использования атомной энергии - существующие возможности и перспективы. Вопросы атомной науки и техники. Серия: Физика ядерных реакторов. 2023, № 3, с. 4–16.

4. Huang Q., Peng Sh., Deng J., Zeng H., Zhang Z., Liu Y., Yuan P. A review of the application of artificial intelligence to nuclear reactors: where we are and what's next. Heliyon. 2023, v. 9, p. e13883.

5. Ali S., Abuhmed T., El-Sappagh S., Muhammad Kh., Alonso-Moral J.M., Confalonieri R., Guidotti R., Ser J.D., Díaz-Rodríguez N., Herrera F. Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. Information Fusion. 2023, v. 99, p. 101805.

6. Liu Z., Wang Y., Vaidya S., Ruehle F., Halverson J., Soljacc M., Hou T. Y., Tegmark M. KAN: Kolmogorov-Arnold Networks. ArXiv preprint, 2024. arXiv:2404.19756.

УДК 004.93’1

С.В. КТИТРОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ПРИМЕНЕНИЕ ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ФИНАНСОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Предлагается применение дискретного вейвлет-преобразования для анализа аномалий в потоке данных, представимых вектором параметров. На примере выявления мошеннических транзакций, связанных с банковскими картами, показано, что методика позволяет получить сопоставимые по точности результаты по сравнению с рядом часто используемых подходов, таких как нейронные сети, робастные и регрессионные методы. Особенностью подхода является применение вейвлет-преобразования для формирования профиля отдельной транзакции.

Одним из направлений повышения безопасности программного обеспечения, обрабатывающего финансовые транзакции может быть встраивание в него механизма оценки транзакции на предмет ее мошеннического характера.

Возможность применения вейвлет-преобразования (ДВП), лежащего в основе частотно-временного анализа [1], например, для выявления мошеннических платежей с использованием банковских карт, не очевидна, так как требуется анализировать поток однотипных транзакций, содержащих не связанные между собой данные. Однако каждая такая транзакция содержит сама значительный объем коррелированных параметров, с использованием которых становится возможным построить так называемый профиль транзакции.

Для выявления аномалии предлагается следующий алгоритм. Пусть транзакция T_i представлена набором параметров $\{V_{1,i},...,V_{M,i}\}$. Применив к T_i вейвлет-преобразование, получаем набор коэффициентов $C_i = \{c_1,...,c_M\}$, включающий коэффициенты наивысшего уровня разложения, по которым определяем энергию $E_i = \sum_{k=1}^{M} c_k^2 / M$ текущей транзакции и среднее значение $\overline{E}$ по предыдущим наблюдениям на заданную глубину. Если $\left|\overline{E} - E_i\right| > \Delta$, то транзакция T_i признается аномальной и исключается из дальнейших вычислений (Δ – некоторое пороговое значение, выбираемое эмпирически).

Применение в реальном времени упрощает пирамидальный алгоритм Малла, вычислительная сложность которого может быть охарактеризована как $O(M)$. Для тестирования алгоритма использовался публичный реальный набор данных, содержащий сведения о транзакциях с кредитными картами [2]. Из 30 атрибутов каждой транзакции были выбраны 8, что существенно снизило сложность вычислений.

Тестирование проводилось с использованием вейвлетов Хаара и вейвлетов Добеши различных порядков с объемом выборки предыдущих подлинных транзакций равным 3000. Для оценки качества классификации был применен коэффициент корреляции Мэтьюса.

Сравнение результатов тестирования проводилось с [3], в которой использовался тот же набор данных, и в которой применялись следующие алгоритмы классификации: случайные леса, метод опорных векторов, метод логистической регрессии, деревья решений, случайные деревья, многослойный персептрон, наивный байесовский классификатор, градиентное дерево, одноуровневое дерево принятия решений, нейронная сеть прямого распространения, глубокое обучение с использованием стохастического градиентного спуска с обратным распространением, линейная регрессия. Также была проведена классификация с использованием робастной оценки параметра положения на основе медианы обучающей выборки. Применение вейвлетов различных типов дало практически совпадающие значения.

Наилучших результатов по балансу верных и ложных обнаружений показали нейронная сеть и метод опорных векторов. Однако ДВП позволяет достичь сопоставимых результатов при малых вычислительных затратах, что позволяет встраивать предлагаемую методику в программное обеспечение, формируя дополнительный рубеж контроля. При этом ценой увеличения ложных срабатываний выбором параметра порога Δ можно получить наивысший процент правильно обнаруженных аномалий при числе ошибок, не превышающих 0.5%.

Список литературы

1. Mallat S. A Theory for Multiresolution Signal Decomposition: The Wavelet Representation. IEEE Trans. on Pattern Analysis and Machine Intelligence. 1989. vol. 11. no. 7. p. 674–693.

2. Credit Card Fraud Detection. https://www.kaggle.com/mlg-ulb/creditcardfraud (дата обращения 17.09.2024).

3. Randhawa K., Loo C.K., Seera M., Lim C.P., Nandi A.K. Credit Card Fraud Detection Using AdaBoost and Majority Voting. IEEE Access. 2018. vol. 6. P. 14277-14284. doi: 10.1109/ACCESS.2018.2806420.

УДК 004.056

В.С. КИРЕЕВ
Национальный исследовательский ядерный университет «МИФИ», Москва

СОВРЕМЕННЫЕ МЕТОДЫ ФЕДЕРАТИВНОГО МАШИННОГО ОБУЧЕНИЯ

Федеративное обучение (Federated Learning, FL) как новая парадигма в искусственном интеллекте машинном обучении, находится на стыке задач доверенного искусственного интеллекта и конфиденциальных вычислений, и подразумевает различные формы отказа от централизации данных и переноса обучения непосредственно на границу пользовательского устройства. В данном. докладе автором представлены результаты обзора основных методов FL, обеспечивающих баланс между конфиденциальностью, производительностью, точностью, стоимостью накладных расходов федеративного обучения.

Введение

Федеративное обучение позволяет нескольким клиентам совместно обучать модель машинного обучения, используя преимущества различных наборов данных от клиентов без обмена своими локальными обучающими наборами данных. Дискуссии по применению конфиденциальных вычислений получили особенное развитие после 8 августа 2024 г., когда был подписан закон с новыми правилами обработки обезличенных персональных данных [1]. Например, при участии Ассоциации ФинТех (АФТ) обсуждаются вопросы конфиденциального обмена данными для построения моделей скоринга и антифрода. К сожалению, FL все еще имеет ряд проблем, связанных с конфиденциальностью и безопасностью, описываемые далее.

Конфиденциальное федеративное обучение

Риски атак на конфиденциальность в FL возникают, когда центральный сервер или другие участники получают доступ к параметрам модели, совместно используемым на этапах обучения или агрегирования.

Рис. 1. Подходы к конфиденциальному федеративному обучению

Кроме того, вредоносные клиенты могут вступить в сговор друг с другом, чтобы украсть данные, модели у обычных клиентов или испортить глобальную обучающую модель. Для снижения этих рисков применяются методы, которые можно обобщенно сгруппировать, как на рис. 1:

На основе шифрования. Данные методы используют безопасные многосторонние вычисления (Secure Multi-Party Computation, SMPC) [2], например, с использованием доверенных анклавов (Trusted Execution Environments, TEE) и гомоморфное шифрование (Homomorphic Encryption, HE) [3, 4].

На основе возмущения. Эти методы в целом делятся на две категории: локальная дифференциальная конфиденциальность (LDP), реализуемая на стороне клиента, и глобальная дифференциальная конфиденциальность (GDP) [4], организуемая на стороне сервера. Эти методы вносят контролируемый шум или рандомизацию в обновления модели перед их объединением.

На основе блокчейна. Методы на основе блокчейна используют серию неизменяемых блоков данных с временными метками, управляемых распределенной сетью компьютеров, что исключает зависимость от одного контролирующего лица [3].

Гибридные методы применяют интеграцию шифрования, возмущения и технологии блокчейн, что позволяет создать комплексную защиту конфиденциальности [3].

Заключение

В докладе автором рассмотрены современные конфиденциальные методы федеративного обучения, основанные на шифровании, на основе блокчейна, на основе возмущений, и гибридные подходы. Описаны их достоинства и недостатки.

Список литературы

1. Федеральный закон № 233-ФЗ [Электронный ресурс]. URL: https://www.garant.ru/hotlaw/federal/1746724/ (дата обращения: 13.09.2024).

2. Предварительный национальный стандарт № 845-2023. Техническая структура федеративной системы машинного обучения [Электронный ресурс]. URL: https://www.garant.ru/hotlaw/federal/1746724/ (дата обращения: 13.09.2024).

3. Mo F., Haddadi H., Katevas K., Marin E., Perino D., Kourtellis N.. Privacy-preserving federated learning with trusted execution environments. Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services (2021), p. 94–108

4. Запечников С.В. Конфиденциальное машинное обучение на основе трехсторонних протоколов безопасных вычислений. Безопасность информационных технологий, 2022, № 1 (29), с. 30–43. DOI: http://dx.doi.org/10.26583/bit.2021.4.03.

УДК 004.05

Д.В. ДЕМИДОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ЦЕНА РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Рассматриваются вопросы уместности разработки безопасного программного обеспечения и объёмы накладных расходов в сравнении с заказной разработкой.

Подходы к производству программного обеспечения

Производители программного обеспечения тяготеют к одному их двух полюсов: разработка на заказ (проектный подход) и вендорство (продуктовый подход). Где-то между этими полюсами располагается платформенный подход. При этом компании первой группы могут дрейфовать в сторону продуктового подхода, обобщая и капитализируя свой опыт в некую платформу, а компании-вендоры под давлением серьёзных заказчиков зачастую злоупотребляют заказной разработкой и отклоняются от курса.

В заказной разработке требования к работам и результату определяются контрактом с заказчиком, причём трудоёмкая верификация результата является обязанностью заказчика. При разработке продукта производитель ориентируется на своё понимание потребностей рынка, а в целях снижения рисков заказчиков вендор может подтверждать соответствие заявляемым требованиям путём добровольной сертификации.

Уместность разработки безопасного программного обеспечения

Безопасность программного обеспечения требует формального подтверждения путём получения соответствующих лицензий на компанию-производителя и сертификации изделия, партии или серийного производства. Без такого подтверждения декларация производителя может расцениваться в лучшем случае как реклама, а в худшем как намеренное введение в заблуждение. Таким образом, разработка безопасного ПО уместна тогда, когда заказчик готов приобретать только сертифицированный продукт. В остальных случаях затраты на подтверждение безопасности ПО вряд ли будут оправданы. Кроме того, если сертификат выдаётся на продукт, то лицензируется деятельность в целом. Это значит, что выпуск и сертификация каждого последующего

продукта будет обходиться дешевле в удельном выражении, так как расходы на лицензирование и организацию безопасной разработки уже понесены.

Расходы на разработку безопасного программного обеспечения

Для организации разработки безопасного ПО производителю требуется:

1. Лицензировать во ФСТЭК деятельность по разработке и производству средств защиты конфиденциальной информации, а также деятельность по технической защите конфиденциальной информации. Это обходится порядка 3 млн. руб. и требует наличия аттестованного помещения со спецоборудованием и нескольких штатных сотрудников в отделе информационной безопасности. Проще, если в организации уже внедрена система менеджмента качества и разработаны регламенты управления разработкой.

2. Приобрести специальные программные средства для проведения различных видов тестирования, предусмотренных в безопасной разработке: средства статического анализа кода (проверка на известные уязвимости), динамического анализа кода (имитация атак), фаззинг-тестирования. Может обойтись порядка 10 млн. руб.

3. Ввести в процесс производства процессы тестирования, обработки результатов (разметки найденных сканерами уязвимостей на ложно-положительные и истинно-положительные), устранения уязвимостей (поиск патчей, написание патчей, пересборка пакетов), документирования процессов разработки безопасного ПО. Это дополнительные человекомесяцы (в зависимости от объёма продукта). При широком использовании ПО с открытым исходным кодом в составе разрабатываемого продукта трудоёмкость устранения уязвимостей может взрывоопасно вырасти, а процесс сборки версий продукта усложнится. Использование бинарных пакетов других производителей может вовсе поставить крест на сертификации продукта.

В ходе сертификации продукта документальные свидетельства процессов разработки безопасного ПО выступают основой для подтверждения соответствия требованиям доверия. Расходы на сертификацию складываются из оплаты труда выбранной испытательной лаборатории и назначенного ФСТЭК органа по сертификации (несколько млн. руб. суммарно). Последующие процедуры инспекционного контроля новых версий продукта обходятся сильно дешевле, так как охватывают только изменения продукта.

УДК 004.05

Д.В. ДЕМИДОВ

ООО «БАЗИС», Москва

ТРЁХМЕРНАЯ МОДЕЛЬ ПРЕДСТАВЛЕНИЯ СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматриваются вопросы выбора свода требований для сертификации программного продукта, анализа применимости в информационных системах, предварительной оценки сложности аттестации.

Связь процессов сертификации и аттестации

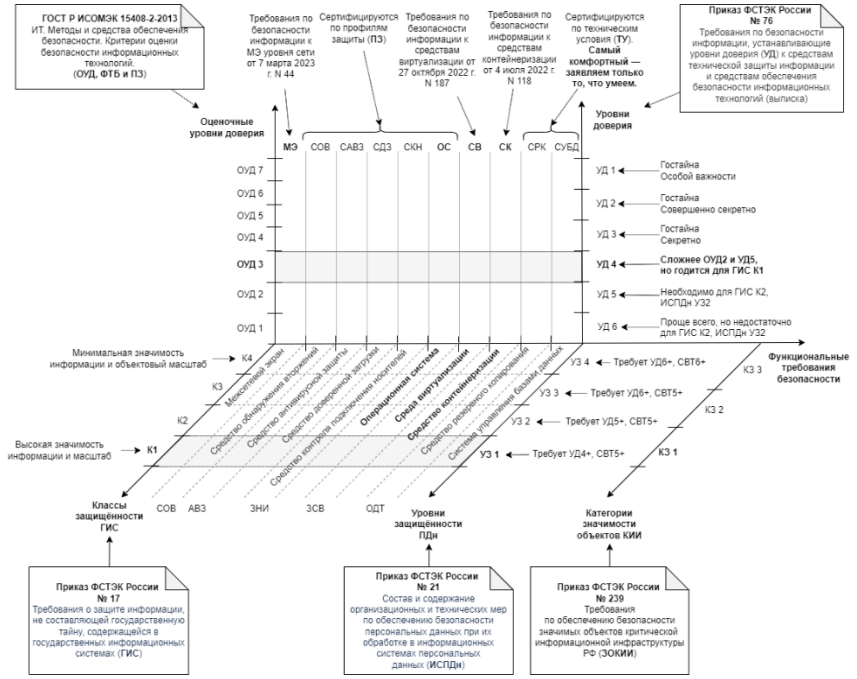
В работе рассматривается свод нормативной документации, применяемой при сертификации средств защиты информации (СЗИ) по линии ФСТЭК России. Сам программный продукт в случае такой сертификации расценивается как СЗИ, однако часть его функций может и не относиться к функциям безопасности. Кроме того, продукт может быть комплексным и иметь черты сразу нескольких классов СЗИ, определённых ФСТЭК России. Тогда объём сертификационных испытаний и документации соответствующим образом возрастает.

Приобретаемый заказчиком программный продукт может являться составной частью аттестуемого программно-аппаратного комплекса, который в свою очередь может составлять основу информационной системы (ГИС, ИСПДн или ЗО КИИ). Наличие сертификата на продукт кардинально облегчает аттестацию, поскольку снимает с заказчика необходимость доказательства соответствия требованиям к СЗИ. Чем больше требования к аттестации пересекаются с требованиями к СЗИ, тем проще провести аттестацию.

Заказчик может и не планировать аттестацию, а коммерческий заказчик не обязан использовать сертифицированные продукты, однако наличие сертификата позволяет снизить риски приёмки и эксплуатации системы на базе такого продукта.

Система координат сертификации СЗИ

Ниже представлена система координат, осями которой являются функциональные требования и требования доверия, дополненная осью категорий защищённости информационных систем.



Сертифицированный программный продукт будет занимать в этом пространстве некоторую область, не обязательно связную. Например, платформа виртуализации может быть сертифицирована одновременно и как средство виртуализации, и как операционная система, если она базируется на гипервизоре первого типа, и как межсетевой экран, по уровню доверия 4 в соответствие с Приказом № 76 ФСТЭК России, что соответствует оценочному уровню доверия 3 по ГОСТ Р ИСОМЭК 15408, и следовательно пригодна для применения в ГИС всех классов защищённости вплоть до К1, в ИСПДн всех уровней защищённости вплоть до УЗ 1, и в ЗО КИИ вплоть до 1 категории значимости. Трудоёмкость подобной сертификации описана, например, в [1].

Данная модель позволяет сравнивать СЗИ и оценивать перспективу аттестации и остаточную трудоёмкость реализации мер защиты.

Список литературы

1. Demidov D.V. A systematic approach to describing the source code of a cloud platform with assured security. 5th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2017, p. 31–36.

УДК 004.056.5

М.С. ЮРИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СИСТЕМАХ УПРАВЛЕНИЯ ИДЕНТИФИКАЦИЕЙ: НОВЫЕ ГОРИЗОНТЫ БЕЗОПАСНОСТИ

В условиях растущей киберугрозы системы управления идентификацией (IDM) нуждаются в улучшении безопасности и эффективности. Данная статья рассматривает возможности применения искусственного интеллекта (ИИ) для решения этих задач. В работе анализируются ключевые применения ИИ в IDM, такие как улучшенная аутентификация, авторизация, предотвращение несанкционированного доступа, а также оптимизация процессов управления идентификацией. В статье также рассматриваются вызовы и перспективы развития ИИ в IDM.

Введение

В условиях растущих киберугроз, традиционные системы управления идентификацией (IDM) сталкиваются с трудностями в обеспечении надежной защиты данных. Искусственный интеллект (ИИ) предлагает решение этой проблемы, повышая безопасность и эффективность IDM за счет улучшения обнаружения угроз, автоматизации задач, персонализации доступа и усовершенствования защиты от мошенничества.

Пути улучшения IDM при помощи ИИ

ИИ предлагает новые возможности для IDM. Он может анализировать поведение пользователей, их местоположение, тип устройства и другие факторы, чтобы строить динамические правила авторизации, предоставляя доступ только к необходимым ресурсам и минимизируя риски. Использование ИИ в IDM обеспечивает следующие преимущества [1]:

Аутентификация: ИИ позволяет создавать более надежные методы аутентификации, чем традиционные логин/пароль. Например, многофакторная аутентификация с использованием одноразовых паролей, биометрических данных и анализа поведения пользователя [2].

Авторизация: ИИ делает авторизацию более динамичной, учитывая контекст доступа пользователя (местоположение, тип устройства, поведение в системе), предоставляя только необходимый доступ и минимизируя риски.

Предотвращение несанкционированного доступа: ИИ анализирует поведение пользователей, выявляя аномалии, которые могут свидетельствовать о попытке несанкционированного доступа. Также ИИ

учится на данных о прошлых атаках, чтобы предсказывать и блокировать новые угрозы.

Для достижения высокого уровня безопасности в IDM используются конкретные методы ИИ, такие как:

Машинное обучение: выявление аномалий в поведении пользователей, что позволяет предсказывать и блокировать возможные угрозы. Например, методы обучения с учителем анализируют прошлые случаи атак и создают модели для предотвращения несанкционированного доступа [3].

Глубокие нейронные сети (Deep Learning): анализ сложных моделей поведения пользователей, что улучшает надежность биометрической аутентификации, включая распознавание лиц и отпечатков пальцев [4].

Алгоритмы обработки естественного языка (NLP): анализ текстовых данных, используемых для авторизации, например, при проверке ответов на вопросы безопасности или при анализе содержимого сообщений для выявления фишинга.

Заключение

В статье рассмотрено применение ИИ в системах управления идентификацией (IDM) для повышения их безопасности и эффективности. Ключевыми направлениями использования ИИ являются аутентификация, динамическая авторизация, обнаружение угроз и оптимизация процессов управления идентификацией. Также были рассмотрены вызовы, связанные с безопасностью данных, прозрачностью решений и этическими аспектами. Несмотря на эти трудности, ИИ открывает новые горизонты для улучшения IDM в условиях изменяющегося киберпространства.

Список литературы

1. «Ethical Considerations in Artificial Intelligence: A Guide for Policymakers and Businesses» // Brookings Institution, 2023. – URL: https://www.brookings.edu/research/ethical-considerations-in-artificial-intelligence-a-guide-for-policymakers-and-businesses/ (дата обращения 12.06.2024).

2. ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация. // Позитив текнолоджиз, 2020. – URL: https://docs.cntd.ru/document/1200130318 (дата обращения 12.06.2024).

3. Narayana, P., & Saxena, A. (2020). AI-Driven Cybersecurity in Identity Management Systems: A Comprehensive Review. International Journal of Computer Science. // Informational Fusion 97, 2023 – С. 16–19

4. Соков Б.Б. Создание прототипа системы биометрической аутентификации по геометрии лица с помощью методов машинного обучения //Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2018. – С. 175–179.

УДК 681.5:621.039

В.Н. САМАНЧУК

Национальный исследовательский ядерный университет «МИФИ», Москва

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ РЕАКТОРОВ ТИПА РБМК ПУТЕМ РАЗРАБОТКИ ВЫСОКОТОЧНОГО ЦИФРОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАСЧЕТА ПОЛЕЙ ЭНЕРГОВЫДЕЛЕНИЯ В АКТИВНОЙ ЗОНЕ

Целью настоящей работы является совершенствование штатного программного обеспечения энергетических реакторов типа РБМК. Предлагается замена используемых численных методов на высокоточную цифровую обработку реакторных данных, позволяющая снизить среднеквадратическую погрешность вычисления поля энерговыделения в активной зоне реактора примерно в два раза.

Безопасное программное обеспечение (ПО) систем контроля и управления сложных технических объектов, например, энергетических ядерных реакторов типа РБМК, должно отвечать двум основным требованиям. Во-первых, оно должно иметь защиту от хакерских атак и внедрения вредоносного ПО и, во-вторых, обеспечивать надежное и безопасное функционирование подобных объектов. Например, для реакторов РБМК-1000 одним из основных факторов, влияющих на безопасность их эксплуатации, является точность расчета поля энерговыделения в активной зоне (АЗ) [1, 2]. Трудности в решении этой задачи обусловлены значительной пространственной неравномерностью поля энерговыделения, большим количеством (около 1500) тепловыделяющих сборок (ТВС) в активной зоне реактора и редкой сеткой установленных детекторов контроля энерговыделения - ДКЭ(р), размещенных менее, чем в 10% всех ТВС реактора [1, 2]. В результате в штатном алгоритме при вычислении поля энерговыделения используются не только сигналы ДКЭ(р) – $N^{д}(r_j)$, но и результаты периодически выполняемого нейтронно-физического расчета (НФР) мощности каждой ТВС – $\tilde{N}(r)$. При этом учитывается, что погрешность НФР в области низших пространственных частот может достигать десятков процентов [3], а погрешность калибровки большинства ДКЭ(р) невелика и обычно не превышает 2%. В результате основным расчетным блоком штатного алгоритма оперативного вычисления оценок мощности ТВС является модуль коррекции результатов НФР, работающий следующим образом [2]:

Вначале для всех ДКЭ(р) вычисляются коэффициенты коррекции физрасчета в местах установки датчиков – $V_j^{д} = N^{д}(r_j)/\tilde{N}(r_j)$. Затем дискретное поле коэффициентов $V_j^{д}$ аппроксимируется на все ячейки активной зоны эмпирическим выражением вида:

$$\tilde{V}(r_j) = a_1 r_j^3 + a_2 r_j^2 + a_3 r_j + a_4 + a_5 r_j^2 \sin\varphi_j + a_6 r_j \sin\varphi_j + a_7 r_j^2 \cos\varphi_j + a_8 r_j \cos\varphi_j , \quad (1)$$

где r_j и φ_j – полярные координаты j-ого ТК, a_i – константы, определяемые по методу наименьших квадратов [2].

Ограниченность набора из восьми пробных функций в соотношении (1) приводит к заметной погрешности аппроксимации, достигающей 10–15%. Для ее уменьшения в штатном алгоритме в дальнейшем используется оптимальная статистическая интерполяция, в результате чего среднеквадратичная погрешность оценок мощности ТВС по штатному алгоритму равна ~ 5% [1, 2].

Для ее заметного уменьшения в настоящей работе предлагается учесть регулярную пространственную сетку размещения ТВС и ДКЭ(р) в активной зоне реактора и вместо метода наименьших квадратов применить к отсчетам $V_j^{д}$ двумерный цифровой интерполяционный фильтр [4, 5], обеспечивающий погрешность интерполяции ~ 0.2% для всех ТВС реактора РБМК-1000. В результате замены штатного модуля коррекции НФР на высокоточную цифровую обработку среднеквадратичная погрешность оценок мощности ТВС составляет ~ 3% для всех профилей полей энерговыделения в активной зоне.

Таким образом, переход от классических численных методов к высокоточной цифровой обработке позволяет значительно повысить качество оперативного контроля не только полей энерговыделения, но и рассчитываемых на их основе других параметров активной зоны реактора, определяющих безопасность и эффективность его работы.

Список литературы

1. Доллежаль Н.А., Емельянов И.Я. Канальный ядерный энергетический реактор. М.: Атомиздат, 1980.

2. Филипчук Е.В., Потапенко П.Т., Постников В.В. Управление нейтронным полем ядерного реактора. М.: Энергоиздат, 1981.

3. Горюнов В.К. Перекосы поля нейтронов в реакторах при случайно распределенных возмущениях макросечений. – Атомная энергия, 1980, т. 49, вып. 5, с. 321–323.

4. Каппелини В., Константинидис А., Эмилиани П. Цифровые фильтры и их применение. Пер. с англ. М.: Энергоатомиздат, 1983.

5. Даджион Д., Мерсеро Р. Цифровая обработка многомерных сигналов. М.: Мир, 1988.

УДК 004.056

А.В. ТРИФОНЕНКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ПРИНЦИПЫ РАЗРАБОТКИ ПРОГРАММНЫХ СРЕДСТВ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ АЭС

В атомной энергетике контролирующие организации предъявляют чёткие требования к критически важному для безопасности программному обеспечению. В данной работе изучена общая структура требований к программным средствам, важным для безопасности атомных электростанций, на примере международных стандартов, требования проанализированы в контексте современного рынка информационных технологий, рассмотрены частные примеры программного обеспечения, отвечающего стандартам, с целью формирования новых практик и стандартов в различных сферах информационных технологий.

Современный рынок информационных технологий перенасыщен решениями для разработки программного обеспечения (ПО). Всё больше программных систем разработки проектируется с учётом необходимости предотвращения ошибок, вызываемых человеческим фактором.

Существующие своды принципов и рекомендаций к разработке ПО, выработанные крупными инженерными компаниями, направлены, в основном, на оптимизацию масштабирования, сокращение затрат на подготовку специалистов, зависят от конкретного языка программирования, применяемого фреймворка или архитектуры программной системы. Принципы, разработанные отдельными специалистами в индустрии, разрозненны, и не всегда применимы к произвольному программному проекту.

С целью выявления универсальных практик, подходящих для разработки отказоустойчивого ПО, было решено изучить стандарты, применяемые в сферах, где безопасность и отказоустойчивость имеют высшую ценность [1] по сравнению с отдельными потребительскими свойствами, а также в которых на этапе проекта предполагается закладывать значительные средства на обеспечение безопасности и отказоустойчивости ПО.

Требования к разработке программных средств, важных для безопасности атомной электростанции (АЭС), сформулированы Международной электротехнической комиссией (МЭК) в стандартах IEC 60880 и 62138. Аналогичные российские стандарты зафиксированы Росстандартом, как ГОСТ Р МЭК 60880-2010 [2] и 62138-2021 [3], и

являются переводными версиями соответственных документов МЭК. Разделы этих документов регламентируют многие аспекты проектирования, написания и трансляции программных средств [4], некоторые из которых могут представлять интерес для разработчиков ПО, применяемого и в менее критичных с точки зрения безопасности и отказоустойчивости сферах.

Общие требования к проектам программного обеспечения, согласно стандарту, предусматривают поэтапное следование процессам управления проектом, обеспечения и контроля качества ПО, управления конфигурацией, обеспечения защищённости и верификации ПО.

Кроме того, стандарт описывает принципы выбора языков программирования, программных инструментов и вспомогательных средств, предупреждения отказов и изготовления документации.

Были выделены и отдельно рассмотрены некоторые частные примеры требований стандартов, для них был проведён сравнительный анализ с известными мировыми практиками и принципами разработки ПО. Также требования соотнесены с принципами работы современных языков программирования и известных фреймворков. Приведены некоторые примеры реализации рассмотренных стандартов в атомной отрасли [5].

Список литературы

1. Development of Safety-Critical Systems. Architecture and Software. / G. Karmarkar, A. Wakankar, A. Kabra, P. Pandya. – Кам, Швейцария: Springer, 2023. – 498 с. – ISBN: 978-3-031-27900-3. – DOI: https://doi.org/10.1007/978-3-031-27901-0.

2. ГОСТ Р МЭК 60880-2010. Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А. – М.: Стандартинформ, 2011. – 90 с.

3. ГОСТ Р МЭК 62138-2021. Программное обеспечение систем контроля и управления атомной станции, выполняющих функции безопасности категории В и С. – М.: Российский институт стандартизации, 2022. – 46 с.

4. J. Lahtinen и др. Comparison between IEC 60880 and IEC 61508 for Certification Purposes in the Nuclear Domain // Computer Safety, Reliability, and Security29th International Conference: . Proceedings, Vienna, Austria, September 2010. – Вена, Австрия, 2010. – С. 55–67. – ISSN 0302-9743. – DOI: https://doi.org/10.1007/978-3-642-15651-9_5.

5. SimInTech: среда динамического моделирования технических систем / Б.А. Карташов, Е.А. Шабаев, О.С. Козлов, А.М. Щекатуров. – М.: ДМК-Пресс, 2017. – 424 с. – ISBN: 978-5-97060-482-3.

Направление

Теоретическая и практическая криптография

Руководитель секции – ПУДОВКИНА М.А.,
д.ф.-м.н., профессор

УДК 519.7

М.А. ПУДОВКИНА

Национальный исследовательский ядерный университет «МИФИ», Москва

О БУМЕРАНГ-МАТРИЦАХ НАД АБЕЛЕВЫМИ ГРУППАМИ

Для оценки параметров атак на основе метода бумеранга над полем $GF(p^n)$ применяются бумеранг-матрицы. В настоящей работе в связи с исследованием различных групп наложения ключа рассматриваются свойства бумеранг-матриц над произвольными конечными абелевыми группами. В качестве иллюстрации полученных результатов приведены характеристики бумеранг-матриц криптографических преобразований над аддитивной группой кольца Z_{2^n}.

В последние годы при изучении криптографических параметров подстановок блочных шифрсистем относительно различных методов криптоанализа, кроме «традиционных» разностных и корреляционных матриц, над аддитивными группами поля $GF(p^n)$ и n-мерного векторного пространства $V_n(p)$ над полем $GF(p)$ рассматриваются: матрица бумеранга [1]; матрица ω-бумеранга; матрица бумеранга для преобразования Фейстеля [2]; бумеранг-разностная матрицу для преобразования Фейстеля [3]. В настоящей работе данные матрицы рассматриваются над произвольной конечной абелевой группой $(X,+)$ с нейтральным элементом 0_X.

В связи с исследованием различных групп наложения ключа для подстановки $s \in S(X)$ введем бумеранг-матрицу $\mathbf{b}(s) = \left(b_{\varepsilon,\lambda}(s)\right)$, бумеранг-разностную матрицу $\mathbf{b}^{(F)}(s) = \left(b^{(F)}_{\varepsilon,\lambda}(s)\right)$, бумеранг-разностную матрицу $\mathbf{bd}^{(F)}(s) = \left(bd^{(F)}_{\varepsilon,\lambda,\tau}(s)\right)$ блочной шифрсистемы с раундовой функцией на основе преобразования Фейстеля над произвольной конечной абелевой группой $(X,+)$, элементы которых для каждых $\varepsilon,\gamma,\tau \in X \setminus \{0_X\}$ задаются соответственно условиями

$$b_{\varepsilon,\lambda}(s) = \left|\left\{\alpha \in X \mid ((\alpha+\varepsilon)^s + \lambda)^{s^{-1}} = (\alpha^s + \lambda)^{s^{-1}} + \varepsilon\right\}\right|,$$

$$b^{(F)}_{\varepsilon,\lambda}(s) = \left|\left\{\alpha \in X \mid (\alpha+\varepsilon)^s - \alpha^s = (\alpha+\varepsilon+\lambda)^s - (\alpha+\lambda)^s\right\}\right|,$$

$$b^{(F)}_{\varepsilon,\lambda,\tau}(s) = \left|\left\{\alpha \in X \mid (\alpha+\varepsilon)^s - \alpha^s = (\alpha+\varepsilon+\lambda)^s - (\alpha+\lambda)^s\right\}\right| = \tau\Big|.$$

Эти матрицы характеризуют «качество» S-боксов относительно соответственно метода бумеранга, бумеранг-разностного и бумеранг-разностного для блочных шифрсистем, у которых раундовая функция основана на преобразовании Фейстеля.

Исследование различных групп наложения ключа приводит к необходимости рассмотрения различного вида эквивалентностей S-боксов (см. [3]). Так, обобщением аффинной-эквивалентности и расширенной аффинной эквивалентности преобразований над векторным пространство $V_n(p)$ может являться голоморф-эквивалентность на абелевой группе $(X,+)$. Назовем подстановки $s_1, s_2 \in S(X)$ *голоморф-эквивалентными* на абелевой группе $(X,+)$, если существуют такие преобразования $a_1, a_2 \in \mathrm{Hol}(X,+)$, что $s_2 = a_1 s_1 a_2$. Показано, что если подстановки $s_1, s_2 \in S(X)$ являются голоморф-эквивалентными, то бумеранг-матрицы $\mathbf{b}(s_1)$, $\mathbf{b}(s_2)$ отличаются только перестановкой строк и столбцов. Также получены верхние оценки элементов бумеранг-матрицы:

1) $b_{\varepsilon,\lambda}(s) \le |X|$ для всех $s \in S(X)$, $\varepsilon, \gamma \in X \setminus \{0_X\}$;

2) $b_{\varepsilon,\lambda}(s) = |X|$ для всех $h \in \mathrm{Hol}(X,+)$, $\varepsilon, \gamma \in X \setminus \{0_X\}$.

В качестве иллюстрации полученных результатов приведены характеристики бумеранг-матриц криптографических преобразований над аддитивной группой кольца Z_{2^n}. Также введена обобщенная бумеранг-матрица $\mathbf{b}^{[t]}(s)$ на t-граммах. Для ряда подгрупп $H \le S(X)$ получены значения элементов матрицы $\mathbf{b}^{[t]}(s)$ для $s \in H$.

Список литературы

1. Cid C., Huang T., Peyrin T., Sasaki Y., Song L. Boomerang connectivity table: a new cryptanalysis tool. Eurocrypt 2018, LNCS, vol. 10821, p. 683–714, 2018.

2. Boukerrou H., Huynh P., Lallemand V., Mandal B., Minier M. On the feistel counterpart of the boomerang connectivity table introduction and analysis of the FBCT. IACR Transactions on Symmetric Cryptology, 2020(1), p. 331–362 (2020).

3. Mesnager S., Mandal B., Msahli M. Survey on recent trends towards generalized differential and boomerang uniformities. Cryptography and Communications, 2022, Vol. 14, p. 691–735.

УДК 519.7

Д.А. БУРОВ[1], С.В. КОСТАРЕВ[2]

[1]*Лаборатория ТВП, Москва*

[2]*ФСРБИТ, Москва*

ПОСТРОЕНИЕ МАКСИМАЛЬНО РАССЕИВАЮЩИХ МАТРИЦ С НЕТРИВИАЛЬНОЙ ГРУППОЙ АВТОМОРФИЗМОВ

Предлагается подход к построению максимально рассеивающих (MP) матриц путем случайного выбора из классов матриц с нетривиальной группой автоморфизмов. Описаны свойства группы автоморфизмов MP-матриц. Экспериментально показано, что доля MP-матриц в классах с большей группой автоморфизмов может существенно увеличиваться.

Напомним, что $A \in (\mathrm{F}_{2^r})_{n,n}$ называется MP- или MDS-матрицей (см., например, [1]), если линейный код с порождающей матрицей $(E_{n\times n}, A)$ является МДР-кодом. Задача построения MP-матриц является актуальной в связи с обеспечением стойкости алгоритмов блочного шифрования относительно линейного и разностного методов анализа. Существует ряд подходов к построению MP-матриц [1]. Через S_n обозначим симметрическую группу подстановок степени n. Определим действие S_n^2 на $(\mathrm{F}_{2^r})_{n,n}$: $g = (g_1, g_2) \in S_n^2$ действует на $A = (a_{i,j}) \in (\mathrm{F}_{2^r})_{n,n}$ по правилу $A^g = A^{(g_1,g_2)} = (a_{g_1(i),g_2(j)})$.

Ряд используемых на практике максимально рассеивающих матриц являются достаточно структурированными: циркулянтные матрицы (AES, Shark, Whirlpool), матрицы Адамара (Khazad, Anubis). Эта структурированность может быть формализована с помощью следующего понятия.

Определение 1. *Группой автоморфизмов матрицы* $A \in (\mathbb{F}_{2^r})_{n,n}$ *назовем такую подгруппу* $Aut(A) < S_n^2$, *что для любого* $g \in Aut(A)$ *имеет место равенство* $A^g = A$.

Пусть $G < S_n \times S_n$. Тогда через G_1, G_2 обозначим проекции группы G на первую и вторую координаты соответственно. A является циркулянтной тогда и только тогда, когда $\{(g,g) \mid g \in Z_n^+\} < Aut(A)$. A является матрицей

является матрицей Адамара тогда и только тогда, когда группы $Aut(A)_1$, $Aut(A)_2$ содержат группу $\{(g,g) \mid g \in (Z_2^+)^n\} < Aut(A)$.

Основная идея работы – повышение вероятности случайного выбора МР-матриц за счет увеличения группы автоморфизмов.

Теорема 2. *Пусть* $A \in GL(n,2^r)$ *МР-матрица,* $G = Aut(A)$. *Тогда справедливы следующие утверждения.*

1. $G_1 \cong G_2$.

2. Для любой подстановки $(g_1, g_2) \in G$, $g_1, g_2 \neq \varepsilon$, *выполнено* $|fix(g_1)|, |fix(g_2)| \leq 1$.

3. Цикловые структуры подстановок $g_1 \in G_1$, $g_2 \in G_2$, *где* $(g_1, g_2) \in G$, *совпадают и имеют один из следующих видов:* $[1, s^{n-1/s}]$, $\left[t^{n/t}\right]$.

4. Если G_1 *и* G_2 *транзитивные группы, то* G_1 *и* G_2 *группы Фробениуса и подстановочно изоморфны.*

Следствие 3. *Пусть* n *четное число,* $A \in (\mathbb{F}_{2^r})_{n,n}$ *МР циркулянтная матрица. Тогда* $Aut(A)_1 = Aut(A)_2 = Z_n^+$.

Результаты экспериментов приведены в табл. 1, где $B = \mathrm{diag}(2,2)$.

Таблица 1. Число МР-матриц в случайной равновероятной выборке матриц из $(\mathrm{F}_{2^s})_{n,n}$ объёма 10^5 с группой автоморфизмов $Aut(A) = \{(g,g) \mid g \in G\}$, $G < S_n$

n	G	Число МР-матриц
7	Z_7^+	29050
7	D_7	64497
9	Z_9^+	0
9	D_9	373
9	$Z_3^+ \times Z_3^+$	0
9	$\langle Z_3^+ \times Z_3^+, B \rangle$	448

Список литературы

1. Gupta K. C., Pandey S. K., Ray G. I., Samanta S. Cryptographically significant mds matrices over finite fields: A brief survey and some generalized results. Advances in Mathematics of Communications. 2019, № 13(4), p. 779–843.

УДК 004.056

М.В. ПОЛЯКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

Московский государственный технический университет им. Н.Э. Баумана

ООО «Код Безопасности», Москва

СЛОЖНОСТЬ ПОИСКА СКРЫТЫХ ЛИНЕЙНЫХ СТРУКТУР НА КВАНТОВОМ КОМПЬЮТЕРЕ

Работа посвящена анализу сложности описка скрытых линейных соотношений групп подстановок с помощью квантового компьютера. Приводится алгоритм, использующий квантовое преобразование Фурье и представления некоммутативных групп. Показывается, что предложенный метод полиномиален по числу запросов к квантовому оракулу, но полная схема поиска соотношений имеет экспоненциальную сложность.

Алгоритмы квантовых вычислений не единожды применялись к анализу стойкости криптографических схем. В 1994 г. публикация алгоритма Шора [1] показала уязвимость криптосистему RSA и протокола Диффи-Хеллмана. В 1997 г. Лов Гровер опубликовал квантовый алгоритм, который позволяет со сложностью $O(\sqrt{N})$ проводить поиск в неотсортированном массиве размера N. Применение данного алгоритма позволяет снижать сложность атаки полным перебором $n-$ битного ключа: $O(2^{n/2})$ с помощью алгоритма Гровера вместо $O(2^n)$.

Введем определение симметричной шифрсистемы и уравнение зашифрования. Пусть $\mathbb{Z}_2^n$ – множество открытых и шифрованных текстов, $\mathbb{Z}_2^m$ – множество ключей шифрования. Тогда $E: \mathbb{Z}_2^n \times \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ – функция зашифрования. Для выбранного ключа $K \in \mathbb{Z}_2^n$ определим частичную функцию зашифрования $E_K: \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Т.к. функция зашифрования по своему определению функция обратимая, то и частичная функция зашифрования также обратимая (при знании ключа K). В таком случае справедливо следующее $E_K \in S(\mathbb{Z}_2^n)$. Т.е. частичную функцию зашифрования можно рассматривать как некую подстановку, действующую на множестве открытых и шифрованных текстов. Следовательно, задачу поиска линейных структур итеративных функций зашифрования можно интерпретировать как поиск подстановок с определенной линейной структурой.

В соответствии с [3] приведем определение линейной структуры. Пусть $S(\mathbb{Z}_2^n)$ – симметрическая группа, действующая на векторах булевого

куба размерности n. Тогда для булевого вектора $x \in \mathbb{Z}_2^n$ под записью x^g будем понимать образ действия подстановкой $g \in S(\mathbb{Z}_2^n)$ на вектор x. Тогда будем оворить, что подстановка $g \in S(\mathbb{Z}_2^n)$ обладает линейной структурой $(\alpha, \delta) \in (\mathbb{Z}_2^n \backslash \{0\}, \mathbb{Z}_2^n \backslash \{0\})$, если выполняется следующее соотношение

$$x^g \oplus (x \oplus a)^g = \delta, \quad \forall x \in \mathbb{Z}_2^n.$$

Элемент α называется линейным транслятором отображения g. В работе [4] было показано, что множество всех подстановок с линейной структурой обладает групповой структурой:

$$\Pi_{\alpha,\delta} = \{g \in S(\mathbb{Z}_2^n) \mid x^g \oplus (x \oplus a)^g = \delta\}.$$

В той же работе показано, что $\Pi_{\alpha,\delta} = S_2 \wr S_{2^{n-1}}$ где $S_2 \wr S_{2^{n-1}}$ – операция сплетения групп подстановок S_2 и $S_{2^{n-1}}$. Тогда для поиска таких линейных структур можно применить алгоритмы квантовых вычислений.

В работе [5] автором для решения сформулированной задачи был предложен квантовый алгоритм, использующий стандартный подход для задач о скрытой подгруппе. В частности, показано, что сложность алгоритма по числу повторений всей квантовой схемы – $O\left(\sqrt[3]{\frac{1}{|\Pi_{\alpha,\delta}| \log(2^{n!}/\gamma)} \sqrt{\frac{2^{n!}}{[S(\mathbb{Z}_2^n):\Pi_{\alpha,\delta}]}}}\right)$, где γ – некоторое малое положительное число. Однако, основываясь на статье [6], можно предложить алгоритм, полиномиальный по числу запросов к квантовому оракулу, а именно $O(\log^4(2^n!))$

Список литературы

1. P. Shor. Polynomial time algorithms for prime factorization and discrete logarithm on quantum computer. SIAM J. Comput., 26:5, 1997, 1484-1509.

2. Grover, Lov K. (1996-07-01). "A fast quantum mechanical algorithm for database search". Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, p. 212–219.

3. J.H. Evertse. Linear structures in block ciphers. EUROCRYPT'87, Springer-Verlag, 1987.

4. Б. А. Погорелов, М. А. Пудовкина, "Факторструктуры преобразований", Матем. вопр. криптогр., 3:3 (2012), p. 81–104.

5. Polyakov, M., Kluycharev, P. Searching linear structures of permutation groups with quantum computer. J Comput Virol Hack Tech (2024). https://doi.org/10.1007/s11416-024-00523-3.

6. M. Ettinger, P. Hoyer, E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. arXiv:quant-ph/0401083v1.

УДК 519.7

М.А. ПУДОВКИНА, А.М. СМИРНОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АТАКА НА КЛАСС РЕДУЦИРОВАННЫХ XSL-АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

В работе анализируется класс редуцированных XSL-алгоритмов блочного шифрования с алгоритмом развертывания ключа второго порядка и матрицы линейного преобразования, у которой существует хотя бы два равных элемента в одной строке в случае 4, 5 и 6 раундов. При атаке используется подход «йо-йо», методы невозможных разностей и встречи посередине. Получены оценки трудоемкости атаки и вероятности её успеха.

Синтез современных блочных шифров осуществляется в соответствии неформально сформулированными принципами К. Шеннона: перемешивание и рассеивание. С данной точки зрения важным классом для рассмотрения являются XSL-алгоритмы блочного шифрования. Многие современные алгоритмы блочного шифрования являются XSL-алгоритмами, например, AES, «Кузнечик», MIDORI64, 3D.

Пусть $V_n(2^m)$ – n-мерное векторное пространство над полем $\mathbb{F}_{2^m}$, где $n, m \in \mathbb{N}$, $\oplus$ – операция сложения в $V_n(2^m)$, $I(A)$ – индикатор выполнения условия A, $g: V_n(2^m) \times V_n(2^m) \longrightarrow V_n(2^m)$ – раундовая функция XSL-алгоритма блочного шифрования. k – раундовый ключ из $V_n(2^m)$.

Пусть $h = ||h_{i,j}||$ – матрица в стандартном базисе порядка n над полем $\mathbb{F}_{2^m}$ линейного слоя раундовой функции g, $h^{-1} = ||h_{i,j}^{(-1)}||$ – обратная матрица в стандартном базисе порядка n над полем $\mathbb{F}_{2^m}$ линейного слоя раундовой функции g, d – число равных элементов в матрице $h^{-1} = ||h_{i,j}^{(-1)}||$, $s = (s_1, \dots, s_n) \in S(\mathbb{F}_{2^m})^n$. Для произвольного $\alpha = (\alpha_1, \dots, \alpha_n)$ раундовая функция g задается равенством

$$g(\alpha, k) = hs(\alpha \oplus k).$$

Для каждого $i \in \{1, \dots, n\}$ определим отображение $\chi_i: V_n(2^m) \longrightarrow \mathbb{F}_2$ условием

$$\chi_i(\alpha) = I(\alpha_i \neq 0).$$

Положим $\chi(\alpha) = \big(\chi_1(\alpha), \dots, \chi_n(\alpha)\big)$.

Для каждого $\varepsilon^{(i)} = \big(\varepsilon_1^{(i)}, \dots, \varepsilon_n^{(i)}\big) \in V_n(2^m)$ при $i \in \{1, \dots, n\}$, положим

$$\varepsilon_t^{(i)} = I(i = t).$$

Опишем идею атаки на редуцированный XSL-алгоритм блочного шифрования.

Очевидно, что

$$\chi(\alpha^{(1)} \oplus \alpha^{(2)}) = \chi(s(\alpha^{(1)}) \oplus s(\alpha^{(2)})) \quad (1)$$

для всех $\alpha^{(1)}, \alpha^{(2)} \in V_n(2^m)$, $s \in S(V_n(2^m))$.

Теорема 1. *Пусть* $\alpha, k \in V_n(2^m)$ *и существуют такие* $i, j_1, j_2 \in \{1, \dots, n\}$, *что элементы матрицы линейного отображения* h^{-1} *удовлетворяют условиям*

$$(h^{(-1)})_{i,j_1} = (h^{(-1)})_{i,j_2}, (h^{(-1)})_{i,j_1} \neq 0, s_{j_1} = s_{j_2}.$$

Тогда существует такое $\delta \in \mathbb{F}_{2^m}$, *что уравнение*

$$((hs)^{-1}(\alpha \oplus x \cdot \varepsilon^{(j_2)} \oplus k) \oplus (hs)^{-1}(\alpha \oplus \delta \cdot \varepsilon^{(j_1)} \oplus (\delta \oplus x) \cdot \varepsilon^{(j_2)} \oplus k))_i = 0$$

имеет 2^m *решений относительно* $x \in \mathbb{F}_{2^m}$.

Теорема 2. *Пусть* $\alpha, k \in V_n(2^m)$ *и существуют такие* $i, j_1, j_2 \in \{1, \dots, n\}$, *что элементы матрицы линейного отображения* h^{-1} *удовлетворяют условиям*

$$h_{i,j_1} = h_{i,j_2}, h_{i,j_1} \neq 0, s_{j_1} = s_{j_2}.$$

Тогда существует такое $\delta \in \mathbb{F}_{2^m}$, *что уравнение*

$$(hs(\alpha \oplus x \cdot \varepsilon^{(j_2)} \oplus k) \oplus hs(\alpha \oplus \delta \cdot \varepsilon^{(j_1)} \oplus (\delta \oplus x) \cdot \varepsilon^{(j_2)} \oplus k))_i = 0$$

имеет четное число решений относительно $x \in \mathbb{F}_{2^m}$.

На основании модификаций равенства (1), алгоритма построения невозможных разностей в [2], теорем 1 – 3 предложена атака на класс редуцированных XSL-алгоритмов блочного шифрования в случае 4,5,6 раундов. Доказано, что для 4 раундов трудоемкость атаки составляет $(2^m - 1)^2 + 2^{n(m+2)}$, для 5 раундов – $2^{m(n-1)} + 2^{nm}$, для 6 раундов –

$$7 \cdot 17^{n-2} \cdot 2^{2nm-n+2} \cdot 10^{1-n} \cdot \left(1 - \frac{n}{2^m - 1}\right)^d$$

операций зашифрования. Вероятность успеха атаки равна 1 в случае 4 и 5 раундов, 0.7 – в случае 6 раундов.

Список литературы

1. Ronjom S., Bardeh N. G., and Helleseth T.Yoyo tricks with AES // ASIACRYPT 2017. Lect. Notes Comput. Sci. 2017. V. 10624. No. 1. P. 217–243.

2. Shen X., Liu G., Sun B. and Li C. Impossible differentials of SPN-ciphers // LNS 2017. V. 10143. P. 47–63.

3. Altawy R. A meet in the middle attack on reduced round Kuznyechik. // IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2015.

УДК 519.7

М.А. ПУДОВКИНА, С.В. СВЕТЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ РАЗНОСТНОЙ ХАРАКТЕРИСТИКИ В НЕКОТОРЫХ КОНЕЧНЫХ ГРУППАХ

В работе экспериментально исследуется наибольший элемент матрицы переходов разностей для случайного биективного отображения и подстановок, применяемых в различных алгоритмах шифрования. Разностная характеристика рассматривается над группами, представимыми прямым произведением групп, используемых в криптографии.

Развитие общего подхода [1] в работе [2], позволило построить атаки на блочные шифры Midori и Scream при помощи введенной разностной характеристики (аффинная равномерность). Одной из задач, возникающих в таких исследованиях, является изучение этой характеристики для нелинейного компонента шифра (S-блока).

В статье [3] проведено экспериментальное исследование разностной характеристики биективных отображений относительно различных групп. В настоящей работе предлагается рассмотрение дифференциальной характеристики в конечных группах, являющихся прямым произведением некоторых групп, естественных для криптографической практики [4].

Пусть $s: G \to G$ – биективное отображение, $\mathrm{q}^{(\circ,\circ)}(s) = \| q_{\epsilon,\delta}^{(\circ,\circ)}(s) \|$ – матрица переходов разностей, элементы которой заданы условием

$$q_{\epsilon,\delta}^{(\circ,\circ)}(s) = |\{\alpha \in G: s(\alpha \circ \epsilon) = s(\alpha) \circ \delta\}|,$$

$$(G,\circ) = (H_1,*_1) \times (H_2,*_2),$$

$$(H_i,*_i) \in \{(V_{2^{m/2}},\oplus), (Z_{2^{m/2}},+), (Z_{2^{m/2}+1},\odot), (H_1,*_1) \neq (H_2,*_2)\}.$$

Будем рассматривать значение $q^{(\circ,\circ)}(s) = \max\{ q_{\epsilon,\delta}^{(\circ,\circ)}(s) : \epsilon,\delta \in G^{\times} \}$. В табл. 1 приведены значения характеристики для 8-битных подстановок, используемых в различных шифрах.

Для каждого случая была сгенерирована выборка из 1000000 8-битных подстановок. Для каждой выборки рассчитано выборочное среднее значение характеристики. Результаты экспериментов приведены в табл. 2.

Таблица 1. Значение характеристики для известных S-блоков

S-box	$(\oplus,+)$	$(+,\oplus)$	$(\oplus,\odot)$	$(\odot,\oplus)$	$(+,\odot)$	$(\odot,+)$
AES	5	6	7	8	7	7
BelT	6	7	8	8	7	8
Fantomas	16	20	32	16	9	8
iScream	20	16	20	12	9	9
Kalyna pi0	7	8	7	7	8	7
Kalyna pi1	6	7	8	7	7	7
Kalyna pi2	8	7	7	8	7	7
Kalyna pi3	7	7	8	9	7	7
Khazad	8	8	10	10	11	14
Kuznechick	8	7	7	8	8	7
Liliput_AE	10	9	12	9	12	8
Picaro	6	7	6	10	9	13
SMS4	8	7	8	8	9	8
Safer	32	16	224	8	28	11
Scream	10	15	12	10	8	7
Snow 3G	8	8	8	8	7	8
TEA1	10	10	8	10	7	8
TEA2	10	12	8	12	7	7
ZUC_S0	8	12	16	8	9	7
ZUC_S1	7	6	6	7	7	7

Таблица 2. Выборочное среднее значение характеристики

$(\oplus,+)$	$(+,\oplus)$	$(\oplus,\odot)$	$(\odot,\oplus)$	$(+,\odot)$	$(\odot,+)$
8,231	8,240	8,231	8,241	7,281	7,280

Список литературы

1. Wagner D., “Towards a Unifying View of Block Cipher Cryptanalysis”. In: Roy, B., Meier, W. (eds) Fast Software Encryption. FSE 2004. Lecture Notes in Computer Science, vol 3017. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-25937-4_2

2. Baudrin J., Felke P., Leander G., Neumann P., Perrin L., Stennes L., “Commutative Cryptanalysis Made Practical”. 2023. *IACR Transactions on Symmetric Cryptology* 2023 (4): 299-329. DOI: https://doi.org/10.46586/tosc.v2023.i4.299-329.

3. Власова В.В., Пудовкина М.А. “О свойствах максимального элемента матрицы вероятностей переходов разностей биективного отображения относительно различных групповых операций”, *ПДМ. Приложение*, 2019, № 12, p. 203–205, DOI: https://doi.org/10.17223/2226308X/12/57.

4. Погорелов Б.А., Пудовкина М.А., “О группах, порождённых преобразованиями смешанного типа и группами наложения ключа”, *ПДМ. Приложение*, 2016, № 9, p. 14–16, DOI**:** https://doi.org/10.17223/2226308X/9/5

УДК 519.719.2

Д.М. КРАПИВЕНЦЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

МНОЖЕСТВО МАТРИЦ-ЦИРКУЛЯНТОВ, ИНВАРИАНТНЫХ ОТНОСИТЕЛЬНО ГРУППЫ ПОДСТАНОВОК

Криптосистемы исследуются с точки зрения алгебраических свойств. В работе рассматриваются свойства алгебраических структур, возникающих в ряде современных криптосистем, использующих преобразования, построенные с использованием циклического сдвига. В работе приведен пример изоморфизма групп матриц-циркулянтов и потенциальное применение для анализа криптосистем.

Обозначим через $a \ll r$, $a \in V_n, r \in \mathbb{Z}_n$ операцию циклического сдвига влево двоичного регистра на r бит, через $\bigoplus$ операцию побитового XOR. В современных криптосистемах, например, в хэш-функциях Keccak, SHACAL и алгоритме шифрования SM4 [1] используется преобразование вида $g: a \mapsto a \bigoplus (a \ll r_1) \bigoplus \dots \bigoplus (a \ll r_d)$, $r \in \mathbb{N}, d \in \mathbb{Z}$. Такое преобразование обеспечивает эффективное на практике свойство рассеивания, постулированное К. Шенноном [2]. Свойство рассеивания в криптосистемах в частности отражает распространение влияния одного входного бита на множество выходных бит. Ряд работ направлен на исследование свойств рассеивания [1, 3].

Преобразование g хорошо известно из алгебраической теории кодирования [4]: действие g на регистр, содержащий битовую строку a есть действие циркулянтной матрицы над полем $\mathbb{F}_2$ на вектор a. Циркулянтная матрица является матрицей, порожденной первой строкой элементов $(c_0, c_1, \dots, c_{n-1})$, циклически сдвигаемой на каждой последующей строке. Также широко применяется изоморфизм, сопоставляющий циркулянтной матрице элемент кольца $R \cong \mathbb{F}_2[x]/(x^n - 1)$, что часто используется в циклических кодах. Исследование циркулянтов часто сводится к исследованию свойств мультипликативной группы кольца R, которую обозначим как R^*. Действие циркулянтов на вектора эквивалентно умножению их представлений в кольце R.

Группу циркулянтов R^* составляет множество обратимых матриц-циркулянтов. Критерий обратимости циркулянтов известен, например, из [4]: циркулянт C обратим тогда и только тогда, когда его соответствующее

представление $c \in R$ в кольце многочленов взаимнопросто с $x^n - 1$: $(c, x^n - 1) = 1$.

Групповая структура R^* известна из работы [5], где выведена формула получения групповой структуры матриц-циркулянтов произвольного порядка $n \in \mathbb{N}$ над произвольным конечным полем $\mathbb{F}_{p^q}$, p – простое, $q \in \mathbb{N}$. Группа R^* является абелевой и представляется в виде прямого произведения циклических групп.

Через b обозначим многочлен $x^{n-1} + \cdots + x + 1 \in R$. Для произвольного поля $\mathbb{F}$ очевидно разложение $x^n - 1 = (x - 1)(x^{n-1} + \cdots + x + 1) = (x - 1) \times b$ многочлена, по которому факторизуется кольцо $R \cong \mathbb{F}_p[x]/(x^n - 1)$. Рассмотрим кольцо $\mathbb{F}_p[x]/(x^{n-1} + x^{n-2} + \cdots + x + 1)$, которое обозначим через $\bar{R}$, а его мультипликативную группу через $\bar{R}^*$. В работе был произведен поиск взаимосвязи между $R \cong \mathbb{F}_p[x]/(x^n - 1)$ и $\bar{R} \cong \mathbb{F}_p[x]/(x^{n-1} + x^{n-2} + \cdots + x + 1)$.

Верно утверждение об изоморфизме групп $\theta: R^* \cong \bar{R}^*$, если n – нечетное и $p \nmid n$. Данное утверждение верно для полей $\mathbb{F}_p$ простого порядка. Изоморфизм θ задается через отображение $a \mapsto a - b$. Данный изоморфизм множества циркулянтов R сохраняет инвариантом групповую структуру мультипликативной группы.

Полученное соотношение можно использовать для анализа рассеивающих свойства отображения g, построенного на циклических сдвигах, в некоторых криптосистемах, в которых порядок циркулянтов подходит под условия утверждения. Например, в алгоритме Keccak преобразование, обозначенное через π сводится к действию произведения циркулянтов $C_1 \otimes C_2$, где один из циркулянтов подходит под критерий утверждения.

Список литературы

1. Крапивенцев Д.М., Пудовкина М.А. Рассеивающие свойства преобразований, заданных комбинацией циклических сдвигов, в различных алгебраических структурах. Теоретическая и прикладная криптография, 2023, с. 119–126.

2. Словарь криптографических терминов. / Под ред. Б.А. Погорелова и В.Н. Сачкова. М.: МЦНМО, 2006. – 94 с.

3. Давыдов С. А., Шкуратов Ю. Д. Использование матриц-циркулянтов над $\mathbb{F}_2$ при построении эффективных линейных преобразований с высокими показателями рассеивания. Математические вопросы криптографии, т.15, № 2, с. 29–46, 2024.

4. Мак-Вильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки: пер. с англ. – М.: Связь, 1979. – 744 с.

5. Sharma R.K., Yadav P. Unit group of algebra of circulant matrices. International Journal of Group Theory, 2013, v. 2, № 4, p. 1–6. 2013.

УДК 519.719.2

А.С. ТИССИН

ООО «Центр сертификационных исследований», Москва

ЧИСЛО ПОЯВЛЕНИЙ ЭЛЕМЕНТОВ НА ОТРЕЗКАХ УСЛОЖНЕНИЙ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В данной работе рассматривается последовательность v, полученная усложнением $v(i) = f(v_1(i), \dots, v_r(i)), i \geq 0$, где v_j – последовательности, построенные по правилу $v_j(i) = f_j\left(u_{j1}(i), \dots, u_{jk_j}(i)\right), i \geq 0,\ j \in \overline{1,r}$, $u_{j1}, \dots, u_{jk_j}$ – линейные рекуррентные последовательности над полем P с характеристическим многочленом $F_j(x)$, $f_j(x)$ и $f(x)-$ сбалансированные функции. Изучается величина $N_l(z, v)$, равная количеству появлений элементов $z \in P$ среди элементов $v(0), v(1), \dots, v(l-1)$; получены ее нетривиальные оценки к шифрам $GEA-1$ и $GEA-2$.

Введение

Пусть $P = GF(q) -$ конечное поле из q элементов, где $q = p^t$, $p -$ простое число, N – множество натуральных чисел. Пусть $u_{js} = (u_{js}(i))_{i=0}^{\infty} -$ линейная рекуррентная последовательность (ЛРП) над полем P с характеристическим многочленом F_j(x) для всех $j \in \overline{1,r}$, $s \in \overline{1,k_j}$, где $r \in$ N и $k_j \in$ N.

Определим отображение μ_c: $P^k \to C^*$, где $c \in P$, равенством

$$\mu_c(\vec{x}) = \chi_c(\mathrm{f}(\vec{x})),\ \vec{x} \in P^k,$$

где $\chi_c -$ аддитивный характер поля P.

Кривизной функции f: $P^k \to P$ назовём следующую величину [3]

$$\sigma(f) = \max_{c \in P} \sum_{\vec{c} \in P^k} \left|\nu_{\mu_c}(\vec{c})\right|,$$

где $\nu_{\mu_c} -$ коэффициенты при разложении μ_c по базису характеров группы P^k.

В работе изучается величина $N_l(z, v)$, равная количеству появлений элемента $z \in P$ среди элементов $v(0), v(1), \dots, v(l-1)$, где $l -$ произвольное натуральное число.

Оценки частот появлений элементов на отрезках усложнений ЛРП

Теорема 1. *Пусть $F_1(x), F_2(x), \dots, F_r(x) -$ реверсивные многочлены степеней m_1, m_2, …, m_r над полем $P = GF(q)$ соответственно, причем многочлены $F_i(x)$ и $F_j(x)$ взаимно просты для всех $i \neq j$. Пусть*

$$\vec{u} = \left(u_{j1}, u_{j2}, \dots, u_{jk_j}\right)$$

– устойчивая система ЛРП с характеристическим многочленом $F_j(x)$ *для любого* $j \in \overline{1,r}$, *функции* $f, f_1, f_2, \dots, f_r -$ *сбалансированы,* $v -$ *последовательность, определённая по правилу (2). Тогда для любого элемента* $z \in P$ *при* $l \leq T(F)$ *справедлива оценка*

$$\left|N_l(z,v) - \frac{l}{q}\right| \leq \frac{q-1}{q}\sigma(f)\, C_l(F) \prod_{j=1}^{r}\sigma(f_j),$$

где F(x) =$\prod_{j=1}^{r} F_j(x)$.

Применение теоремы к шифрам GEA-1 и GEA-2

Для шифра $GEA-1$ [5] применим теорему 1 для оценки частот $N_l(z,v)$ появления элемента $z \in P$. При всех $l < (2^{31} - 1)(2^{32} - 1)(2^{33} - 1)$ и $z \in P$

$$\left|N_l(z,v) - \frac{l}{2}\right| < 1{,}8 \cdot 2^{60}.$$

Для шифра $GEA-2$ [5] применим теорему 1 для оценки частот $N_l(z,v)$ появления элемента $z \in P$. При всех $l < (2^{29} - 1)(2^{31} - 1)(2^{32} - 1)(2^{33} - 1)$ и $z \in P$

$$\left|N_l(z,v) - \frac{l}{2}\right| < 1{,}63 \cdot 2^{78}.$$

Список литературы

1. Камловский О.В. Количество появлений элементов в выходных последовательностях фильтрующих генераторов. Прикладная дискретная математика. 2013, № 21(3), с. 129–145.

2. Камловский О.В Неабсолютные оценки для неполных тригонометрических сумм от линейных рекуррент и их приложения. Математические вопросы криптографии. 2014, № 65(2), с. 17–34.

3. Логачев О.А., Федоров С.Н., Ященко В.В. Оценки для числа появлений знаков на отрезках рекуррентной последовательности над конечным полем, Дискретная математика. 2018, № 30(1), с. 39–55.

4. Глухов М.М., Елизаров В.П., Нечаев А.А., Алгебра, Лань, Санкт-Петербург, 2022, 608 с.

5. Christof Beierle and Patrick Derbez and Gregor Leander and Gaetan Leurent and Havard Raddum and Yann Rotella and David Rupprecht and Lukas Stennes, “Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2”, Cryptology ePrint Archive, 2021 https://eprint.iacr.org/2021/819.

УДК 519.7

Д.А. ЗАХАРОВ, М.А. ПУДОВКИНА

Национальный исследовательский ядерный университет «МИФИ», Москва

О СЛАБОСТЯХ КЛАССОВ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ ФЕЙСТЕЛЯ К АТАКЕ МЕТОДОМ НЕВОЗМОЖНЫХ РАЗНОСТЕЙ

Работа посвящена обзору атак на классы алгоритмов блочного шифрования Фейстеля методом невозможных разностей и исследованию слабостей алгоритмов, которые привели к возникновению атаки. В результате для алгоритмов приведены актуальные данные по числу раундов атаки и используемых слабостей.

Метод невозможных разностей, предложенный в 1999 г. в [1], является одним из эффективных методов анализа алгоритмов блочного шифрования. Он позволяет частично восстановить секретный ключ на основе невозможной разностной характеристики. Метод был применен практически ко всем существующим алгоритмам шифрования.

В работе выполнен анализ работ, опубликованных с 2010 г. в открытой литературе по атакам методом невозможных разностей с функциями усложнения типа XSL, SP и SPS на алгоритмы блочного шифрования Фейстеля и их обобщения 1-го типа с 4 ячейками.

В табл. 1 приведены алгоритмы блочного шифрования Фейстеля и указаны известные характеристики (число анализируемых раундов, тип функции усложнения, используемые для атаки слабости) метода невозможных разностей.

В результате исследования получено, что наиболее слабыми блоками алгоритмов шифрования Фейстеля сбалансированных и 1-го типа с 4 ячейками с функциями усложнения типа SP, SPS и XSL по отношению к методу невозможных разностей являются алгоритм развертывания ключа и линейный слой.

Таблица 1 — алгоритмы шифрования Фейстеля и параметры метода невозможных разностей (α, β — параметры, зависящие от свойств линейного преобразования)

Алгоритм	Тип алгоритма Фейстеля	Тип функции усложнения	Где найдена слабость?	Число раундов
LBlock	Сбалансированный	XSL	Развертывание ключа	23 [2]
Camellia	Сбалансированный	XSL	Развертывание ключа	14 [3]
MIBS	Сбалансированный	XSL	Развертывание ключа	15 [4]
ESF	Сбалансированный	XSL	Развертывание ключа	15 [5]
Lici-2	Сбалансированный	XSL	Развертывание ключа	25 [6]
SM4-SP	1-ый тип	SP	Линейный слой	12 [7]
MARS-SP	1-ый тип	SP	Линейный слой	11 [7]
CAST-SP	1-ый тип	SP	Линейный слой	$20 + \alpha$ [8]
MARS-SPS	1-ый тип	SPS	Линейный слой	12 [8]
CAST-SPS	1-ый тип	SPS	Линейный слой	$20 + \beta$ [8]
GRANULE	Сбалансированный	XSL	Линейный слой	∞ [9]

Список литературы

1. Biham E., Biryukov A., Shamir A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials //Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18. – Springer Berlin Heidelberg, 1999. – С. 12–23.

2. Chen J. et al. Impossible differential cryptanalysis of LBlock with concrete investigation of key scheduling algorithm //Cryptology ePrint Archive. – 2014.

3. Boura C., Naya-Plasencia M., Suder V. Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon (full version) : дис. – IACR Cryptology ePrint Archive, 2014.

4. Cheng L., Xu P., Wei Y. New related-key impossible differential attack on MIBS-80 //2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS). – IEEE, 2016. – С. 203–206.

5. Wu X. et al. Impossible Differential Cryptanalysis on ESF Algorithm with Simplified MILP Model //KSII Transactions on Internet & Information Systems. – 2021. – Т. 15. – №. 10.

6. Zhang K. et al. Related-Key Multiple Impossible Differential Cryptanalysis on Full-Round LiCi-2 Designed for IoT //Security and Communication Networks. – 2022. – №. 1. – С. 11.

7. Cui T., Jin C., Ma J. A new method for finding impossible differentials of generalized Feistel structures //Chinese Journal of Electronics. – 2018. – Т. 27. – №. 4. – С. 728–733.

8. Shen X. et al. Revisiting impossible differential distinguishers of two Generalized Feistel Structures //Security and Communication Networks. – 2021. – Т. 2021. – №. 1. – С. 10.

9. Zakharov D., Pudovkina M. Full round impossible differentials for Feistel ciphers //Journal of Computer Virology and Hacking Techniques. – 2023. – С. 1–6.

УДК 519.7

И.В. МАХОНИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ИССЛЕДОВАНИЕ СВОЙСТВ СИСТЕМЫ АНОНИМНОГО ПОДТВЕРЖДЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ U-PROVE

По мере распространения цифровых технологий в сфере экономики повышаются объемы персональных данных, передаваемых по сети. Особого внимания заслуживает тенденция к росту числа сервисов, требующих от пользователей предоставления личной информации. Существуют методы защищенной передачи персональных данных, однако, нельзя гарантировать их безопасность на стороне сервиса. Одним из решений является использование систем подтверждения персональных данных с нулевым разглашением, к которым относится U-Prove. В данной работе рассмотрены целевые свойства безопасности систем данного класса, исследована атака на систему U-Prove и приведены рассуждения о возможности применения системы U-Prove для анонимного подтверждения персональных данных.

U-Prove – это криптосистема, предназначенная для выпуска и подтверждения прикладных данных, служащих для подтверждения владением определенным набором атрибутов, без их открытого предоставления или с частичным раскрытием отдельных атрибутов. Актуальное описание криптосистемы представлено в работе [1].

Определяющими криптографическими механизмами системы U-Prove являются схема подписи вслепую, используемая в протоколе выпуска токенов и доказательство с нулевым разглашением, используемое в протоколе предъявления токенов.

Существуют общие свойства безопасности, актуальные для систем схожего типа и описанные в [2]. В работе представлено четыре свойства: корректность, неподделываемость, несвязываемость эмитентов и несвязываемость токенов. Свойство корректности является априорным, поэтому отдельно в данной работе оно рассматриваться не будет.

Свойство несвязываемости токенов не обеспечивается в системе U-Prove. Однако, при необходимости обеспечения несвязываемости сессий подтверждения одного набора атрибутов, предполагается, что возможно выпускать множество токенов и использовать каждый из них однократно.

Также, отдельно можно выделить свойство конфиденциальности атрибутов, поскольку перечисленные ранее свойства не включают в себя

сохранение конфиденциальности данных клиента при выполнении протоколов системы.

Рассмотрим известную атаку на U-Prove и определим нарушаемые свойства безопасности. Атака ROS (Random inhomogeneities in a Overdetermined Solvable system of linear equations) из работы [3] позволяет нарушителю сгенерировать валидный токен на наборе атрибутов клиента после открытия нескольких параллельных сессий выпуска токена, что нарушает свойство неподделвыаемости. Данная атака применима к различным схемам подписи, основанным на схеме подписи Шнорра одной из которых является схема подписи Шаума-Педерсена [4], используемая в U-Prove.

Схему Шаума-Педерсена нельзя заменить в протоколе выпуска токенов U-Prove другой схемой подписи вслепую без дополнительных модификаций. Причина этого заключается в доказательстве Шаума-Педерсена, используемом в протоколе выпуска токенов для обеспечения неподделываемости токена «нечестным» пользователем.

В работе [5] приведена альтернативная схема протокола выпуска токенов U-Prove, стойкая к атаке ROS, использующая матрицы элементов группы простого порядка. Ее стойкость основана на задаче KMDH (Kernel Matrix Diffie-Hellman).

Подводя итоги, можно сказать, что систему U-Prove возможно использовать для анонимного подтверждения персональных данных в сценариях, в которых либо не требуется свойство несвязываемости токенов, либо не предполагается параллельный выпуск большого числа токенов. В противном случае, возможно использовать модифицированную схему из работы [6]. Однако, при ее применении рекомендуется отдельное тестирование производительности системы на конкретных параметрах.

Список литературы

1. U-Prove Cryptographic Specification V1.1. Revision 5. Microsoft Corporation. DOI: https://www.microsoft.com/en-us/research/project/u-prove/.

2. Kavki S. A., Martin K. M., Putman C., Quaglia E. A. SoK: Anonymous Credentials Security Standardisation Research. 2023, с. 129–151.

3. Benhamouda F., Lepoint T., Loss J., Orr`u M., Raykova M. On the (in)security of ROS. Journal of Cryptology №35, 2020.

4. Chaum D., Pedersen T.P. Wallet databases with observers. Lecture Notes in Computer Science. 1992, с. 89–105.

5. Orru M., Tessaro S., Zaverucha G., Zhu C. Oblivious issuance of proofs. Advances in Cryptology – CRYPTO 2024. 2024, с. 254–287.

УДК 519.7

К.В. АНТОНОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

МИНИМИЗАЦИЯ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ В АЛГЕБРАИЧЕСКИХ АТАКАХ НА КЛАСС SIMON-ПОДОБНЫХ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

Одним из форматов булевых схем являются И-Не графы (And Inverter Graph, AIG), на его основе можно задавать задачи криптоанализа. Представлен подход к применению AIG-минимизации для ускорения анализа алгебраическими методами функций симметричной криптографии. Проведены эксперименты по построению атак на примере алгоритма блочного шифрования Simon. Получены трудоёмкости атак восстановления ключа по подобранным открытым текстам на версии Simon64/32, редуцированные до 11 и 12 раундов.

Алгебраический криптоанализ [1] имеет дело с системами уравнений (алгебраических и логических). В рамках SAT-подхода задача криптоанализа сводится к задаче булевой выполнимости (SAT). Задача SAT – NP-полная [2], однако практические экземпляры SAT в форме КНФ могут решаться эффективно, применяются так называемые SAT-решатели.

Для задач криптоанализа экземпляры SAT можно строить при помощи программ-трансляторов. Промежуточным представлением между алгоритмом симметричного шифрования и КНФ может являться схема из функциональных элементов над базисом $\{\neg,\wedge\}$, называемая И-Не графом (And-Inverter Graph, AIG). В работе применяются алгоритмы AIG-минимизации для построения более компактных КНФ.

Будут описаны атаки на низкоресурсный алгоритм блочного шифрования Simon64/32 [3]. Алгебраическая атака на 12 раундов Simon64/32 описана в [4], однако автор не приводит оценки трудоёмкости атаки. В работе [5] строятся алгебраические атаки на 10 раундов Simon64/32, их трудоёмкость далека от практической.

Построим атаки по подобранным открытым текстам на алгоритм блочного шифрования. Тогда при шифровании k блоков задача сводится к анализу отображения $f_k: \mathbb{Z}_2^n \times \mathbb{Z}_2^{km} \to \mathbb{Z}_2^{km}$, где n и m – размеры ключа и блока в битах.

С помощью транслятора получаем И-Не граф, задающий f_k. Далее фиксируем значения блоков открытого текста и выполняем минимизацию

схемы. После минимизации происходит трансляция в КНФ. В КНФ фиксируем значение шифртекста и подаём на вход SAT-решателю.

В исследовании применялись транслятор Transalg [6], средство минимизации ABC [7] и SAT-решатель kissat [8].

Анализировались версии Simon64/32, редуцированные до 11 и 12 шагов инициализации. Помимо минимизированных представлений задач строились также КНФ без применения минимизации. В табл. 1 и 2 приводятся размеры файлов КНФ и время решения задачи восстановления ключа при различных значениях k для случаев с применением AIG-минимизации и без. Полужирным выделены лучшие трудоёмкости атак.

Таблица 1. Параметры атак на 11 раундов Simon

	Без минимизации		С минимизацией	
k	Размер, Мбайт	Время атаки, сек.	Размер, Мбайт	Время атаки, сек.
10	0,49	>10800	0,59	>10800
20	0,99	2040	2040	2900
50	2,57	3,84	2,70	35,9
100	5,20	**1,74**	5,47	11,9
200	10,9	2,31	11,0	4,60
500	28,9	5,68	27,6	14,6
1000	58,8	6,77	54,2	17,2

Таблица 2. Параметры атак на 12 раундов Simon

	Без минимизации		С минимизацией	
k	Размер, МБ	Время атаки, сек.	Размер, МБ	Время атаки, сек.
100	5,67	>10800	6,19	6250
200	11,9	2720	12,7	3150
500	31,6	3140	32,0	2560
1000	64,2	2500	64,0	**1380**

Список литературы

1. Bard G. Algebraic cryptanalysis. Springer Science & Business Media, 2009.
2. Cook S. The complexity of theorem proving procedures. Third Annual ACM Symposium on Theory of Computing, 1971. P. 151–158.
3. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. The Simon and Speck lightweight block ciphers. 52nd CAD Conference, 2015. P. 175:1–175:6.
4. Raddum H. Algebraic analysis of the simon block cipher family // LATINCRYPT 2015. Springer International Publishing, 2015. P. 157–169.
5. Семёнов А.А., Антонов К.В., Грибанова И.А. Порождение дополнительных ограничений в задачах алгебраического криптоанализа при помощи SAT-оракулов. Прикладная дискретная математика. Приложение. 2021. №. 14. С. 104–110.
6. Otpuschennikov I., Semenov A., Gribanova I., Zaikin O., Kochemazov S. Encoding cryptographic functions to SAT using Transalg system // ECAI 2016. P. 1594–1595.
7. Mishchenko A. ABC. https://github.com/berkeley-abc/abc.
8. Biere A. The Kissat SAT Solver. https://github.com/arminbiere/kissat.

УДК 519.719.2

А.А. МУХОРТОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ СЕМЕЙСТВА 8-РАУНДОВЫХ XSL-АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ МНОГОМЕРНЫМ МЕТОДОМ ВСТРЕЧИ ПОСЕРЕДИНЕ

В работе исследуется семейство XSL-алгоритмов шифрования, основанное на алгоритмах MANTIS и PRINCE, двумерным методом встречи посередине. Предложена атака на 8-раундовые алгоритмы семейства, приведены оценки сложности, необходимый объем памяти и объем материала, включая оценки сложности для оригинальных MANTIS и PRINCE.

Атака двумерным методом встречи посередине является обобщением метода встречи посередине, предложенным в 1977 г. Диффи и Хеллманом [1]. Впервые многомерный метод встречи посередине был предложен применительно к алгоритму KATAN в 2014 г. [2]. Позднее была построена атака методом встречи посередине на алгоритм шифрования PRINCE [3].

PRINCE [4] – низкоресурсный блочный алгоритм шифрования, основанный на XSL-алгоритме шифрования. PRINCE обладает свойством α-отражения, которое определяется как возможность расшифрования шифртекста функцией зашифрования с сопряженным ключом. Раунд шифрования состоит из побитового сложения с раундовым ключом и раундовой константой, подстановки, умножения на матрицу.

MANTIS [5] – низкоресурсный блочный алгоритм шифрования, основанный на алгоритмах PRINCE [4] и MIDORI [6]. От алгоритма шифрования PRINCE MANTIS унаследовал свойство α-отражения и ключевое расписание, а от MIDORI – раундовую функцию.

В работе исследуется обобщенное семейство алгоритмов шифрования, объединяющее алгоритмы MANTIS и PRINCE, а также обобщенное по количеству бит в блоке текста.

В работе проведена модификация атаки, предложенной для алгоритма PRINCE в 2016 г. [3]. Суть атаки состоит в проведении двух атак методом встречи посередине – на первых трех раундах алгоритма и на последних трех. Средние два раунда не используют ключ в соответствии со строением алгоритма шифрования, поэтому в атаке участвуют опосредованно.

Для каждого состояния после трех раундов зашифрования перебираются некоторые биты ключей, после чего происходит встреча после 1.5 раундов зашифрования и 1.5 раундов расшифрования, где и проверяется, удовлетворяют ли ключи условию, что на них был зашифрован данный открытый текст. После отсева ключей, оставшиеся ключи проверяются на второй паре текстов, и остается лишь ключ, на котором было зашифровано сообщение. Таким образом, атака осуществляется с единичной вероятностью.

Временная сложность атаки для алгоритма шифрования выделенного семейства в общем случае при количестве бит в ячейке r и количестве ячеек в блоке текста d варьируется от $2^{r\left(2d-\sqrt{d}\right)}\left(d-\sqrt{d}\right)\cdot d^{-1}\cdot 6^{-1}$ функций зашифрования до $2^{r\left(2d-\sqrt{d}\right)}\left(3d-\sqrt{d}\right)\cdot d^{-1}\cdot 8^{-1}$. Необходимый объем памяти для осуществления атаки варьируется от $2^{r\left(\frac{3}{2}d-2\sqrt{d}\right)}$ до $2^{r\left(\frac{3}{2}d-2\sqrt{d}+3\right)}$ ячеек памяти по $2\cdot \mathrm{r}\left(d-2\sqrt{d}+1\right)$ бит. Необходимый объем материала – 2 пары открытый текст и шифртекст.

Для оригинального 8-раундового MANTIS оценки сложности для атаки многомерным методом встречи посередине предложены в работе впервые, временная сложность алгоритма: $2^{110.8}$ функций зашифрования. Объём памяти: 2^{67} ячеек памяти по 72 бита. Для оригинального PRINCE временная сложность атаки $2^{110.8}$ функций зашифрования. Объем памяти: 2^{65} ячеек памяти по 72 бита, что подтверждает ранее полученные результаты.

Список литературы

1. W. Diffie W. and Hellman M. E., "Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard" // Computer, vol. 10, no. 6, p. 74-84, 1977.
2. Zhu, B., Gong, G. “Multidimensional meet-in-the-middle attack and its applications to KATAN32/48/64” // Cryptography and Communications, 2014.
3. Rasoolzadeh S. and Raddum H., “Cryptanalysis of PRINCE with Minimal Data” // AFRICACRYPT 2016 – vol. 9646, 2016.
4. Borghoff, J. “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications.” // Advances in Cryptology – ASIACRYPT 2012. Lecture Notes in Computer Science, vol. 7658, 2012.
5. Beierle, C. “The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS.” // Advances in Cryptology – CRYPTO 2016. Lecture Notes in Computer Science, vol 9815, 2016.
6. Banik, S. “Midori: A Block Cipher for Low Energy.” // Advances in Cryptology – ASIACRYPT 2015. Lecture Notes in Computer Science, vol. 9453, 2015.

УДК 004.056

П.А. ЧЕЖЕГОВА[1, 3], М.В. ПОЛЯКОВ[1, 2, 3]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Московский государственный технический университет им. Н.Э. Баумана*

[3]*ООО «Код Безопасности», Москва*

ОБЗОР МЕХАНИЗМОВ ШИФРОВАНИЯ СООБЩЕНИЙ С АУТЕНТИФИКАЦИЕЙ – SIGNCRYPTION

Работа посвящена обзору подходов к построению механизмов одновременного шифрования и подписи передаваемых сообщений – Signcryption. Такие механизмы активно используются в различных мессенджерах и групповых протоколах. Сформулированы основные требования безопасности и исследуется возможность применения отечественной и постквантовой криптографии.

Описание алгоритма поиска

В 1997 г. была предложена идея одновременного шифрования и подписи передаваемых сообщений – Signcryption [1]. Основной целью такого механизма было одновременное обеспечение невозможности подделки подписи и нарушения конфиденциальности. Кроме того, по заявлениям авторов, внедрение подобных механизмов сокращает трудоемкость реализуемых преобразований и информационных взаимодействий по сравнению с механизмами Sign-then-encryption. На текущий момент такие схемы можно встретить, например, в мессенджерах [2].

К механизмам подобного рода предъявляется ряд требований:

- Корректность – расшифрование и проверку электронной подписи может осуществить только владелец ключей, соответствующих ключам, использованным при зашифровании и подписи;
- Эффективность – трудоемкость реализации должна быть «ниже», чем у совокупности независимых механизмов, используемых для решения аналогичной задачи конфиденциальной передачи информации с обеспечением свойства невозможности подделки подписи;
- Безопасность – механизм должен обеспечивать следующие свойства:
  - Конфиденциальность;
  - Аутентификация источника сообщения;
  - Невозможность отказа от авторства;
  - Целостность.

- Дополнительные требования:
  - Защита от чтения назад;
  - Всеобщая проверка корректности переданного сообщения.

Первоначально в [1] было предложено два варианта реализации signcryption – SECDSS1 и SECDSS2. В основе обеих реализаций была схема электронной подписи Эль-Гамаля, а также ключевое хэширование. Стоит отметить, что достоинством схем была возможность использования произвольного блочного алгоритма шифрования. Затем были предложены модификации, обеспечивающие возможность всеобщей верификации, а также дополнительные требования безопасности [2–7].

Сейчас к проблемам механизмов signcryption можно отнести:

- Атаки, позволяющие по одному скомпрометированному ключу прочитать все предыдущие сообщения;
- Обеспечивается аутентификация только зашифрованного сообщения;
- Все современные схемы построены на эллиптических кривых, которые не являются квантово стойкими.

Также перспективными являются: использование российских криптографических алгоритмов и построение гибридной схемы на основе личностного шифрования [8].

Список литературы

1. Y. Zheng. Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost(Encryption). Advances in Cryptology - CRYPTO ’97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings, 1997.
2. Bellare, M., Stepanovs, I. (2020). Security Under Message-Derived Keys: Signcryption in iMessage. In: Canteaut, A., Ishai, Y. (eds) Advances in Cryptology – EUROCRYPT 2020. EUROCRYPT 2020. Lecture Notes in Computer Science, vol 12107. Springer, Cham.
3. F. Bao и R. Deng. A signcryption scheme with signature directly verifiable by public key. In: Proceedings of PKC 98, LNCS 1431, Springer-Verlag, 1998, p. 55–59, 1998.
4. Y. Han, X. Yang и Y. Hu. Signcryption based on elliptic curve and its multi-party schemes. In Proceedings of the 3rd ACM International Conference on Information Security, 2004.
5. E. Mohamed и H. Elkamchouchi. Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy. International Journal of Computer Science and Network Security, vol. 9(1), p. 395–398, 2009.
6. F. Amounas, H. Sadki и E. Kinani. An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem. International Journal of Information & Network Security, vol. 2(3), p. 253–259, 2013.
7. M. Toorani и A. Shirazi. An elliptic curve-based signcryption scheme with forward secrecy. Journal of Applied Sciences, vol. 9 (6), p. 1025–1035, 2010.
8. Minh Thuy Truc Pham, Ngoc Ai Van Nguyen, Mei Jiang, Dung Hoang Duong, Willy Susilo. Wildcarded identity-based encryption from lattices. doi.org/10.1016/j.tcs.2021.12.007.

УДК 004.056

В.Г. ИВАНЕНКО[1], И.Д. ИВАНОВА[2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Российский университет транспорта (МИИТ), Москва*

ОПЕРАЦИИ ПО МОДУЛЮ В ПОСТКВАНТОВЫХ СХЕМАХ ПОДПИСИ

Цель исследования: ускорение вычислений над полиномами в постквантовых криптографических системах. Проведен сравнительный анализ алгоритмов приведения чисел по модулю и обоснована применимость алгоритма K-RED в составе постквантовой схемы подписи Falcon. В результате предложен метод ускорения операций генерации ключей и проверки подписей путем синтеза быстрых алгоритмов вычисления числового теоретического преобразования и алгоритма K-RED.

В постквантовой схеме подписи Falcon для создания подписей применяются операции над полиномами в факторкольце, в том числе ресурсоемкое умножение. Для упрощения вычислений может применяться числовое теоретическое преобразование (NTT), в ходе которого коэффициенты преобразованного полинома вычисляются по формуле (1):

$$\tilde{a}_i = \sum_{j=0}^{n-1} a_j \omega^{ij} \; mod \; q, \tag{1}$$

где a – вектор, выражающий исходный полином, q – модуль, по которому производятся вычисления в факторкольце, ω – примитивный корень единицы степени n (по числу коэффициентов полинома).

Для осуществления умножения полиномов используется свойство NTT, выражаемое формулой (2):

$$c = INTT\big(NTT(a) \circ NTT(b)\big), \tag{2}$$

где $INTT$ – обратное преобразование NTT, а $\circ$ – покомпонентное умножение векторов.

Сложность прямого вычисления отрицательно завернутой свертки при помощи NTT составляет $O(n^2)$, потому для достижения сложности $O(n \log n)$ применяются алгоритмы Кули-Тьюки и Джентльмена-Санде для прямого и обратного преобразований соответственно. Однако на

практике существует еще одна проблема: операции по модулю могут быть достаточно затратными при больших значениях порядка q и требовать отдельных алгоритмов ускорения [1].

В эталонной реализации Falcon, представленной на конкурсе NIST, для ускорения операций умножения по модулю в составе NTT используется алгоритм приведения Монтгомери. Данный алгоритм требует приведения величин в форму Монтгомери, что на практике является ресурсоемким. Применение алгоритма приведения по модулю K-RED позволяет ускорить выполнение преобразования NTT в 2 раза [2]. При условии, что модуль, применяемый в алгоритме Falcon, имеет вид:

$$q = 12289 = 3 * 2^{12} + 1. \quad (3)$$

приведение чисел по модулю будет осуществляться при фиксированных параметрах $k = 3, m = 12$ в два шага:

1. Входное число c представляется в виде:

$$v = v_0 + 2^m * v_1. \quad (4)$$

2. Алгоритм возвращает:

$$kv_0 - v_1. \quad (5)$$

Для использования алгоритма K-RED необходимо предварительно вычислить массив масштабированных коэффициентов поворота, а также константы, позволяющие уменьшить в 2 раза количество умножений и приведений по модулю в ходе обратного преобразования NTT [3]. Внедрение алгоритма K-RED в схему подписи Falcon позволяет ускорить операции генерации ключей и проверки подписи в схеме подписи Falcon.

Список литературы

1. Mert A. C. et al. Design and Implementation of a Fast and Scalable NTT-Based Polynomial Multiplier Architecture // 2019 22nd Euromicro Conference on Digital System Design (DSD). 2019, p. 253-260. DOI:10.1109/DSD.2019.00045.

2. Bisheh-Niasar M., Azarderakhsh R., Mozaffari-Kermani M. High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography // In Proceedings of the IEEE symposium on Computer Arithmetic (ARITH). 2021, p. 94–101. DOI: 10.1109/ARITH51176.2021.00028.

3. Иваненко В.Г., Иванова И.Д., Иванова Н.Д. Вычисления над полиномами в постквантовых схемах подписи // Вопросы кибербезопасности. 2024, № 4(62), с. 65–70. DOI: 10.21681/2311-3456-2024-4-65-70.

УДК 004.056.55

С.А. БЫСТРЕВСКИЙ, А.Е. БОРШЕВНИКОВ,
Ю.В. ДОБРЖИНСКИЙ

Дальневосточный федеральный университет, Владивосток

ОБ ОДНОЙ СХЕМЕ КОНФИДЕНЦИАЛЬНОГО СЛОЖЕНИЯ НА ОСНОВЕ ГОМОМОРФНОГО ШИФРОВАНИЯ

В настоящее время исследователи выделяют два подхода к алгоритмам конфиденциальных вычислений: на основе схем разделения секрета и на основе искажения логического контура [1]. Однако данные подходы имеют недостатки и необходимо искать новые способы решения задачи конфиденциальных вычислений [2]. В данной работе предложен алгоритм конфиденциальных вычислений, выполняющий операцию сложения, имеющий в своей основе гомоморфное отображение.

Аддитивный алгоритм конфиденциальных вычислений с использованием гомоморфного отображения можно описать следующим образом.

Пусть $F(x_1, x_2, x_3, \dots, x_N) = \sum_{i=1}^{N} x_i$; $E_{pk}(x)$ – функция шифрования; pk – открытый ключ; $D_{sk}(x)$ – функция расшифрования; sk – закрытый ключ; $\oplus$ – операция с открытыми текстами, которая приводит к сложению закрытых текстов.

Вход: пользователи $P_1, P_2, P_3, \dots, P_N$ с секретными значениями $x_1, x_2, x_3, \dots, x_N$; арбитр A.

Выход: $F(x_1, x_2, x_3, \dots, x_N) = \sum_{i=1}^{N} x_i$

1. A: pk, sk – генерация ключей, где $n \in pk$ – модуль сложения
2. Для i от 1 до N:
   2.1. $A \rightarrow P_i$: pk
3. Для i от 1 до N - 1:
   3.1. Для j от i + 1 до N:
      3.1.1. $P_i \leftrightarrow P_j$: k_{ij} – общий секрет.
      3.1.2. P_i: $x_i = x_i + k_{ij} \pmod n$
      3.1.3. P_j: $x_j = x_j - k_{ij} \pmod n$
4. Для i от 1 до N:
   4.1. $P_i \rightarrow A$: $c_i = E_{pk}(x_i)$
5. A: $M = D_{sk}(c_1 \oplus c_2 \oplus c_3 \oplus \dots \oplus c_N)$

Выход: M

Корректность:

Корректность данной системы следует из следующих рассуждений. Так как на шагах 3.1.2. и 3.1.3. одному значению прибавляется k_{ij}, а от другого отнимается, то общая сумма секретных значений не меняется. Таким образом, $c_1 \oplus c_2 \oplus c_3 \oplus \dots \oplus c_N = E_{pk}(x_1) \oplus E_{pk}(x_2) \oplus E_{pk}(x_3) \oplus \dots \oplus E_{pk}(x_N) = E_{pk}\left(\sum_{i=1}^{N} x_i\right)$. Расшифровав это значение, арбитр получит $\sum_{i=1}^{N} x_i$.

Этапы работы алгоритма:

Данный алгоритм можно рассмотреть по частям.

1. Генерация ключей арбитром.
2. Получение открытых ключей от арбитра для шифрования данных.
3. Маскирование данных. Основной шаг, определяющий безопасность всей схемы. Ниже будет описан подробнее.
4. Шифрование замаскированных данных для арбитра.
5. Вычисление целевой функции арбитром.

Эффективность:

Главную сложность составляет третий шаг, который в свою очередь зависит от алгоритма генерации общего секрета, тем самым сложность составляет $O(N^2)$. Данная оценка допустима.

Заключение

Таким образом, предложенная схема эффективна и удовлетворяет требованиям безопасности, не давая возможности арбитру произвести неверные вычисления, а также устраняя сговор участников. Единственная возможность — это вступить в сговор с арбитром в нужном количестве пользователей. А добиться доверия от арбитра проще. При этом арбитр не является в протоколе главным и приходится лишь посредником, и самостоятельно ничего определить не имеет возможности.

Благодарности

Исследование проведено при финансовой поддержке Минобрнауки России («Грант ИБ МТУСИ») № 40469-08/23-К.

Список литературы

1. Запечников С.В. Конфиденциальное машинное обучение на основе четырехсторонних протоколов безопасных вычислений //безопасность информационных технологий. – 2022. – Т. 29. – №. 2. – С. 46–56.

2. Быстревский С.А., Боршевников А.Е. Об одном алгоритме конфиденциальных вычислений на основе гомоморфного шифрования для проведения аукционных торгов //Молодежь. Наука. Инновации. 2023. Т. 1. С. 143–148.

УДК 519.7

В.С. БУДНИКОВ, К.Л. ГЕУТ, С.С. ТИТОВ

Уральский государственный университет путей сообщения, Екатеринбург

О ВЕСОВОМ СПЕКТРЕ КОДОВ, ПОРОЖДЕННЫХ БЛОК-СХЕМАМИ

Работа посвящена бинарным кодам со свойством однозначного декодирования к ближайшему. Рассмотрена задача порождения таких кодов в проективных плоскостях над полями GF(4) и GF(8).

Задача определения весового спектра линейного кода – классическая сложная задача теории кодирования [1]. Даже определение кодового расстояния и радиуса покрытия некоторых кодов приводят к таким проблемам, которые ещё ждут своего решения. Так, на Олимпиаде NSUCRYPTO [2] поставлена задача описания бинарных кодов со свойством однозначного декодирования к ближайшему (ОДКБ-коды). Отталкиваясь от класса совершенных кодов, естественно ставить задачу исследования кодов, порождаемых множеством кодовых слов, носители которых являются блоками некоторой блок-схемы [3]. В частности, такие блоки могут быть носителями кодовых слов минимального положительного веса Хэмминга. При этом удобно использовать их геометрическую интерпретацию.

В [4] высказана гипотеза, что ОДКБ-коды представляют собою тензорные произведения совершенных кодов, и доказано, что в линейных (бинарных) ОДКБ-кодах минимальные по включению носители битовых строк, декодирующихся не в нуль, образуют циклы некоторого матроида. Очевидно, для совершенных кодов этот матроид – пороговый. Таким образом, одним из путей построения таких кодов может быть конструирование матроидов из блок-схем с дальнейшим их обобщением, согласно [5].

Для блок-схем из списка в [3] удалось непосредственно выяснить, что они не порождают ОДКБ-коды, кроме блок-схем конечных плоскостей, в которых блоками являются множества точек прямых. Так, если взять EG(2,5) – плоскость над GF(5), то через точку проходит 5 + 1 = 6 прямых, чётное число! Поэтому их **XOR** будет вся плоскость, но без этой данной точки. Значит, дополнение будет одноэлементное, так что кодовое расстояние равно **1,** а не 5, и такой код не способен исправлять ошибки.

Согласно [1, с. 168] весовым спектром кода называется совокупность чисел A_i – количество его кодовых слов веса Хэмминга i.

Для аффинной и проективной плоскостей небольшого порядка путём автоматизации перебора всевозможных побитовых сумм по модулю 2 удалось определить весовой спектр линейного кода, порождённого прямыми относительно операции симметрической разности (XOR).

Для проективной плоскости над GF(4) имеем

i	0	5	8	9	12	13	16	21
A_i	1	21	210	280	280	210	21	1

Таким образом, кодовое расстояние равно 5, в соответствии с работой [5].

Для проективной плоскости над GF(8) получаем.

i	16	21	24	25	28
A_i	2 628	56 064	784 896	137 9700	6 671 616
i	29	32	33	36	37
A_i	10596096	29369214	36301440	49056000	49056000
i	40	41	44	45	48
A_i	36301440	29369214	10596096	6671616	1379700
i	49	52	57	64	71
A_i	784896	56064	2628	73	1

Таким образом, эти коды могут быть использованы при помехоустойчивом кодировании, так как их кодовое расстояние равно минимуму веса ненулевых кодовых слов [1, 6], хотя они и не являются ОДКБ-кодами:

Утверждение. Прямые проективных плоскостей над GF(q) при $q = 4$ и при $q = 8$ не порождают ОДКБ-коды.

Список литературы

1. Логачёв О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО. 2004.

2. https://nsucrypto.nsu.ru/archive/2023/round/2/task/7/#data

3. Холл М. Комбинаторика. М.: Мир, 1970. 424 с.

4. Ананичев Д.С., Геут К.Л., Титов С.С. О кодах с однозначным декодированием к ближайшему – Прикладная дискретная математика. Приложение. 2024. № 17. С. 138–140.

5. Ведунова М.В., Геут К.Л., Игнатова А.О., Титов С.С. Преломляющие биекции в тройках Штейнера. Прикладная дискретная математика. Приложение. 2020. № 13. С. 6–8.

5. Коваленко М.Э. О радиусе покрытия линейных кодов, порожденных аффинными геометриями над полем из четырёх элементов. ПДМ №4 (26) 2014.

6. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. М.: Связь, 1979.

УДК 004.056.53

М.А. ГРИШИН[1], И.Ю. КОРКИН[2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*АО «Позитив Текнолоджиз», Москва*

ГИБРИДНАЯ СХЕМА НАПРАВЛЕННОГО ФАЗЗИНГ-ТЕСТИРОВАНИЯ ЯДРА LINUX С ИСПОЛЬЗОВАНИЕМ ИНСТРУМЕНТА SYZKALLER

Предложена новая гибридная схема фаззинг-тестирования, сочетающая статический анализ, профилирование и реализованных инструментов автоматизации. Данный подход в отличие от существующих обеспечил возможность реализации направленного фаззинга ядра Linux без необходимости многократного запуска syzkaller. Экспериментальная оценка показала увеличение покрытия кода и обнаружение большего числа уязвимостей по сравнению с классическим подходом за одинаковое время тестирования.

Существует множество подходов к фаззингу ядра операционной системы [1, 3]. Комбинированные методы или гибридные схемы [2–4, 8] сочетают элементы статического и динамического анализа. В данной работе предлагается способ улучшения схемы направленного фаззинга с использованием статического анализатора [3], а в качестве базового инструмента выбрано средство syzkaller [6], реализующее технологии мутационного и генерационного фаззинга [5].

Предлагаемая схема заключается в односеансовом использовании syzkaller с предварительной обработкой результатов статического анализа для определения целей и восстановления методом профилирования [7] последовательности системных вызовов. Данная последовательность составляет корпус начальных входных данных.

Авторами реализован программный комплекс (фаззинг-система) из трех модулей: FuzzController, SvFilter и SysFinder. FuzzController управляет процессом, инициируя сборку ядра и статический анализ, результаты которого сохраняются в csv-файл. SvFilter обрабатывает этот файл, выделяя функции ядра с критическим уровнем опасности, а SysFinder использует ftrace для записи трасс выполнения и определения последовательности системных вызовов. Утилита FuzzController инициирует сборку ядра с заранее подготовленной конфигурацией и запуск статического анализа.

В рамках исследования проводилось сравнение разработанной фаззинг-системы с популярной реализацией Syzkaller. Время тестирования составило 46 часов для каждого фаззера. По результатам работы статического анализатора были выделены потенциально опасные функциональные объекты, разделенные на группы по типу потенциальной уязвимости.

Итоги тестирования показали, что построенная фаззинг-схема позволила верифицировать большее число ошибок в исходных текстах по сравнению с классической реализацией, что отражено в табл. 1: было обнаружено 21 уязвимость, из которых 9 являются уникальными.

Таблица 1. Сравнение результатов верификации двумя фаззерами

Класс ошибок	**Количество ФО**	**Syzkaller (direct + FuzzController)**	**Syz-kaller**
Несоответствие размеров буфера при выделении памяти	28	6	4
Переполнение буфера на стеке	23	5	2
Разыменование нулевого указателя	20	2	0
Повторное освобождение памяти	30	3	2
Переполнение буфера на куче	5	4	3
Прочие ошибки при работе с памятью	19	1	0

Список литературы

1. Обзор различных средств фаззинга как инструментов динамического анализа программного обеспечения [Электронный ресурс] – 2018 – Режим доступа: https://moluch.ru/archive/186/47575/.

2. No Grammar, No Problem: Towards Fuzzing the Linux Kernel without System-Call Descriptions /Bulekov Alexander, Das Bandan, Hajnoczi Stefan. – 2023. – p. 16.

3. Егорова В.В., Панов А.С., Тележников В. Ю., Подходы, направленные на повышение эффективности фаззинг-тестирования компонентов защищенной ОС [Текст]//Труды ИСП РАН: Т.34, вып. 4 – 2022 г. – 21 – 34 с.

4. Dan Li, Hua Chen. KLEE: FastSyzkaller: Imporving Fuzz Efficiency for Linux Kernel Fuzzing // IOP Conference Series: Journal of Physics. – 2020 – P.30 – 38.

5. Бегаев А.Н., Кашин С.В. Выявление уязвимостей и недекларированных возможностей в программном обеспечении [Текст] / Университет ИТМО, 2020 – 38 с.

6. Syzkaller – kernel fuzzer. [Электронный ресурс] – Режим доступа: https://github.com/google/syzkaller.

7. Введение в ptrace [электронный ресурс] – 2018 – Режим доступа: https://habr.com/ru/post/430302/.

8. Maxim Grishin, Igor Korkin: Human-Controlled Fuzzing With AFL // Proceedings of the 15th Annual ADFSL 2022 Conference on Digital Forensics, Security and Law, Florida, USA, July 25, 2022, https://commons.erau.edu/adfsl/2022/presentations/3/

УДК 004.056

А.А. КОЗЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

МОДЕМ В SoC: ВОЗМОЖНОСТЬ ПОСТРОЕНИЯ ДОВЕРЕННОЙ МОБИЛЬНОЙ ПЛАТФОРМЫ НА СУЩЕСТВУЮЩЕЙ КОМПОНЕНТНОЙ БАЗЕ

Построение доверенной мобильной платформы является актуальной проблемой, особенно в контексте четвертой промышленной революции [1]. Модемы на базе SoC могут являться частью технического решения этой проблемы. Но информация о программном и аппаратном устройстве таких модемов известна только производителю. Поэтому возникает необходимость анализа их модели угроз [2]. В докладе описываются ранее неизвестные технические подробности внутреннего устройства современных модемов на базе SoC на примере различных мировых производителей. На основе этого приводится анализ источников угроз для SoC со стороны модемов и делаются выводы о возможных мерах по снижению связанных рисков.

В мобильных платформах основными электронными компонентами являются процессор прикладных задач (на нем выполняется бизнес-логика пользователя, далее пользовательский процессор) и модем. Сегодня технологии передачи данных поддерживают скорости, которые ранее были доступны только для проводной передачи - десятки гигабит в секунду. Для обеспечения таких скоростей модем и пользовательский процессор интегрируют внутри единой микросхемы. Такие системы носят название системы на кристалле (System-on-chip, SoC).

Модем в SoC отвечает за поддержку стандартов мобильной связи (от 2G до 5G в одном устройстве). При этом, с одной стороны, отсутствуют строгие формальные требования к программному коду этих изделий, и отсутствуют внешние сертификационные лаборатории. С другой стороны, исследование безопасности этих изделий силами специалистов по ИБ затруднено из-за закрытого характера их исходных кодов. В итоге несмотря на то, что эти изделия применяются повсеместно, их действительный уровень безопасности остается неизвестным. При этом их компрометация может привести к компрометации пользовательского процессора, и даже всего SoC, а следовательно, и изделия, в котором этот SoC используется.

Для существующих мобильных платформ на базе SoC в докладе разбираются три основных источника угроз для пользовательского процессора со стороны модема:

- Shared RAM. В зависимости от используемой архитектуры доступ к этой памяти может быть разграничен внутренними средствами безопасности конкретного CPU (MPU, MMU), или внешними, с помощью отдельного арбитра адресной шины SMMU;
- Ring Buffers. Этот алгоритмический механизм обмена данными между двумя абонентами исторически применяется для обеспечения надежного и простого канала связи, например через Shared Ram;
- Inter CPU communication (mailboxes). Аппаратно-программный механизм обмена данными между несколькими CPU.

С целью снижения рисков реализации угроз путем эксплуатации уязвимостей в описанных источниках угроз необходимо:

- инвентаризировать угрозы, которые несут в себе модемы в SoC для современных мобильных платформ;
- описать тактики и техники атак на существующие SoC через модемы в составе мобильных платформ;
- актуализировать существующие модели угроз подсистем SoC в составе мобильных платформ.

В качестве мер для снижения рисков реализации угроз ИБ на системах SoC со встроенным модемом в докладе рассматриваются:

- возможность использовать Trust Zone в качестве арбитра безопасности;
- применение концепции монитора безопасности для верификации операций со стороны модема;
- применение криптографических методов защиты Ring Buffers данных.

Список литературы

1. Артамонова Е.В., Сафонов А.Е. Индустрия 4.0: Будущее ИТ-сферы // Россия: тенденции и перспективы развития. 2022. №17-2. С. 382–394.

2. C. Xenakis and C. Ntantogian, "Attacking the baseband modem of mobile phones to breach the users' privacy and network security," *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, Estonia, 2015, p. 231–244, doi: 10.1109/CYCON.2015.7158480.

УДК 004.05

А.В. ЖАРКОВА, А.В. МЯЗИН

Саратовский национальный исследовательский государственный университет им. Н.Г. Чернышевского

О СИСТЕМЕ ШИФРОВАНИЯ ДАННЫХ ДЛЯ ХРАНЕНИЯ

В работе рассматривается проблема управления данными и их безопасностью в условиях современных реалий. Предложено решение в виде программы для шифрования данных пользователя с возможностью выбора различных алгоритмов шифрования и построением графиков для анализа их эффективности. Проведено исследование, которое в том числе показало, что чем больше длина ключа, тем дольше выполняется зашифрование/расшифрование данных; поточные алгоритмы шифрования работают быстрее, чем блочные; самыми быстрыми оказались RC5, ChaCha и Salsa20, самыми медленными – «Магма», RC2 и AES.

В настоящее время, когда объемы информации увеличиваются, важно эффективно управлять данными и обеспечивать их безопасность. Большинство организаций подвержены риску различных угроз из-за доступа злоумышленников к их конфиденциальным сведениям, поэтому обеспечение безопасности данных становится стратегической необходимостью. Организации часто переходят к электронному хранению данных, что повышает риски, связанные с их конфиденциальностью. Шифрование данных – ключевой элемент стратегии обеспечения безопасности, при котором используются специальные алгоритмы для защиты информации.

Для шифрования данных на уровне файлов или на уровне драйверов можно выбрать разные методы. Шифрование на уровне файлов означает, что каждый файл шифруется отдельно, что требует дополнительных действий. Шифрование на уровне драйвера обеспечивает защиту всего логического диска, но требует более сложной разработки. Оба метода имеют свои преимущества и недостатки.

При выборе метода шифрования важно учитывать практические характеристики, такие как универсальность и прозрачность. Универсальность позволяет защитить данные на разных уровнях системы, прозрачность позволяет модулю обеспечивать защиту для всех вышестоящих компонентов без внесения изменений в них. Также возможно использование аппаратных решений для защиты данных [1, 2].

Была разработана и реализована программа для шифрования данных пользователя с возможностью построения графиков для анализа работы

различных алгоритмов шифрования. Программа написана на языке C# с использованием библиотеки BouncyCastle (блочные шифры «Магма», AES, Blowfish, Cast5, Cast6, RC2, RC5, SM4; поточные шифры ChaCha, Salsa20) и SQL Server для хранения учётных данных.

Программа предоставляет пользователю выбор между различными блочными и поточными шифрами, которые также можно применять последовательно. После авторизации пользователя с ролью «user» монтируется логический диск, который по сути является папкой с данными пользователя. Благодаря этому можно будет ограничивать пользователям доступ к файлам компьютера, пользователь будет работать только с предоставленным логическим диском, содержащим его данные. Пользователь выбирает алгоритм шифрования и указывает файлы с ключом и вектором инициализации, после чего данные шифруются и становятся защищёнными. Также ведётся журнал событий, где фиксируются действия пользователей.

Анализируя полученные данные, было замечено следующее: чем больше длина ключа, тем дольше выполняется зашифрование/расшифрование данных; поточные алгоритмы шифрования работают быстрее, чем блочные [3]; самыми быстрыми алгоритмами стали RC5, ChaCha и Salsa20, самыми медленными – «Магма», RC2 и AES; при шифровании поточными алгоритмами данные пользователя не увеличиваются в размере, в то время как файлы, зашифрованные алгоритмами блочного шифрования, занимают на диске больше места.

Различные алгоритмы шифрования имеют свои особенности, разную производительность, поэтому выбор метода шифрования зависит от конкретных требований и условий эксплуатации системы.

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. М.: Триумф, 2002. 610 с.

2. Алексеев Е.К., Ахметзянова Л.Р., Бабуева А.А., Смышляев С.В. Защищенное хранение данных и полнодисковое шифрование. Прикладная дискретная математика. 2020, № 49, с. 78–97. DOI: https://doi.org/10.17223/20710410/49/6.

3. Жаркова А.В., Проданов М.Д. О сравнении блочных и поточных шифров. Компьютерные науки и информационные технологии: Материалы Междунар. науч. конф. Саратов: ООО Издательство «Научная книга», 2021. С. 65–68.

Направление

Финансовая и экономическая безопасность

Руководитель секции – НОРКИНА А.Н., к.э.н., доцент,
директор ИФТЭБ НИЯУ МИФИ

УДК 004.056

Авторы: С.Ю. БАТАЕВ, А.В. АДЖИБЕКОВ,
Научный руководитель – В.А. РЫЧКОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

РАЗРАБОТКА И ВНЕДРЕНИЕ ОТЕЧЕСТВЕННЫХ СРЕДСТВ КИБЕРЗАЩИТЫ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТУКТУРЫ

В данной работе исследуются современные отечественные решения для обеспечения кибербезопасности объектов критической информационной инфраструктуры (КИИ). Рассматриваются такие системы, как InfoWatch ARMA, PT Platform 187 и Platform V SOWA, которые обеспечивают защиту сетей, приложений и данных. Также анализируется роль государства в обеспечении безопасности КИИ через законодательные меры, такие как Федеральный закон № 187-ФЗ и программы импортозамещения.

Основная часть

Важность защиты критической информационной инфраструктуры (КИИ) невозможно переоценить. Она обеспечивает экономическую стабильность, предотвращая сбои в работе энергетических систем и финансовых учреждений. Социальные последствия атак на КИИ могут нарушить жизненно важные услуги, такие как здравоохранение и образование. Важной задачей является национальная безопасность, поскольку атаки на КИИ могут подорвать суверенитет государства [1].

Основные угрозы включают эскалацию кибератак, использование сложных векторов и целенаправленных атак, таких как известная атака WannaCry [2]. Проблемы замены иностранных решений добавляют сложности, так как возникают вопросы совместимости и отсутствия поддержки. Необходимость внедрения отечественных решений и обучения специалистов по кибербезопасности также важна, поскольку дефицит кадров ограничивает возможности защиты [3].

Российские системы, такие как InfoWatch ARMA и PT Platform 187, помогают защитить критическую инфраструктуру и обеспечивают мониторинг, анализ угроз и координацию действий с госорганами. Эти решения играют ключевую роль в повышении уровня безопасности в таких секторах, как промышленность и финансы [4].

Законодательная поддержка включает Федеральный закон № 187-ФЗ, требующий внедрения мер по кибербезопасности, и программу импортозамещения, направленную на развитие отечественных технологий и снижение зависимости от зарубежных решений [5].

Заключение

Обеспечение киберзащиты объектов КИИ требует комплексного подхода, который включает в себя как технические, так и организационные меры. Разработка и внедрение отечественных решений, таких как InfoWatch ARMA, PT Platform 187 и Platform V SOWA, играют ключевую роль в повышении уровня безопасности критической инфраструктуры. Однако для достижения максимальной эффективности необходимо продолжать совершенствовать технологии, внедрять инновационные решения и поддерживать тесное взаимодействие между государственными органами и субъектами КИИ.

Список литературы

1. Статья о текущих угрозах и возможностях отечественных решений для защиты объектов критической инфраструктуры от spbit.ru.
2. Информация о решениях и платформах для защиты объектов КИИ. Включая Platform V SOWA и другие разработки, с сайта itsec.ru.
3. Данные о системе защиты InfoWatch ARMA/ представленном на сайте компании InfoWatch.
4. Решения компаний Positive Technologies для защиты объектов КИИ, опубликованные на сайте ptsecurity.com.
5. http://www.kremlin.ru/acts/bank/42128

УДК 004.056

А.И. ВЕДЕНЕЕВА, В.А. КЕЛЬГАЕВА

Национальный исследовательский ядерный университет «МИФИ», Москва

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ В СИСТЕМАХ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Данная работа посвящена актуализации способов защиты данных при помощи криптографии. Цель исследования – рассмотреть существующие методы шифрования, применяемые в электронных системах голосования, выявить проблемы и предложить подходы к их решению. В результате анализа предложены меры по предотвращению несанкционированного доступа и усилению безопасности голосов избирателей.

Введение

Электронное голосование приобретает большую популярность как инструмент для повышения эффективности и доступности избирательных процессов. Однако, с ростом его использования возникают существенные вопросы безопасности данных. Основной задачей становится обеспечение конфиденциальности и целостности голосов избирателей, что требует внедрения современных методов криптографической защиты.

Пути решения

Одним из основных методов защиты данных является асимметричное шифрование, где каждый голос зашифровывается с использованием открытого ключа избирательной комиссии. Это предотвращает изменение голосов посторонними лицами [1]. Однако такая система не всегда может обеспечить полную анонимность, так как можно сопоставить голос с конкретным избирателем, если известен его ключ.

Для обеспечения анонимности применяются такие технологии, как протоколы «слепого» шифрования, позволяющие пользователям анонимно подтверждать свои голоса, а также доказательства с нулевым разглашением, которые дают возможность подтвердить правильность голоса без раскрытия его содержания [2]. Также активно используются методы гомоморфного шифрования, позволяющие проводить математические операции с зашифрованными данными, что обеспечивает возможность подсчета голосов без их расшифровки [3].

Новые идеи и результаты экспериментов

Применение блокчейн-технологий в электронных выборах позволяет создать распределенную базу данных, защищенных от несанкционированного изменения информации. Исследования показывают, что комбинация блокчейна с гомоморфным шифрованием позволяет достичь высокой прозрачности и безопасности.

Мы предлагаем усложнить применение блокчейн-технологий при помощи создания циклической структуры. В традиционном блокчейне каждый блок связан с предыдущим, создавая линейную цепочку, которая легко отслеживается. Наша идея состоит в том, чтобы сделать цепочку "циклической", где неясно, какой блок является первым. Основное новшество здесь заключается в том, что новые блоки могут добавляться только в начало цепи, но местоположение этого начала скрыто. Для этого, необходимо, чтобы информация о текущем «начале» блока была зашифрована. Доступ к добавлению новых блоков имел бы только тот, кто владеет специальным ключом, который позволяет расшифровать местоположение начала.

Заключение

На данный момент основные проблемы, с которыми сталкиваются системы электронного голосования, связаны с необходимостью найти баланс между анонимностью и прозрачностью, а также обеспечить защиту данных от возможных утечек и фальсификаций. Использование криптографических методов является ключевым для обеспечения безопасности таких систем.

Выводы

Будущие электронные системы голосования потребуют внедрения передовых криптографических методов для повышения доверия к результатам выборов. Широкое использование технологий блокчейна станет важной частью развития электронных выборов. Важным направлением останется разработка новых решений для усиления безопасности голосов и доверия к электронным системам голосования.

Список литературы

1. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York: Wiley, 1996, с. 165.

2. Juels A., Catalano D., Jakobsson M. Coercion-resistant electronic elections. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society

3. Gentry C. Fully Homomorphic Encryption Using Ideal Lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing, 2009.

УДК 004.056

А.С. КОСТЫЛЕВА, Ю.Б. РАКИТИНА

Национальный исследовательский ядерный университет «МИФИ», Москва

ПОЛИТИКА БЕЗОПАСНОСТИ КАК ИНСТРУМЕНТ СОЦИОТЕХНИЧЕСКОЙ ЗАЩИТЫ ОРГАНИЗАЦИИ

Целью данной работы является рассмотрение социотехнических угроз, которые могут нанести ущерб информационной системе организации, а также разработка политики безопасности, с помощью которой можно будет минимизировать риски, связанные с нарушением принципов информационной безопасности: целостности, конфиденциальности и доступности.

Введение

Социотехническая система состоит из нескольких составляющих – технической и социальной подсистем и из внешней среды, которая взаимодействует с организацией. Следовательно, защитные меры, созданные для обеспечения безопасности такой системы, должны учитывать как особенности технических устройств, так и человеческий фактор.

Постановка задачи

Разработка политики безопасности является важным аспектом в защите социотехнической системы.

Меры, разработанные в рамках данной политики, должны предусматривать защиту от социально-инженерных атак, например, фишинга – атаки, которая заключается в отправке зараженных электронных писем из якобы проверенных источников. Цели могут быть различны: собрать личные данные либо другую информацию или же сделать так, чтобы человек установил на свой компьютер специальные программы, которые могут предоставить удаленный доступ мошенникам к системе.

Следующей угрозой может быть претекстинг – тип атаки, при которой злоумышленник путем психологической манипуляции побуждает жертву раскрыть конфиденциальную информацию.

Существует еще одна актуальная социотехническая атака, называемая мошенничеством, связанным с высшим руководством. Это ситуация, когда нарушитель выдает себя за генерального директора компании или другого начальника, тем самым заставляя сотрудников передавать ему важные сведения или денежные средства.

Приманка – способ, при котором действия злоумышленника приводят к заражению корпоративных устройств вредоносным ПО. Обычно это происходит посредством распространения рекламы.

Наряду с защитой от социально-инженерных атак следует помнить и о технической части обеспечения безопасности. Сюда входят детальная проработка политики использования паролей, внедрение двухфакторной аутентификации, использование биометрических данных и цифровых сертификатов.

Установка систем управления доступом на корпоративные устройства – одно из решений задач безопасности. Они помогают разграничивать уровни доступа; это также подразумевает наличие белых списков, которые ограничивают перечень приложений, доступных для установки.

Для контроля и защиты трафика, проходящего через инфраструктуру организации, необходимо применение (с использованием сегментации) виртуальных приватных сетей. Принцип данного подхода заключается в том, что сеть предоставляет доступ к определенному сегменту только тем сотрудникам, которым он необходим.

Заключение

Политика безопасности регламентирует поведение работников в организации при попытке злоумышленника провести социотехническую атаку на информационную систему. Именно осведомленность сотрудников минимизирует риски, связанные с нарушением принципов информационной безопасности.

Список литературы

1. Кравченков С.И., Инновации в информатике. Безопасность социотехнических систем. 2018, с. 20–22. DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.3.

2. Костылева А.С., Рычков В.А., Рычкова В.И. Разработка и анализ модели образовательного приложения для изучения пользователями социально-инженерных атак, методов их предупреждения и предотвращения, 2023 / А.С. Костылева, В.А. Рычков, В.И. Рычкова, с. 803–809.

3. Ракитина Ю.Б., Рычков В.А. Разработка комплекса мер, обеспечивающих удаленный защищенный доступ к информационным ресурсам организации, 2023.

4. Кристофер Хэднеги Искусство обмана: Социальная инженерия в мошеннических схемах /Кристофер Хэднеги: ООО "Альпина Паблишер", 2023 – 430 с.

УДК 004.056

И.Д. ВЕРЕЩАГИН, К.Р. ПИВОВАРОВ
Научный руководитель – В.А. РЫЧКОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ: БУДУЩЕЕ УСТОЙЧИВЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

В работе отражена сущность постквантовой криптографии, а также ее достоинства по сравнению с современными методами шифрования. Описаны популярные подходы в ней, которые используются и разрабатываются в настоящее время, их преимущества, недостатки. Также в работе указано какое потенциальное будущее есть у этой технологии.

Введение

Ученые всего мира разрабатывают алгоритмы решения математических задач с помощью квантового компьютера. Таким образом, становятся актуальны алгоритмы постквантового шифрования, построенные на математических задачах, которые считаются трудно разрешимыми как электронными компьютерами, так и квантовыми.

Постквантовая криптография имеет следующие преимущества: устойчивость к квантовым атакам, долгосрочная безопасность данных, разнообразие криптографических подходов, а также она более оптимальна по затратам и не подразумевает большие расходы на интеграцию в АС.

Постквантовая криптография, основанная на хэш-функциях

Алгоритмы этого направления применяются для формирования и проверки ЭЦП и используют только криптографически стойкую хэш-функцию. К хэш-функциям при таком виде шифрования в современном российском стандарте ГОСТ Р 34.11-2012 (Стрибог) [1] предъявляются следующие требования: сопротивление поиску прообраза, сопротивление поиску второго прообраз, стойкость к коллизиям.

Одним из самых распространенных криптографических алгоритмов, основанных на хэш-функции, является подпись Меркла [2]. Существенным недостатком такого подхода к шифрованию является ограниченное количество подписей, используемых один раз для каждого сообщения, что препятствует массовому использованию такого подхода. Основные преимущества данного метода шифрования:

– Целостность данных.

– Скорость и эффективность.
– Фиксированный размер выходных данных.

Постквантовая криптография, основанная на многомерных квадратичных системах

Данная задача является NP-полной [3], а её стойкость основывается на сложности решения системы многомерных квадратичных многочленов над конечным полем. Наиболее популярным стандартом такого подхода является AES (англ. Advanced Encryption Standard). Он используется правительством США для шифрования государственной тайны.

К главным преимуществам AES относят высокую скорость и низкие требования к оперативной памяти устройства. Так, например, на процессоре Pentium Pro шифрование AES требует 18 тактовых циклов на байт (cpb) [4]. Таким образом, подход уже в настоящее время активно применяется в различных отраслях.

Заключение

В ходе работы были рассмотрены преимущества два популярных подхода к постквантовой криптографии: на основе хэш-функции и на основе многомерных квадратичных систем. Оба этих направления имеют как свои преимущества, так и недостатки, уже сейчас вводятся стандарты и разрабатываются алгоритмы, которые можно причислить к постквантовой криптографии. Международные организации, такие как NIST (National Institute of Standards and Technology), работают над стандартизацией постквантовых алгоритмов. Это позволит обеспечить согласованные подходы к безопасности и защиту данных в глобальном масштабе, что станет новым золотым стандартом в криптографии.

Список литературы

1. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования – дата введения: 2013-01-01.
2. Батенко К.Е. Пост-квантовый алгоритм электронно-цифровой подписи на основе дерева Меркла и ГОСТ РФ 34.11-12. «Стрибог» – Молодой ученый – 2017 – №23(157), с. 100–103.
3. Комарова Антонина Владиславовна, Коробейников Анатолий Григорьевич Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности. 2019. №2 (30).
4. Schneier, Bruce; Kelsey, John; Whiting, Doug; Wagner, David; Hall, Chris; Ferguson, Niels (1999-02-01). "Performance Comparisons of the AES submissions". Archived from the original on 2011-06-22. Retrieved 2010-12-28.

УДК 004.056

Е.Д. СОКОЛОВА, М.В. СОЛДАТОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: УГРОЗА МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Цель работы – выявить слабые места многофакторной аутентификации и найти способы защитить пользователей от возрастающих атак.

Введение

Сейчас многофакторная аутентификация (MFA) стала стандартом для защиты учетных записей от несанкционированного доступа. Однако MFA не является панацеей и остается уязвимой перед атаками социальной инженерии. Данная работа призвана проанализировать, как злоумышленники могут обходить MFA, используя психологические манипуляции, и рассмотреть меры по защите от таких атак.

Описание проблемы

Несмотря на наличие многофакторной аутентификации (MFA), злоумышленники все еще могут получить доступ к учетным записям пользователей, используя методы социальной инженерии.

MFA считается одним из наиболее надежных способов защиты от несанкционированного доступа, но методы социальной инженерии обходят ее. Злоумышленники активно используют эти методы, чтобы получить доступ к конфиденциальным данным пользователей [1]. Незнание этих методов и недостаточная осведомленность о них у пользователей создают уязвимость для атак. Потери от таких атак могут быть значительными, включающие финансовые потери, утечку персональной информации и репутационные риски.

Согласно статистике Positive Technologies, доля инцидентов в отношении частных лиц в сравнении с 2021 г. увеличились с 88% до 93% [2], а количество атак на организации осталось на прежнем уровне. Тем не менее, доля использования метода снизилась с 50% до 43%. Преступники в 2022 г.. в 16% от успешных атак на организации получали доступ к целевым системам и учетным данным компаний, что сделало это атаки гораздо опаснее.

Предлагаемые решения

- Повышайте осведомленность: Знайте распространенные методы социальной инженерии и как их распознать.
- Никогда не делитесь информацией о себе: не предоставляйте свои учетные данные или одноразовые пароли (OTP) никому.
- Проверяйте ссылки: прежде чем кликать на ссылки в электронных письмах или сообщениях, убедитесь, что они правильные.
- Будьте осторожны с просьбами: не доверяйте сообщениям, которые требуют от вас личной информации или действий, которые вы не можете проверить.
- Используйте надежные пароли: создавайте уникальные и сложные пароли для разных учетных записей.
- Включите уведомления о безопасности: получайте оповещения о подозрительной активности в ваших аккаунтах.
- Регулярно обновляйте: обновляйте программное обеспечение и используйте антивирусные программы.
- Проверяйте финансы: регулярно проверяйте банковские выписки и отчеты о кредитных картах на наличие подозрительных операций.

Помимо предлагаемых известных решений хочется предложить усовершенствование технологии MFA и внедрение новых систем оповещения и подтверждения личности. Например, для пожилых пользователей ввести рассылки, профилактические передачи и рекламу.

Заключение

Важно понимать, что никакая система безопасности не идеальна. Ключом к успешной защите является постоянная бдительность и готовность адаптироваться к новым угрозам.

Список литературы

1. Хаднаги, Кристофер. (2023). Социальная инженерия: искусство человеческого взлома.
2. PT Security. (2023). Социальная инженерия: искусство человеческого взлома. https://www.ptsecurity.com/ru-ru/research/analytics/social-engineering/ (дата обращения: 20.09.2024).
3. NIST. (2023). SP 800-63B: Digital Identity Guidelines. https://pages.nist.gov/800-63-3/sp800-63b.html (дата обращения: 20.09.2024).

УДК 004.056

Ю.С. ШАРКОВА, А.А. САФОНОВА, В.Ю. РАДЫГИН

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ КОНКУРЕНТОСПОСОБНОСТИ НИЯУ МИФИ НА МЕЖДУНАРОДНОМ РЫНКЕ ВЫСШЕГО ОБРАЗОВАНИЯ В СФЕРЕ ЦИФРОВОЙ СРЕДЫ

Цифровизация высшего образования является ключевым фактором в предоставлении качественных образовательных услуг. В работе проведён анализ состояния уровня цифровизации мировых университетов и дана оценка положения НИЯУ МИФИ. Результаты выявили основные недостатки цифровой инфраструктуры университетов, подчёркивая необходимость её модернизации.

Введение

Цифровая трансформация высшего образования соответствует целям, установленным Правительством РФ [1]. Несмотря на активные усилия, российские университеты сегодня всё ещё отстают от лидирующих зарубежных вузов по уровню внедрения цифровых технологий, что, в том числе, обусловлено санкционным давлением и ростом стоимости программного обеспечения. В связи с этим, необходимо критически оценить текущее состояние цифровых услуг университетов и выявить основные недостатки и направления развития.

Методологические подходы к оценке цифровизации университетов

Анализ цифровизации университетов опирается на локальные и глобальные рейтинги, такие как QS, THE и ARWU. Локальные рейтинги акцентируют внимание на цифровом оборудовании, а глобальные часто не оценивают цифровые услуги, что затрудняет детальный анализ и планирование цифровой трансформации. Академические публикации и стратегии цифровизации вузов [2] предлагают полезные модели, но зачастую ориентированы на специфические условия. Дополнительную информацию могут дать научные публикации [3, 4], анализирующие состояние вузовских кампусов. НИЯУ МИФИ важно провести собственное исследование для оценки своего положения среди вузов и разработки задач по улучшению цифровых сервисов.

В исследования использовались систематизированные данные опросов студентов из разных стран и независимая оценка онлайн-ресурсов университетов. Оценка проводилась по 17 критериям, охватывающим

общие цифровые сервисы, разнообразие платформ, а также учебные, внеучебные и дополнительные услуги. Метрики включали такие параметры, как доступность сервисов, наличие мобильных версий и альтернативных платформ, а также качество взаимодействия студентов с университетскими цифровыми ресурсами.

Заключение

Результаты исследования показали значительные различия в уровне цифровой трансформации университетов. Университеты были разделены на три группы: с высоким уровнем цифровизации, промежуточным и низким. Анализ показал, что 69% университетов предоставляют мобильные приложения (87,5% среди российских), однако лишь 50% (71,4% по России) из них полностью соответствуют функционалу веб-версий. НИЯУ МИФИ вошел в число лучших университетов, заняв 4 место. Лидерами рейтинга стали Национальный университет Сингапура, Американский университет (Вашингтон) и Бизнес-школа «Эмлион».

Кроме того, анализ цифровой трансформации университетов показал существенные различия в уровне внедрения цифровых технологий на международном и национальном уровнях. Многие университеты, включая российские, находятся на промежуточной стадии цифровизации и нуждаются в улучшении функциональности своих цифровых сервисов, особенно мобильных приложений. Для дальнейшего развития вузам необходимо улучшать соответствие мобильных и компьютерных решений и расширять доступность цифровых услуг, что укрепит их позиции на глобальной арене и повысит удовлетворённость студентов.

Список литературы

1. Распоряжение Правительства РФ от 21 декабря 2021 г. № 3759-р «Об утверждении стратегического направления в области цифровой трансформации науки и высшего образования» // Собрание законодательства Российской Федерации. – 2022. – № 1 – с. 265.

2. Digitalisation Strategy of the University of Vienna, 2020. URL: https://digital.univie.ac.at/fileadmin/user_upload/p_digital/Dokumente/Digitalisierungsstrategie_ENG.pdf (дата обращения: 19.09.2024).

3. Maltese V. Digital Transformation Challenges for Universities: Ensuring Information Consistency Across Digital Services. Cataloging & Classification Quarterly. 2018, 56(7), с. 592–606. DOI: 10.1080/01639374.2018.1504847.

4. Корсаков Г.О., Михайлова И.П. Профиль цифровой зрелости университета как инструмент цифровой трансформации системы высшего образования. Инновации и инвестиции. 2022, № 7, с. 53–57. EDN: MRFPVV.

УДК 004.652.3:004.822.732

А.О. ЯКУШИН, Р.В. ГАЯЗОВ
Научный руководитель – В.А. РЫЧКОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПОСТКВАНТОВОЕ ШИФРОВАНИЕ. НА ПОРОГЕ НОВОЙ СТУПЕНИ КРИПТОГРАФИИ

Целью работы является анализ постквантовых алгоритмов шифрования данных, выявление их положительных и отрицательных сторон, относительная оценка совместимости с нынешними информационными системами. Главным методом исследования является сравнительный анализ. В результате работы были выявлены ряд недостатков, а также перспектив и потенциальных преимуществ развития данной ветви криптографии.

Введение

В последние десятилетия развитие вычислительных технологий привело к значительным изменениям в области информационной безопасности. Одним из наиболее заметных факторов, способствующих этим изменениям, стало появление квантовых вычислений, которые обещают революционизировать подходы к обработке данных и решению сложных задач. Однако вместе с этими возможностями возникли серьезные угрозы для традиционных криптографических систем, основанных на математических задачах, таких как факторизация и дискретный логарифм. Квантовые алгоритмы, такие как алгоритм Шора, ставят под сомнение устойчивость большинства современных методов шифрования, что делает необходимым переход к новым подходам.

Постквантовое шифрование представляет собой ответ на эти вызовы. Это область криптографии, которая разрабатывает алгоритмы, устойчивые к атакам с использованием квантовых компьютеров. На пороге новой ступени криптографии мы наблюдаем активные исследования и разработки, направленные на создание надежных систем защиты данных, которые будут способны обеспечить безопасность в условиях квантовой эры.

Постановка задач

Цель работы обусловила постановку следующих задач:

1. Провести анализ существующих исследований и технологий в области постквантового шифрования, чтобы оценить текущее состояние и основные достижения.

2. Изучить и классифицировать ключевые методы и алгоритмы, используемые в постквантовом шифровании, чтобы выделить наиболее значимые подходы.

3. Проанализировать преимущества и недостатки существующих постквантовых алгоритмов, чтобы определить их применимость в различных сценариях.

4. Проанализировать потенциальные направления развития и возможности интеграции постквантовых алгоритмов в современные системы безопасности для предсказания их будущего влияния

Заключение

В настоящее время алгоритмы постквантового шифрования вызывают больше неудобств и проблем, чем приносят пользы, поскольку они требуют дополнительных вычислительных ресурсов и сложны в реализации. Однако уже в ближайшие несколько лет вычислительные мощности квантовых компьютеров могут достичь уровня, достаточного для создания угрозы современным криптосистемам. Поэтому стоит уже сейчас изучать и внедрять постквантовые алгоритмы шифрования данных в повседневную жизнь, ведь ближайшие десятилетия постквантовое шифрование станет критически важным для обеспечения безопасности данных.

Список литературы

1. Fast Lattice-Based Cryptography in Post-Quantum Communication. In: International Conference on Information Technology - New Generations. Springer, Cham, 2016, p. 21–30. URL: https://link.springer.com/chapter/10.1007/978-3-031-59711-4_21

2. Внедрение постквантовой криптографии к 2024 году: проблемы и решения Блог Kaspersky Daily, 25 февраля 2022 г. URL:https://www.kaspersky.ru/blog/postquantum-cryptography-2024-implementation-issues/38195

3. Постквантовая криптография: основные подходы и причины использования.URL: https://habr.com/ru/sandbox/163505/

4. Постквантовый TLS внедряют уже сейчас. URL: https://habr.com/ru/companies/globalsign/articles/832078/

Направление

Проблемы информационной безопасности в системе Высшей школы

Руководитель секции – ТОЛСТОЙ А.И. к.т.н.,

заведующий кафедрой №44

УДК 519

В.А. МИНАЕВ[1], А.В. ЩЕПКИН[2], А.С. ЭРДНИЕВ[1]

[1]*Московский университет МВД России им. В.Я. Кикотя*

[2]*Институт проблем управления им. В.А. Трапезникова РАН*

ТЕХНОЛОГИИ ЭКСПЕРТИЗЫ НАУЧНО-ТЕХНИЧЕСКОГО ПОТЕНЦИАЛА ВУЗОВ

Дается обоснование технологии экспертизы научно-технического потенциала ВУЗов с использованием методов теории управления активными системами. Даны строгие математические доказательства существования равновесных состояний в экспертных процедурах, отражающих субъективность экспертов. В частности, отражающих их заинтересованность в результатах экспертизы, а также в собственном рейтинге. Делается вывод, что цифровизация научной и образовательной деятельности ВУЗов имеет важное следствие в виде развития программ оптимального управления результатами их интеллектуальной активности.

Основные задачи экспертизы

Современным ВУЗовским сообществам предстоит серьезная работа по интеграции традиционных подходов к обучению с новыми возможностями цифровой среды. В мире таких возможностей необходимо находить и новые пути экспертизы образовательной и научно-технической деятельности ВУЗов на основе использования цифровых технологий. Одним из ключевых направлений в этой сфере является развитие и формирование научно-технического потенциала ВУЗов. Наличие устойчивых механизмов управления указанным потенциалом, эффективная защита интеллектуальных прав способствуют наращиванию объемов результатов интеллектуальной и повышению интенсивности инновационной деятельности, на которых строится современная экономика развитых стран.

При этом следует отметить, что наибольшим потенциалом, как правило, обладают технические новации. Они рождаются в коллективах, ведущих научно-техническую деятельность. Одним из активных участников соответствующих процессов являются ВУЗы, имеющие ее технические направления. Научная и инновационная деятельность ВУЗов не может вестись без учета и использования принципов эффективного управления интеллектуальной собственностью. На сегодняшний день не разработано унифицированных методик оценки эффективности проектов и программ научно-инновационной деятельности ВУЗов, что во многом связано со сложностью системного описания такого объекта, как научная деятельность в ВУЗовской среде, и неоднозначностью понятий, используемых при

оценке научно-образовательных характеристик современных российских ВУЗов и их интеллектуальной собственности. Эффективным инструментом оценки выполнения научно-технических проектов и программ в ВУЗах, их потенциала развития являются механизмы экспертизы, являющиеся способом проигрывания различных сценариев хода научно-исследовательской и инновационной деятельности в высших учебных заведениях.

Механизмы экспертизы потенциала развития ВУЗов

В работах по исследованию экспертных механизмов [1-3] отмечается – необходимо учитывать тот факт, что сами эксперты либо заинтересованы в результатах экспертизы, либо заинтересованы в повышении своего рейтинга. Для этого авторами осуществлены математические доказательства существования равновесных состояний в экспертных процедурах.

Заинтересованность экспертов в результатах экспертизы соответствует тому, что эксперты, заинтересованы в минимальном расхождении между истинной оценкой проекта и результирующей экспертной оценкой.

Экспертиза проекта двумя различными группами экспертов характеризуется тем, что в одной группе проявляется заинтересованность экспертов в достижении результирующей оценки близкой к собственной, а в другой эксперты заинтересованы в повышении своего рейтинга.

Заключение и выводы

Цифровизация научной и образовательной деятельности современных ВУЗов имеет важное следствие в виде развития программ оптимального управления результатами их интеллектуальной активности. Рассмотренные авторами механизмы экспертных процедур дают возможность с высокой степенью корректности оценивать сложные проекты, связанные с цифровизацией научно-технической продукции, оптимизацией управления ресурсами при выполнении ВУЗовских программ.

Список литературы

1. Бурков В.Н., Коробец Б.Н., Минаев В.А., Щепкин А.В. Механизмы экспертной оценки военно-технологических программ // Вестник МГТУ им. Н.Э. Баумана. Серия: Естественные науки. 2017. №2 (71). – С. 105–117.

2. Коробец Б.Н., Минаев В.А., Щепкин А.В. Комплексное оценивание научно-технического уровня программ вооружений, военной и специальной техники // Радиотехника. 2017. № 4. – С. 149–156.

3. Бурков В.Н., Коробец Б.Н., Минаев В.А., Щепкин А.В. Особенности механизма оценивания научно-технических проектов при участии активных экспертов // Нелинейный мир. 2017. Т. 15. № 3. – С. 79–86.

УДК 004.056

А.С. ЭРДНИЕВ
Научный руководитель – к.т.н., доцент В.С. ГОРБАТОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

КОНЦЕПЦИЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ОВД В СФЕРЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Цель данной работы – совершенствование подготовки кадров для органов внутренних дел (ОВД) в сфере информационной безопасности в условиях перехода на ФГОС 4-го поколения (ФГОС ВО 4).

Работа опирается на результаты исследования [1], в котором обосновано применение для достижения указанной цели законодательного механизма и терминологического аппарата, определяющего сущность критической информационной инфраструктуры (КИИ) в деятельности ОВД. В дополнение к этому изучен потенциал ФГОС ВО 4, применительно к подготовке специалистов в сфере ОВД.

Сущность и структура образовательной деятельности в ОВД выстраивается на основании федерального закона «Об образовании» и приказа МВД России от 2 февраля 2024 г. № 44 [2], согласно которым формирование профессиональных компетенций в рамках высшего профессионального образования осуществляется по двум основным составляющим: профессиональное обучение по должности служащего «Полицейский»; основная образовательная программа.

Для понимания сущности изменений, связанных с переходом на ФГОС ВО 4 сопоставлены тексты стандартов в действующей редакции и проектами будущих нормативов, размещенных, на Официальном портале ФГОС ВО [3]. Первая новация указана в п.1 Проекта ФГОС ВО, где предусмотрены ранее не фигурировавшие в редакции ФГОС 3++ формы реализации образовательной подготовки: базовое ВО и специализированное ВО.

Еще одной обновленной нормой в ФГОС ВО 4 является измененный перечень компетенций. В отличии от редакции ФГОС 3++ в настоящем проекте присутствуют следующие виды компетенций: универсальные (УК), базовые (БК), общепрофессиональные (ОПК) и профессиональные (ПК). Система предлагаемых типов компетенций во ФГОС 4 не претерпела существенных изменений. Однако, в содержании исключена

норма «владеть», в проектной редакции остается только две характеристики: знать и уметь. Норма «владеть» переходит в категория «индикатора достижения компетенций».

Аналитический обзор ФГОС ВО 4 не заканчивается изучением компетентностного компонента. Выстраивание нового образовательного процесса также зависит от смыслового наполнения отдельных специализаций в рамках новых ФГОС ВО, в частности, такой раздел подготовки, как «Безопасность информационных технологий объектов критической информационной инфраструктуры». В условиях нарастающего информационного противоборства подобное направление может оказаться также востребованным и для подготовки специалистов в интересах ОВД. На основе опыта ФУМО ВО по ИБ предложен проект функциональной карты в сфере подготовки специалистов по защите КИИ ОВД, который формулирует определенные траектории дальнейшей работы. Представленный концепт обеспечивает оптимальное соотношение требований к специалистам с образовательной подготовкой, формулируя конкретные траектории развития под задачи заказчиков.

Вместе с тем изучений стадий образовательного процесса демонстрирует диссонирующие конструкции в элементах образовательной подготовки. Так этап формирования базовых компетенций, необходимый для структурирования «технического мировоззрения» вступает в конфликт с этапом профессионального обучения, где формируются базовые компетенции для сотрудника полиции. Преодоление указанного противоречия необходимо основывать на четко выработанной стратегии обучения, обоснованной применением формализованного аппарата, в частности, на примере стандарта SFIA8, описывающий ключевые навыки и управляющий компетенциями специалистов по кибербезопасности [4].

Список литературы

1. Горбатов, Виктор С.; Эрдниев, Александр С. Совершенствование подготовки кадров по обеспечению безопасности информационной инфраструктуры органов внутренних дел. Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 100–119, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.06.

2. Приказ МВД России от 2 февраля 2024 г. № 44 «Об утверждении Порядка организации подготовки кадров для замещения должностей в органах внутренних дел Российской Федерации» (Зарегистрировано в Минюсте РФ 12.03.2024 N 77488)

3. Официальный портал ФГОС ВО // URL: https://fgosvo.ru/ (дата обращения 31.07.2024)

4. Белякова, О. С. Исследование навыков кибербезопасности стандарта SFIA8 / О.С. Белякова, В.А. Сухомлин // International Journal of Open Information Technologies. – 2022. – Т. 10, № 7. – С. 156–193. – EDN ADJBAD

УДК 004.056

А.Г. ОСТАПЕНКО[1], Е.А. МОСКАЛЕВА[1], А.П. ВАСИЛЬЧЕНКО[2], А.А. ОСТАПЕНКО[1]

[1]*Воронежский государственный технический университет*

[2]*Финансовый университет при Правительстве Российской Федерации, Москва*

НЕЙРОСЕТЕВЫЕ КОМПЕТЕНЦИИ И ИНСТРУМЕНТЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В сегодняшних условиях подготовка специалиста по информационной безопасности требует формирования компетенций по использованию технологий искусственного интеллекта и нейросетевых инструментов. В докладе изложены результаты совместного проекта Финансового университета при Правительстве Российской Федерации Института проблем управления РАН и Воронежского государственного технического университета в этом направлении.

«Ученым можешь ты не быть, но нейросеть познать обязан» – этот популярный афоризм может стать эпиграфом для подготовки современных специалистов по защите информации, ибо сегодня выпускник наших образовательных программ, не способный пользоваться нейросетевыми инструментами, подобен человеку с одной рукой. И речь здесь идет не о машинной подготовке пояснительных записок для курсовых и дипломных работ, а о масштабной и систематической проектной деятельности будущего специалиста (при освоении профессиональных знаний и навыков) в нейросетевом пространстве. Особо эффективен такой учебный процесс, если студенты массово вовлечены в создание и модернизацию элементов инструментария проектирования, сопрягающего традиционные средства с технологиями искусственного интеллекта. При этом обучающийся приобретает объективно необходимые в данном случае компетенции:

– агрегации, генерации и форматирования баз профессиональных знаний и данных под нейросетевую реализацию,

– организации машинного обучения нейросети этим сведениям,

– подготовки запросов и использования интеллектуальных подсказок сети в проектных ситуациях защиты информации.

Совместный проект Финансового университета при Правительстве Российской Федерации, Института проблем управления РАН и Воронежского государственного технического университета по созданию атласа кибератак [1] наглядно подтвердил правоту вышеизложенного.

Первоначально проект был нацелен на сбор и систематизацию сведений о кибератаках и используемых ими уязвимостях для информационной и методической помощи дипломникам, которые активно подключились к решению этой задачи, и показали, что потенциал проекта отнюдь не исчерпывается указанным выше. Неполнота и разнородность существующих в этом вопросе баз данных потребовала автоматизации процесса парсинга и расширения номенклатуры используемых сведений и полученных характеристик [2]. Наконец, описания атак и уязвимостей, а также техник противодействия им в упомянутых базах оставляют желать много лучшего. Отсюда вытекает необходимость совершенствования и развития баз знаний, а также разработки удобного для использования формата их представления в атласе. Кроме того, мультиразмерность аккумулируемых и генерируемых сведений потребовала применения средств искусственного интеллекта, что перевело проект в принципиально новую плоскость.

Перечисленные аргументы мотивировали молодых исследователей на создание сервисов риск-анализа успешности многообразия кибератак на известные уязвимости информационных систем и сетей. В результате появилась возможность в ходе учебного процесса строить риск-ландшафты для пар «вектор атаки-уязвимость» при нарушении целостности, доступности и конфиденциальности информации, выявлять наиболее опасные сочетания деструктивов с учетом ценности защищаемой информации [3]. Проведение такого риск-анализа служит основой для выработки регламентов реагирования и ликвидации последствий кибератак, которые образуют политику обеспечения информационной безопасности защищаемых предприятий и организаций, в том числе и критической информационной инфраструктуры (КИИ). Поэтому наши студенты успешно владеют предлагаемым инструментарием, приобретая компетенции в области оценки и регулирования рисков, как важнейшего средства защиты объектов кибербезопасности.

Список литературы

1. Остапенко Г.А. Формализация знаний и данных кибератак и уязвимостей. / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Д.С. Покудин, Н.Н. Корвяков, А.А. Ноздрюхин. // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 231–238.

2. Остапенко Г.А. Модуль нейросетевой регламентации мер противодействия кибератакам. / Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, А.А. Ноздрюхин, Д.С. Покудин, Н.Н. Корвяков. // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 239–246.

3. Смирнов В.В. Кибератаки вида «анализ целевого объекта»: риск-ландшафт векторов атак и уязвимостей телекоммуникационных сетей. / В.В. Смирнов, А.П. Васильченко, А.А. Остапенко, А.В. Гречишкин, С.С. Куликов, Д.Н. Рахманин. // Информация и безопасность. 2024. Т. 27. Вып. 2. С. 273–284.

УДК 004.056.5

В.В. КОМАРОВ

АНО ДПО «Центр повышения квалификации «Академия информационных систем», Москва

РАЗВИТИЕ КОМПЕТЕНЦИЙ СПЕЦИАЛИСТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЕСПЕЧЕНИЯ ГОТОВНОСТИ ЭКСПЛУАТАЦИОННОГО ПЕРСОНАЛА К НЕШТАТНЫМ СИТУАЦИЯМ И К ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК

Рассматриваются результаты анализа необходимых трудовых умений, навыков и знаний специалистов по информационной безопасности, организующих и обеспечивающих выполнение нормативных требований ФСТЭК и ФСБ России по действиям персонала объектов информатизации в нештатных ситуациях, при реагировании на компьютерные инциденты и ликвидации последствий компьютерных атак. Отмечена низкая эффективность подготовки по данному направлению в рамках действующих стандартов профессионального образования.

Введение

Базовые меры безопасности для всех категорий значимости объектов КИИ предусматривают обеспечение готовности действий персонала в нештатных ситуациях при эксплуатации, включающие в себя:

– планирование (ДНС.1);

– обучение и отработка действий персонала (ДНС.2) [1].

Также предусмотрена базовая мера: устранение последствий компьютерных инцидентов (ИНЦ.4).

В требованиях ФСБ России предусмотрено не только реагирование на компьютерные инциденты, включая этап «ликвидация последствий компьютерного инцидента», но ликвидацию последствий компьютерных атак, в том числе обязательное обучение и отработку (тренировку) действий персонала [2].

Необходимые компетенции и пути их развития

Обеспечение бесперебойной работы, обеспечение непрерывности бизнес-процессов, организация и проведение аварийно-восстановительных работ, действия в нештатных ситуациях требует от специалиста не только знаний соответствующих документов (методик, стандартов, приказов и т.д.), но и формирование устойчивых навыков и умений по практической реализации [3, 4].

Дополнительную сложность для обучения вносят следующие факторы:

– отраслевые и ведомственные условия функционирования объектов КИИ;

– необходимость выполнения таких аварийно-восстановительных работ при ликвидации последствий компьютерных атак в условиях наступивших негативных последствий, определенных на этапе категорирования (радиационные аварии, пожары, разрушение промышленных установок, аварии транспортных средств, гибель и/или ранения людей).

Многообразие и вариативность ситуаций не позволяет сформировать универсального специалиста, готового организовать подобные работы на значимых объектах КИИ во всех сферах.

Считаем целесообразным, в рамках программ высшего и среднего профессионального образования формировать базовые компетенций по основам планирования действий и основам педагогической деятельности (обучение персонала), с дальнейшим расширением компетенций по организации, обеспечению и управлению действиями персонала в нештатных ситуациях и аварийно-восстановительных работ при ликвидации последствий компьютерных атак с учетом отраслевых особенностей в рамках дополнительного профессионального образования (повышения квалификации).

Заключение

Необходимо формировать навыки специалиста действиям в условиях, когда система защита информации не смогла предотвратить наступление негативных последствий от компьютерных атак.

Список литературы

1. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

2. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

3. Майорова Е.В. Методические аспекты реагирования на инциденты информационной безопасности в условиях цифровой экономики. // Петербургский экономический журнал. 2020. № 1. С. 155–162. DOI: 10.25631/PEJ.2020.1.155.162.

4. ГОСТ Р 53131 – 2008 (ИСО/МЭК ТО 24762:2008) «Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий», https://docs.cntd.ru/document/1200085087.

УДК 004.056

М.В. РОМАНОВА

Московский государственный лингвистический университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК КОМПОНЕНТ ЦИФРОВОЙ ГРАМОТНОСТИ ВЫПУСКНИКА ПЕДАГОГИЧЕСКОГО ВУЗА

В статье рассматривается проблема формирования цифровой грамотности педагогических работников в отношении уровня их резистентности к кибератакам и средствам социальной инженерии. Подчеркивается необходимость целенаправленной подготовки выпускников педагогических вузов в области информационной безопасности в связи с возрастающим числом кибератак на образовательные учреждения. Приводятся результаты опытного обучения в рамках разработанного авторского учебного модуля по проблемам информационной безопасности специалистов-будущих преподавателей иностранного языка.

Актуальность настоящего исследования обусловлена возрастающим числом кибератак на цифровые системы образовательных учреждений в целом и на представителей профессорско-преподавательского состава российских вузов, в частности. Представители профессионального сообщества в области информационной безопасности отмечают активное развитие средств социальной инженерии, направленных на финансовые махинации и кражу персональных данных профессорско-преподавательского состава российских вузов, а также значительный рост DDoS-инцидентов с целью создания конфликта интересов и нанесения ущерба высшим учебным заведениям, которые отличаются высоким спросом на свои образовательные программы [1].

В этой связи актуализируется необходимость специальной подготовки кадрового состава образовательных учреждений по вопросам информационной и кибербезопасности как важной составляющей цифровой грамотности педагога. Немаловажным фактором для введения такой дисциплины или учебного модуля являются современные требования к педагогическим работникам в отношении наличия знаний, навыков и умений в области информационной безопасности, направленных на избегание возможности инцидента [2, 3, 4].

Для реализации данных требований в ФГБОУ ВО МГЛУ в содержание основных образовательных программ на уровне бакалавриата была

введена дисциплина «Цифровая трансформация профессиональной деятельности» для студентов, в том числе направления подготовки 45.03.02 Лингвистика (Теория и методика преподавания иностранных языков и культур). В 2023 г. в качестве компонента данной дисциплины был разработан и апробирован в экспериментальном обучении студентов – будущих преподавателей иностранного языка учебный модуль по информационной безопасности.

По завершению прохождения учебного модуля для участников опытного обучения был организован контроль устойчивости приобретенных ими знаний и уровня их резистентности к кибератакам и средствам социальной инженерии. Результаты проведенного контроля позволили определить уровень резистентности испытуемых как средний и подчеркнули актуальность целенаправленной подготовки выпускников педагогических вузов в области информационной безопасности через систему заданий, предусматривающих активную образовательную деятельность студентов в процессе освоения данной дисциплины.

Список литературы

1. Денисенко А. Российские вузы атакованы хакерами в самом преддверии приемной кампании // CNews. 2024. URL: https://www.cnews.ru/news/top/2024-05-29_hakery_nachali_atakovat (дата обращения: 10.09.2024).

2. Казинец В.А., Редько Е.А. Информационная безопасность как часть цифровой культуры выпускников педагогических университетов // Современное педагогическое образование. 2022. №5. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-chast-tsifrovoy-kultury-vypusknikov-pedagogicheskih-universitetov (дата обращения: 10.09.2024).

3. Глухов А.П., Камнева О.С., Соломина И.Г. Цифровая грамотность педагогов: концептуализация и мониторинг // Ped.Rev.. 2022. №5 (45). URL: https://cyberleninka.ru/article/n/tsifrovaya-gramotnost-pedagogov-kontseptualizatsiya-i-monitoring (дата обращения: 10.09.2024).

4. Приказ Минтруда России от 18.10.2013 N 544н (ред. от 05.08.2016) «Об утверждении профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)» (Зарегистрировано в Минюсте России 06.12.2013 N 30550). URL: https://www.consultant.ru/document/cons_doc_LAW_155553/.

УДК 004.89

Г.В. РЫБИНА, А.Ю. НИКИФОРОВ, А.А. ГРИГОРЬЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ОБУЧАЮЩИХ СИСТЕМ

Рассматриваются некоторые аспекты информационной безопасности функционирования интеллектуальных обучающих систем, разработанных на основе задачно-ориентированной методологии построения интегрированных экспертных систем и средств инструментального комплекса АТ-ТЕХНОЛОГИЯ.

Обучающие интегрированные экспертные системы (ИЭС) и веб-ИЭС, разработанные в лаборатории «Интеллектуальные системы и технологии» кафедры «Кибернетика» НИЯУ МИФИ, стали неотъемлемой частью учебного процесса и активно применяются с 2008 г. для автоматизированной поддержки базовых дисциплин по направлению подготовки «Программная инженерия», в том числе: «Введение в интеллектуальные системы и технологии», «Интеллектуальные диалоговые системы», «Динамические интеллектуальные системы», «Современные архитектуры интеллектуальных систем», «Проектирование систем, основанных на знаниях».

Созданные на основе авторской (Г.В. Рыбина) задачно-ориентированной методологии построения ИЭС и инструментального комплекса АТ-ТЕХНОЛОГИЯ обучающие ИЭС и веб-ИЭС являются полнофункциональными интеллектуальными обучающими системами (ИОС), обеспечивающими реализацию всех базовых моделей ИОС (модель обучаемого, модель обучения, модель проблемной области, онтологии курсов/дисциплин и др.), а также решение комплекса задач интеллектуального обучения (индивидуальное планирование методики изучения учебного курса/дисциплины; интеллектуальный анализ решения учебных задач; интеллектуальная поддержка принятия решений).

На все оригинальные авторские методики, реализованные в обучающих ИЭС и веб-ИЭС, получены свидетельства о государственной регистрации программ для ЭВМ, а для проведения практических занятий написаны новые учебные пособия [1, 2]. Мониторинг процессов функционирования обучающих ИЭС и веб-ИЭС проводится исходя из требований к надежности и информационной безопасности систем.

Приведем примеры процессов, в рамках которых возможны возникновения угроз безопасности. Режим RunTime: организация веб-тестирования (очное и дистанционное); выявление навыков/умений обучаемых решать различные задачи, в том числе неформализованные и др. Режим DesignTime: формирование заданий к элементам курсов/дисциплин; формирование и загрузка материалов для обучающих воздействий; анализ результатов мониторинга (в рамках анализа данных и т.п.).

Контроль доступа необходимо осуществлять для следующих информационных ресурсов, использующихся в процессах функционирования обучающих ИЭС: учетные и личные данные преподавателей и обучаемых, включая психологический портрет; варианты заданий для компонентов выявления уровня умений обучаемых; все элементы прикладных онтологий различных курсов/дисциплин, включая задания и вопросы к отдельным элементам курсов/дисциплин; сгенерированные варианты тестов, предназначенные для выявления уровня знаний обучаемых; описание заданий, ограничений и информационных ресурсы (изображения, файлы и др.), разработанных для обучающих воздействий; результаты выявления уровня знаний и умений обучаемых (ответы на вопросы, «проблемные зоны», ошибки и др.).

В рамках описанных процессов рассматриваются следующие варианты возможных угроз: DDoS-атаки для перегрузки ПО; MITM-атаки для похищения и/или подмены данных; попытки подобрать пароли или использовать украденные учетные данные (Brute Force и Credential Stuffing); злоупотребление правами доступа; загрузка вредоносных файлов;

Для обеспечения информационной безопасности в обучающих ИЭС применяются следующие подходы: использование защищенных сетевых протоколов с шифрованием; установка брандмауэров и сетевых профилей безопасности для фильтрации типов и протоколов подключений; ограничение доступа из внешних сетей в рамках проведения контрольных мероприятий (использование VPN, фильтрация IP-адресов и др.); анализ журналов и логов получения доступа к вариантам заданий и процессам выявления уровня знаний/умений обучаемых.

Список литературы

1. Рыбина Г.В. Интеллектуальные обучающие системы на основе интегрированных экспертных систем: учебное пособие. М.: Директ-Медиа, 2023. 123 с.

2. Рыбина Г.В., Григорьев А.А. Практические занятия по методам и технологиям построения динамических интеллектуальных систем: учебное пособие. М.: НИЯУ МИФИ, 2024. 140 с.

УДК 004.056

Г.П. ГАВДАН, Д.А. ДЯТЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

О КАДРОВОМ ОБЕСПЕЧЕНИИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ ДЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Доклад посвящён рассмотрению проблем кадрового обеспечения подготовки специалистов по информационной безопасности в системе высшего образования для различных сфер критической информационной инфраструктуры (КИИ). Приоритетным направлением кадровой политики продолжает оставаться качество подготовки и привлечение к педагогической деятельности молодых специалистов в области информационной безопасности. В частности, актуальными остаются вопросы получения преподавателями профессиональных компетенций (знаний, умений, навыков), характерных для субъектов различных сфер КИИ. Решение данной проблемы возможно в системе дополнительного профессионального образования (ДПО) путем разработки соответствующих программ профессиональной переподготовки преподавателей.

Введение

На протяжении уже нескольких лет проблема подготовки кадров в области информационной безопасности (ИБ) не сходит со страниц СМИ и из уст многих государственных чиновников самого высокого ранга [1–4]. Требования по получению обучающимися практико-ориентированных компетенций ужесточаются [5]. Занятия со студентами (бакалавриата, специалитета, магистратуры и аспирантуры) должен проводить преподаватель, имеющий опыт работы по дисциплинам, связанными с обеспечением безопасности КИИ, однако проблема привлечения подобных специалистов, остаётся актуальной и требует решения.

Совершенствование кадрового обеспечения в вузах области КИИ

В настоящее время вопрос обновления критериев классификации специальностей, необходимых для разработки и дальнейшей эксплуатации решений системы обеспечения информационной безопасности значимых объектов КИИ остается открытым [4]. Одним из наиболее востребованных путей решения кадрового вопроса, например, технологической независимости в КИИ, является создание программ, направлений, лабораторий и центров на базе крупнейших технических вузов страны, выпускники которых будут готовы приступить к реализации

проектов КИИ [5]. Другим немаловажным вариантом остаётся «дообучение» уже готовых специалистов внутри компании или на курсах ДПО и повышения квалификации (ПК) [5]. Всем ясно, что хороший преподаватель по профильным дисциплинам должен быть экспертом в своей области [6]. Кроме того, существует материальная проблема, как с подготовкой, так и привлечением к преподаванию молодых специалистов. Высокие заработки специалистов (по сравнению с заработками ППС в вузе) в области ИБ крупных компаний являются достаточно весомым приоритетом у молодых специалистов при выборе ими профессии преподавателя.

Заключение

Потребность специалистов в области обеспечения безопасности значимых объектов КИИ существенно возросла после принятия ряда нормативных правовых актов и санкционных ограничений. Остаются нерешенными проблемы с подготовкой, подбором и материальным стимулированием кадров профессорско-преподавательского состава (ППС). При этом у большинства ППС нет необходимых компетенций в области КИИ. Для решения данной проблемы назрела необходимость разработать и реализовывать соответствующие программы профессиональной переподготовки преподавателей в области КИИ, и существенно поднять уровень материального стимулирования.

Список литературы

1. Белов Е.Б., Лось В.П., Зайцева О.М., Кузора И.В. О необходимости актуализации профессиональных стандартов в области информационной безопасности и информационных технологий // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 119.

2. Зегжда П.Д., Черненко В.Г. Интеграция университетов и промышленных компаний - путь к успеху. опыт Lgpolyrec // Защита информации. Инсайд. 2007. № 1 (13). С. 56–59.

3. Дорофеев А.В., Марков А.С. Обучение специалистов в области кибербезопасности в стиле Purple Team // Защита информации. Инсайд. 2023. № 6. С. 67–71.

4. Горбатов, Виктор С.; Дураковский, Анатолий П. и др. О профессиональных стандартах в интересах подготовки кадров по безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 54–68, дек. 2019. ISSN 2074-7136. Доступно на: https://bit.spels.ru/index.php/bit/article/view/1231. Дата доступа: 06 сен. 2024. doi: http://dx.doi.org/10.26583/bit.2019.4.04.

5. Е.Абакумов (выступление). Трек обзорно-дискуссионных заседаний «Доверенные РЭУ и ЭКБ для критической гражданской инфраструктуры». // Материалы 9-я научная конференция «ЭКБ и микроэлектронные модули», Форума «Микроэлектроника 2023» https://microelectronica.pro/albomyi-provedeniya-foruma-2023. Дата доступа: 11 октября. 2023.

6. Царегородцев, А. В. Кадры решают всё: назад в будущее / А. В. Царегородцев // Безопасные информационные технологии: Сборник трудов Двенадцатой международной научно-технической конференции, Москва, 01–02 ноября 2023 года. – Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2023. – С. 146–149. – EDN QUEMQM.

УДК 004.056

Г.П. ГАВДАН, В.Г. ИВАНЕНКО
Национальный исследовательский ядерный университет «МИФИ», Москва

К ВОПРОСУ О ПОДГОТОВКЕ ВЫСШЕЙ ШКОЛОЙ КАДРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСПЕКТЕ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Рассматриваются вопросы подготовки кадров по информационной безопасности в аспекте обеспечения технологической независимости критической инфраструктуры, не утратившие сегодня своей актуальности. Приоритетным направлением в Мире (в том числе и России) остаётся совершенствование Программы высшего образования и качественной подготовки выпускаемых кадров. Предметом исследования (в условиях существования различных угроз безопасности информации является Высшая школа. Проведённый анализ научных публикаций и др. источников по теме исследования показал, что в данной области имеются проблемы. По результатам работы установлено, что в данной области сегодня ещё имеются нерешенные вопросы.

Введение

Подготовка специалистов по направлению информационная безопасность (ИБ) продолжает оставаться достаточно важной и сложной задачей, которая, тем не менее, сегодня решается. Большинство специализированных кафедр вузов продолжают и реализовывать основные образовательные программы высшего образования, в меньшей степени уделяя внимание программам повышения квалификации (ПК) и профессиональной переподготовки (ПП) по направлению в аспекте обеспечения технологической независимости критической информационной инфраструктуры (ОТНКИИ) [1].

Подготовка Высшей школой кадров в области ИБ

По предварительным расчётам Госкорпорации «Росатом, для достижения и обеспечения технологического суверенитета России к 2027 г. понадобится около 51 тыс. специалистов, задействованных в создании и эксплуатации решений для КИИ, а к 2030 г. – 115 тыс. специалистов [2].

Направленность опубликованного Пентагоном Cyber Workforce Focus (CWF, «Плана реализации стратегии кибертрудовых ресурсов на 2023–2027 гг. годы»), является продолжением Стратегии кибербезопасности США на 2023–2027 гг. [3]. В нём представлены проблемные области, такие как выявление, набор, развитие и удержание. Программой предполагается устранение дефицита за счёт применение государственного и частного партнерства, и принятия

дополнительных специальных мер [4]. Обучение талантов и их поиск, необходимо начинать в детских садах и школах. Подростков и детей увлекать ИТ-технологиями, инженерией, математикой и кибернетикой [4]. Применение в Российской Федерации таких же мер явно бы способствовало ликвидации своего дефицита рабочей силы, что является важной задачей.

Развитие кадрового потенциала в области обеспечения ИБ в аспекте ОТНКИИ и применения информационных технологий (ИТ) может решаться самостоятельно, путем обучения персонала, дискуссий, тренингов, дебатов и др. в соответствии с Политикой подготовки персонала в сфере ИБ [5] в аспекте ОТНКИИ; реализацией Программ в вузах обязательно опираясь на опыт зарубежных коллег [6].

Заключение

Решение проблемы дефицита «кибербезопасников» в России (подготовки, ускорения найма и их удержания: военных, гражданских и служащих) что требует (также как и в США) разработки и принятия, специальных мер. Такое развитие кадрового потенциала по направлению информационная безопасность в аспекте ОТНКИИ должно в настоящее время решаться в России как можно быстрее и качественнее.

Список литературы

1. Гавдан, Г.П. Подготовка для Высшей школы кадров по информационной безопасности / Г.П. Гавдан, В. Г. Иваненко // Кибернетика и информационная безопасность «КИБ-2023»: Сборник научных трудов Всероссийской научно-технической конференции, Москва, 18–19 октября 2023 года. – М.: НИЯУ МИФИ, 2023. – С. 154–155. – EDN CSSFXG (дата обращения: 09.09.2024).

2. Е. Абакумов (выступление). Трек обзорно-дискуссионных заседаний «Доверенные РЭУ и ЭКБ для критической гражданской инфраструктуры». // Материалы 9-я научная конференция «ЭКБ и микроэлектронные модули», Форума «Микроэлектроника 2023» https://microelectronica.pro/albomyi-provedeniya-foruma-2023 (дата обращения:: 11.10.2023).

3. Мельников, Д.А. К вопросу о цели и задачах национальной образовательной инициативы США в области кибербезопасности / Д.А. Мельников, Г.П. Гавдан, И.А. Корсаков // Безопасность информационных технологий. – 2018. – Т. 25, № 2. – С. 23–37. – EDN XRDYBF , doi: http://dx.doi.org/10.26583/bit.2018.2.02 (дата обращения: 09.09.2024)..

4. Горбатов, Виктор С.; Дураковский, Анатолий П. и др. О профессиональных стандартах в интересах подготовки кадров по безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 54–68, дек. 2019. ISSN 2074-7136. Доступно на: https://bit.spels.ru/index.php/bit/article/view/1231. (дата обращения: 09.09.2024). doi:http://dx.doi.org/10.26583/bit.2019.4.04.

5. «DoD Cyber Workforce Strategy Implementation Plan 2023-2027» CLEARED For Open Publication (Jul 13, 2023) Department of Defense. OFFICE OF PREPUBLICATION AND SECURITY REVIEW. URL: https://dodcio.defense.gov/Portals/0/Documents/Library/CW-StrategyImplementationPlan.pdf (дата обращения: 19.09.2023).

6. «США не хватает сотен тысяч специалистов в области кибербеза». Эшелон в телеграм канале. URL: https://t.me/EchelonEyes/1834 (дата обращения: 19.09.2023).

УДК 004.056

В.Л. ЕВСЕЕВ[1], А.С. БУРАКОВ[2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Московский физико-технический институт (Национальный исследовательский университет), Московская обл., Долгопрудный*

ПОВЫШЕНИЕ ТОЧНОСТИ ОПРЕДЕЛЕНИЯ ДЕВИАНТНЫХ ГРУПП ОБУЧАЮЩИХСЯ С ПОМОЩЬЮ ПОИСКА ОПТИМАЛЬНЫХ ЦЕНТРОВ В МЕТОДЕ К-СРЕДНИХ

Исследована проблема скулшутинга в учебных заведениях. Обоснована актуальность данной проблемы. Предложено решение данной проблемы, в рамках которого предлагается использовать онлайн-профайлинг и комбинации с методами машинного обучения. Выявлен основной недостаток данного решения – трудности в определении изначальных центров кластеров. Предложен способ повышения точности кластеризации с помощью подбора наиболее оптимальных центров.

Введение

В современном мире человечество постоянно сталкивается с проблемами разного характера. Одна из самых страшных проблем – это девиации среди подростков и молодых людей, которые приводят к самоубийствам или же к шутингу в учебных заведениях.

В качестве решения данной проблемы предложен метод, с помощью которого предоставляется возможность обнаруживать девиантные группы обучающихся [1]. Метод предполагает сбор информации об обучающихся из открытых источников, например, социальных сетей и последующий ее анализ, на основе которого формируется условный уровень тревожности и агрессивности каждого обучающегося.

После этого среди обучающихся определяются четыре группы: группа без отклонений; группа, склонная у буллингу; группа, склонная к суициду и группа, склонная к скулшутингу.

Но, необходим способ для наиболее точной группировки обучающихся по вышеуказанным группам.

Текущий подход к решению проблемы.

В качестве метода машинного обучения использовался метод кластерного анализа k-средних [2]. Данный метод предполагает определение экспертом количества кластеров и их изначальных центров.

Если количество искомых групп заранее известно, то вот выбор изначальных центров неочевиден. При этом, выбор изначальных центров кластеров напрямую влияет на финальную кластеризацию, так как при одних выбранных центрах определенный ценник может попасть в группу обучающихся способных наложить на себя руки, а при другом наборе центров - он окажется в группе обучающихся без отклонений

Предлагаемое решение

С целью повышения точности кластеризации предлагается находить наиболее оптимальные центры кластеров. Для этого необходимо минимизировать среднее внутрикластерное расстояние [3]. Данная минимизация однозначно свидетельствует о более кучных кластерах, объекты в которых наиболее похожи друг на друга. Что позволяет значительно снизить вероятность ошибки при классификации обучающихся. Данный алгоритм реализован на языке программирования Python.

.

Заключение

Исследование позволило сделать ряд выводов, а именно:

1. В данном методе кластеризации в качестве метрики целесообразно использовать Евклидово расстояние.
2. Для отнесения обучающихся к той или иной группе, необходимо грамотно произвести выбор изначальных центров кластеров, которые напрямую влияют на финальную кластеризацию.
3. Для повышения точности кластеризации предлагается минимизировать среднее внутрикластерное расстояние.

Список литературы

1. Евсеев В.Л., Бураков А.С. Выявление девиантного поведения подростков методом кластерного анализа //Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность «КИБ-2023». Сборник научных трудов. 18-19 октября 2023 г. Москва. М.: НИЯУ МИФИ, 2023. – С. 158–159.
2. Стремоус М.А. Алгоритм кластеризации методом k-средних. // 58-я научная конференция аспирантов, магистрантов и студентов – 2022. – с. 191-193.
3. Дашкина Л.С. Обзор способов оценки качества кластеризации //Информационные технологии. – 2018. – С. 18–21.

УДК 004.056

Е.А. НЕЩЕРЕТНЯЯ
Научный руководитель – к.т.н., доцент В.С. ГОРБАТОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

К КОНЦЕПЦИИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА В СФЕРЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Цель данной работы - совершенствование подготовки кадров среднего звена для организаций обеспечения безопасности информации критической информационной инфраструктуры (КИИ) в условиях изменения требований к уровню подготовки и компетентности специалистов среднего профессионально образования (СПО).

Работа опирается на результаты исследования [1], в котором обосновано применение для достижения указанной цели законодательного механизма и терминологического аппарата КИИ. Сущность и структура образовательной деятельности в СПО выстраивается на основании ФЗ «Об образовании», согласно которым формирование профессиональных компетенций в рамках СПО осуществляется по двум основным составляющим:

- основная образовательная программа;
- профессиональное обучение с формированием профессиональных компетенций по защите информации с использованием программных, технических и криптографических средств защиты.

ФЗ регулирует широкий спектр вопросов от общего регулирования образовательного процесса, до частных вопросов материально-технического обеспечения учебного процесса, связанного со спецификой реализации программ по информационной безопасности гражданского сектора [1].

Однако с выходом Указа Президента РФ от 14 апреля 2022 г. № 203 «О Межведомственной комиссии Совета Безопасности РФ по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации» перед научным сообществом встал ряд сложных задач, в том числе задачи связанные с пересмотром процесса обучения молодых специалистов по информационной безопасности всех уровней подготовки, в том числе и среднего профессионального образования.

Вопрос, как и чему учить определен в ФГОС укрупнений группы 10.00.00. Учебный процесс — это многокомпонентный алгоритм,

включающий в себя ряд процедур, в том числе обеспечение учебно-методической литературой (рис. 1).

Рис.1 Структура обеспечения дисциплин(модуля)

Если задачи методолога-дидактического обеспечения процесса ВО и ДПО уже многие годы решались самостоятельно, путем пополнения научными работами молодых ученых и авторскими курсами отраслевых экспертов, то уровень СПО подобными приобретениями похвастаться не может.

Вопросы дидактического оснащения учебного процесса широко обсуждаются на разных уровнях педагогического и профессионального сообщества [2]. Учебники, предназначенные для учащихся СПО, представляют собой сокращённые версии учебников для вузов, без учёта специфики СПО. Нет синхронизации учебного материала с литературой, рекомендуемой профессиональными сообществами. Изобилие рекомендуемой экспертами к изучению дополнительной литературы вытесняет основную учебную, фактически делая рекомендованную литературу не валидной. Предлагается пересмотреть концепцию методического обеспечения учебной литературой профессионального цикла дисциплин, расширить список литературы привлечением к издательству отраслевых специалистов, сформировать единую профильную библиотеку для СПО по направлению ИБ.

Список литературы

1. Горбатов, Виктор С.; Эрдниев, Александр С. Совершенствование подготовки кадров по обеспечению безопасности информационной инфраструктуры органов внутренних дел. Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 100–119, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.06.

2. XVI общероссийская научно-практическая конференция педагогических работников 2023 года; конференция «Кадровый потенциал в сфере информационной безопасности // Университет Сириус URL: https://ib-bank.ru/kadry/ (дата обращения: 13.05.2024).

УДК 004.056

А.А. БЕРДЮГИН

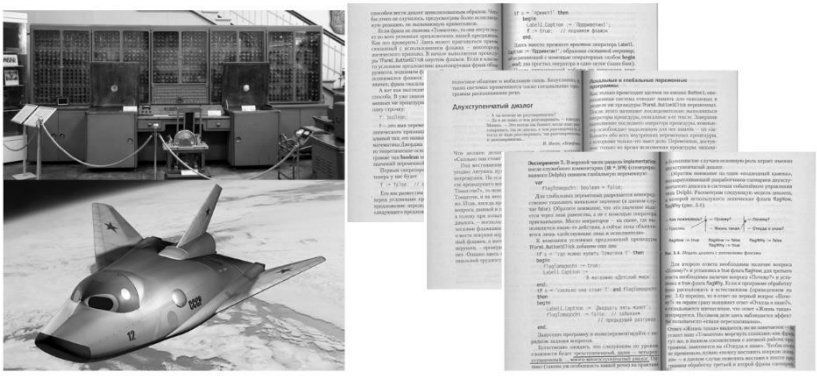
Финансовый университет при Правительстве Российской Федерации, Москва

ПРИЛОЖЕНИЕ PROGRESSQUEST: ВДОХНОВЛЯЯ МОЛОДЁЖЬ НА ПУТИ К ЦИФРОВОЙ ГРАМОТНОСТИ

Программа «Игра-викторина ProgressQuest с элементами Tamagotchi и Easter Egg», написанная автором на языке C# (библиотека Windows Forms .NET), может применяться для популяризации информационных технологий и информационной безопасности среди молодых людей, что отражено в документах Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Завершая обучение на курсах по программированию компании GeekBrains в рамках государственного проекта «Цифровые профессии», автор доклада разработал представленную компьютерную программу в качестве дипломного проекта. Специально адаптированное под нужды цифрового развития России, приложение представляет собой не только увлекательное развлечение, но и ценный образовательный инструмент.

Основой для разработки программы стала экономическая стратегия – десктопная игра «Компьютерщик», которая вышла в далёком 1998 г. и до настоящего времени прекрасно работает на современных компьютерах. В текстовой части диплома содержатся не только главы о практическом создании программы, но и полезная, интересная теория (рис. 1).



Немного истории развития IT и ЭВМ в СССР

Контекст диалога в давних чат-ботах через логические флаги

Рис. 1. Полезная и интересная теория в текстовой части работы

Особенностью программы является возможность отвлечения внимания пользователя от тестирования во время проведения этого тестирования. Это обеспечивают элементы игры «Тамагочи», а также мультимедийные эффекты (рис. 2). Ведь в реальной жизни не всегда удаётся сосредоточенно работать над вопросами, встающими перед нами.

Одна из функциональных возможностей приложения – это запуск спрайтовой игры («пасхального яйца», как это называется в крупных играх) «Zахватчики – invaderZ» при определённых действиях.

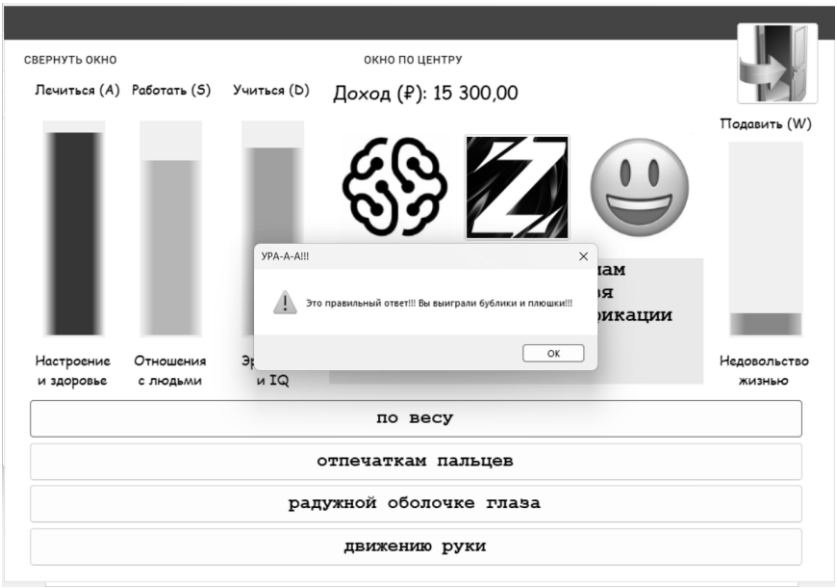


Рис. 2. Интерфейс программы ProgressQuest

По материалам дипломного проекта была проведена регистрация программы для ЭВМ в Федеральной службе по интеллектуальной собственности (ИС) «Роспатент» [1]. Внимание к сфере ИС – это дополнительные возможности для развития науки и технологий России.

Список литературы

1. Игра-викторина ProgressQuest с элементами Tamagotchi и Easter Egg: Рос. Федерация. № RU 2024612236 / Бердюгин А.А., Ревенков П.В.; регистр. 25.01.2024; опубл. 30.01.2024. URL: https://www.elibrary.ru/item.asp?id=60782497 (дата обращения 25.09.2024).

УДК 004.056

Н.Г. МИЛОСЛАВСКАЯ, А.И. ТОЛСТОЙ

Национальный исследовательский ядерный университет «МИФИ», Москва

ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОДГОТОВКИ МАГИСТРОВ ДЛЯ ЦЕНТРОВ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КОМПЬЮТЕРНЫХ АТАК

Рассматриваются вопросы, посвящённые подготовке профессионалов в актуальной в настоящее время области, относящейся к обеспечению защищенности объектов в условиях реализации компьютерных атак. Целью работы является определение компетентностных требований к уровню подготовки кадров выбранного направления с учетом требований профессиональных стандартов и на базе этого формулирование основных положений, необходимых для реализации учебного процесса. Результатом работы является разработка основной образовательной программы подготовки магистров по программе «Центры обнаружения и предотвращения компьютерных атак» (направление 10.04.01).

В настоящее время результативное обеспечение информационной безопасности (ИБ) различных объектов достигается не только путем разработки и эксплуатации систем обеспечения ИБ таких объектов, но и созданием и активным использованием центров, которые своевременно обнаруживают и предотвращают компьютерные атаки. В работе таких центров должны участвовать профессионалы, обладающие необходимыми профессиональными компетенциями.

Анализ действующих образовательных стандартов показал отсутствие требований и рекомендаций по подготовке таких профессионалов. Требуемый высокий уровень профессиональной подготовленности, который должен быть сформирован за короткое время объясняет выбор магистратуры в качестве образовательной базы и ращение разработки и внедрения в НИЯУ МИФИ уникальной магистерской программы ЦОПКА – «Центры обнаружения и предотвращения компьютерных атак» (направление 10.04.01 ИБ).

Цели программы: подготовка магистров, способных успешно работать в сфере деятельности, связанной с проектированием, внедрением и эксплуатацией центров обнаружения и предотвращения компьютерных атак, обеспечивающих сетевую безопасность информационно-телекоммуникационных сетей организаций высокотехнологических

областей, с обеспечением непрерывности функционирования таких объектов в условии существования угроз в информационной сфере, анализом и оценкой уровня ИБ, а также реагированием на компьютерные инциденты и их предотвращением. В результате освоения программы выпускник получит набор универсальных, общепрофессиональных и профессиональных компетенций для решения проектных, научно-исследовательских и организационно-управленческих задач профессиональной деятельности.

Профессиональные компетенции (ПК), которые должны быть сформированы при подготовке магистров по программе ЦОПКА были определены с учетом положений профессионального стандарта ПС 06.053 «Специалист по информационной безопасности в кредитно-финансовой сфере» [1], который сформулировал соответствующие трудовые функции, трудовые действия и рекомендации к их знаниям и умениям.

ПК были положены в основу разработки Основной образовательной программы (ООП) магистратуры ЦОПКА, куда вошли следующие методические документы: Компетентностная модель выпускника, Рабочий учебный план и календарный учебный график, Рабочие программы учебных дисциплин (модулей) и практик, Учебно-методические комплексы отдельных учебных дисциплин, Программа государственной итоговой аттестации.

При реализации ООП планируется не только изучение теории под руководством ведущих преподавателей НИЯУ МИФИ, но и формирование практических навыков на основе решения реальных задачах от партнеров университета с использованием современных средств защиты информации. Обучающиеся будут учиться анализировать и оценивать риски и уровень ИБ, реагировать на компьютерные инциденты и предотвращать их, строить SOCи, осуществлять OSINT, работать в команде и в одиночку и многое другое.

ООП прошла экспертизу в организациях, потенциальных потребителей выпускников.

Список литературы

1. Профессиональный стандарт ПС 06.053 «Специалист по информационной безопасности в кредитно-финансовой сфере» (Приказ Минтруда России от 28 ноября 2022 г. № 739н. Зарегистрирован в Минюсте России 22.12.2022 рег.№ 71784).

ИМЕННОЙ УКАЗАТЕЛЬ АВТОРОВ СТАТЕЙ

Вторая Всероссийская научно-техническая конференция
«Кибернетика и информационная безопасность»

«КИБ-2024»

Сборник научных трудов

Ответственный редактор И.М. Ядыкин

Подписано в печать 10.10.2024. Формат 60x84 1/16.
Печ. л. 18,25. Уч.-изд. 18,5. Тираж 200 экз.
Изд. №019-2. Заказ № 78

Национальный исследовательский ядерный университет «МИФИ»
Типография МИФИ
115409, Москва, Каширское ш. 31