Национальный исследовательский ядерный университет «МИФИ»

Всероссийская научно-техническая конференция

«Кибернетика и информационная безопасность»

«КИБ-2023»

Сборник

научных трудов

18–19 октября 2023 г., Москва

Москва 2023

УДК 004.056 : 001(06)
ББК 32.973.202
В85

Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность «КИБ-2023». Сборник научных трудов. 18-19 октября 2023 г., Москва. М.: НИЯУ МИФИ, 2023. 168 с.

Настоящая книга содержит тезисы научных работ и докладов, предложенных специалистами на конференции «КИБ-2023».

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 20.09.2023

ISBN 978-5-7262-2997-3

СОДЕРЖАНИЕ

ДОВЕРЕННОЕ ПО
И БЕЗОПАСНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

ЗАЩИЩЕННЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ

ПРОМЫШЛЕННАЯ КИБЕРБЕЗОПАСНОСТЬ

ТЕОРЕТИЧЕСКАЯ И ПРАКТИЧЕСКАЯ КРИПТОГРАФИЯ

ФИНАНСОВАЯ И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ВЫСШЕЙ ШКОЛЫ

КИБ-2023
КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Доверенное ПО
и безопасный искусственный интеллект

Руководитель секции – Загребаев А.М., д.ф.-м.н.,
заведующий кафедрой №22

УДК 004.056

А.С. МАРКОВ

Научно-производственное объединение «Эшелон», Москва
Московский государственный технический университет им. Н.Э. Баумана

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В докладе сделан обзор области создания безопасного программного обеспечения в стране. Предложена матрица атак на разработку безопасного программного обеспечения. Приведены оригинальные концептуальные модели разработки безопасного программного обеспечения. Предложен методический подход к аудиту разработки безопасного программного обеспечения. Приведены статистические данные по внедрению безопасных процедур в серийное производство программных средств защиты информации.

Введение

В [1-3] показано, что внедрение процедур разработки безопасного программного обеспечения позволяет существенно сократить число уязвимостей. В настоящее время в стране сложилась нормативно-правовая база разработки безопасных программ и накоплен опыт внедрения процедур безопасной разработки, обзору чего и посвящен данный доклад.

Концептуальные модели разработки безопасного программного обеспечения

Для автоматизации процесса разработки безопасных программ предложено использовать ряд концептуальных моделей. В качестве примера можно привести теоретико-множественную модель, которая характеризуется кортежем [4]:

$\mathbf{C}=\langle B, U, P, O, R, F_0, F_R, F_C\rangle$,

где: $B = \{\beta_1, \beta_2, \ldots, \beta_{24}\}$ – множество требований по разработке безопасного ПО (по ГОСТ Р 56939);

$U = \{u_1, u_2, \ldots, u_a\}$ - множество угроз ИБ, которые являются актуальными для среды разработки программ (по ГОСТ Р 58412);

$P = \{p_1, p_2, \ldots, p_b\}$ - множество идентифицированных положений политик ИБ, которым должна соответствовать среда разработки программ (по аналогии с ISO/IEC 15408);

$O = \{o_1, o_2, \ldots, o_c\}$ - множество целей разработки безопасных программ (по аналогии с ISO/IEC 15408);

$R = \{r_1, r_2, \ldots, r_d\}$, $R \subseteq B$, $d \leq 24$ - подмножество требований, подлежащих выполнению:

F_0: $U \cup P \rightarrow O$ – процедура формирования целей разработки безопасного ПО;

F_R: $B \cup O \rightarrow R$ – процедура выбора требований по разработке безопасного ПО;

F_C: $R \rightarrow C$ – процедура синтеза контрмер разработки безопасного ПО;

$C = \{c_1, c_2, \ldots, c_e\}$ – множество мер разработки безопасного ПО.

Процедуры разработки безопасных программ удобно представлять в виде полуформальных моделей (диаграмм) [5].

В докладе будет представлена статистика по аудиту разработки безопасного программного обеспечения на примере 40 проектов [6, 7].

Заключение

Исследование позволило сделать ряд выводов, а именно:

1. Национальные стандарты ГОСТ Р 58412-2019 и ГОСТ Р 56939-2016 зарекомендовали себя очень хорошо в реализационном плане, направление стандартизации продолжает развиваться.

2. Внедрение даже отдельных процедур разработки безопасных программ существенно повышает уровень безопасности, надежности и качества программных средств.

Список литературы

1. Жидков И.В., Зубарев И.В., Хабибуллин И.В. Выбор рациональной модели разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2021, № 5(45), с. 21–29.

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

3. Петренко С. А. Киберустойчивость цифровой экономики: научно-популярная монография. СПб.: Питер. – 2021. – 384 с.

4. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения. // Вопросы кибербезопасности. 2015, № 5(13), с. 2–10.

5. Гришин М.И., Марков А.С., Цирлов В.Л. Практические аспекты реализации мер по разработке безопасного программного обеспечения // ИТ-Стандарт. 2019. № 2 (19). С. 29–39.

6. 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.

7. 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 (March 22-24, 2023, St. Petersburg Russia), IEEE, 2023, p. 48–54.

УДК 004.8

С.В. ГАРБУК

Национальный исследовательский университет «Высшая школа экономики»

СТАНДАРТИЗАЦИЯ КАК МЕХАНИЗМ УСТРАНЕНИЯ РИСКОВ ПРИ СОЗДАНИИ И ПРИМЕНЕНИИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Целью данной работы является обоснование представительной совокупности требований к системам искусственного интеллекта (ИИ) в области функциональной корректности, максимально полно учитывающей интересы и приоритеты различных заинтересованных сторон и позволяющей избежать существенных рисков при создании и применении систем ИИ.

Структура рисков, обусловленных нарушением функциональной корректности систем ИИ (СИИ), может быть обоснована в разрезе приоритетов различных заинтересованных сторон: непосредственно участвующих в создании и применении СИИ (акторов ИИ) и третьих лиц. При этом целесообразно выделять следующие виды угроз, обусловленных нарушением функциональной корректности СИИ:

- угрозы жизни и здоровью людей, экологические угрозы;
- угрозы информационной безопасности в отношении заинтересованных сторон;
- нарушение этических и других норм «мягкого» права;
- неопределенные потребительские свойства, не влияющие непосредственно на безопасность жизни и здоровья людей, экологическую безопасность.

Наиболее опасные угрозы и, соответственно, наиболее важные характеристики и требования связаны с обеспечением безопасности жизни и здоровья людей, а также с предотвращением крупных инцидентов экологической безопасности.

Особый вид требований связан с предотвращением угроз информационной безопасности (ИБ) в отношении заинтересованных лиц, вызванных нарушением функциональной корректности СИИ. Если в таких системах предполагается обработка персональных данных или некорректная работа систем может привести к реализации деструктивных информационно-психологических воздействий на общество, то в формировании требований ИБ к таким СИИ заинтересованы общество в целом и государственные регуляторы [1].

Для многих прикладных СИИ специфичны угрозы этического характера и другие угрозы, предотвращение которых достигается реализацией мер т.н. «мягкого» права. К таким СИИ относятся, например, системы в кредитно-финансовой сфере и в области образования, поисково-справочные, маркетинговые и иные информационные системы, использующие методы персонализации на основе ИИ.

Для СИИ, не предназначенных непосредственно для решения задач в области безопасности и не представляющих угрозы для жизни, здоровья людей и окружающей природной среды, отклонение функциональных характеристик от установленных требований ограничивается ухудшением потребительских свойств систем.

Часть требований предъявляется непосредственно к характеристикам СИИ, а часть – к характеристикам процессов жизненного цикла (ЖЦ) систем. Степень соответствия требованиям непосредственно к системам ИИ корректно рассматривать в контексте определённой прикладной задачи и в определённых (предусмотренных) условиях эксплуатации, а к процессам ЖЦ – вне какого-либо контекста, с учетом действующих норм и правил.

Формирование требований к СИИ, не дублирующих общие стандарты в области ИТ и отраслевые стандарты, достигается за счёт функциональной декомпозиции СИИ на основе иерархической модели, выделяющей алгоритмы машинного обучения в составе комплексных объектов автоматизации.

Предложенный подход к обоснованию требований к системам ИИ может быть использован при формировании комплекса национальных стандартов в области искусственного интеллекта.

Список литературы

1. Гарбук С.В. Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности. 2021. № 3 (43). С. 68–83. DOI: 10.21681/2311-3456-2021-3-68-83

УДК 519.766.4:004.032.26

МИНАЕВ В.А.
Московский университет МВД России им. В.Я. Кикотя

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ СОЦИАЛЬНЫХ МЕДИА НА ОСНОВЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Разработано математическое и программно-алгоритмическое обеспечение, позволяющее автоматизировать систему оценки социальных медиа на наличие в них текстового контента экстремистского характера. Решена задача поиска и обнаружения материалов экстремистской направленности на основе использования глубинной искусственной нейронной сети BERT. Разработана компьютерная программа, позволяющая в автоматизированном режиме в режиме реального времени осуществлять анализ Telegram-каналов. Проведен ряд вычислительных экспериментов, по результатам которых оценена распространенность экстремистских сообщений в различных категориях социальных медиа (СМ) – социальных сетях и мессенджерах.

Учитывая многоплановость обостряющейся проблемы кибербезопасности, ее исследования предполагают решение многих задач анализа, оценки и прогнозирования распространения деструктивной информации в информационных сетях.

Ценность получаемых при этом научных результатов заключается в новых возможностях методологического обеспечения аналитической деятельности, все более связанной с обработкой и анализом больших данных (Big Data).

Для выбора наиболее эффективного классификатора деструктивного контента проведен анализ десяти наиболее распространенных моделей интеллектуальной классификации. В результате выбраны три наиболее перспективные. Среди них: метод опорных векторов – SVM, рекуррентная нейронная сеть – GRU, классификатор на основе трансформера BERT. При отсутствии шумовых факторов все три классификатора показывают сходное качество работы. Однако при добавлении шумового контента, присутствующего в реальном информационном обмене, наиболее шумостойким является классификатор на основе BERT.

В соответствии с F-мерой классификации наилучшая модель RuBERT-base показывает не менее 97% точности классификации текстов с содержанием идеологии антисемитизма, радикального ислама, нацизма.

Для более детальной оценки программно-алгоритмического обеспечения и оценки эффективности выявления экстремистских материалов сделана и исследована выгрузка реальных данных из 68 случайно выбранных телеграмм каналов.

Каналы сгруппированы с помощью детальных экспертных процедур по восьми категориям. Исследования показали, что группы каналов распределились по выявленной в них доле экстремистских сообщений следующим образом (новостной – 5%, еврейской культуры – 10%, пользовательский – 20%, исламской культуры – 20%, исторический – 22%, националистический – 40%, террористический – 50%, нацистский – 80%).

Проведенные исследования показали эффективность разработанного метода. Его работоспособность и реализуемость доказана результатами применения соответствующего программного продукта. Целесообразно использовать созданный программный продукт и его методическое обеспечение в работе государственных структур, занимающихся выявлением контента противоправного характера в СМ.

Методика выявления и идентификации контента экстремистской направленности, базирующаяся на нейронных сетях, является перспективным направлением применении искусственного интеллекта для исследования СМ.

Высокая точность распознавания деструктивности текстов позволяет использовать полученные результаты для практического совершенствования работы по противодействию распространению идеологии терроризма и экстремизма в СМ. Эта точность необходима для принятия эффективных мер по противодействию и иным деструктивным воздействиям в соцсетях.

Полученные результаты целесообразно учитывать при выявлении информационных воздействий на молодое поколение россиян при склонении подростков к суицидальному поведению, вовлечении их в различные опасные сообщества и мероприятия (руферы, зацеперы, последователи уголовной культуры, противодействующие на территории России разными способами проведению СВО и т.п.).

Такое направление использования современных методов искусственного интеллекта позволяет активизировать деятельность силовых и правоохранительных структур, органов власти, образовательных учреждений страны в самых актуальных направлениях противоборства с деструктивными факторами влияния социальных медиа.

УДК 004.056

И.А. СОЗЫКИН[1], Р.В. ДЗВИНКО[2], В.Д. ПАСТУХОВ[1]

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

[2]*НПЦ «Бизнесавтоматика», Москва*

МОДЕЛЬ ПАТЧ-АТАК НА НЕЙРОСЕТЕВОЙ КЛАССИФИКАТОР ИЗОБРАЖЕНИЙ

Глубокие нейронные сети (ГНС) успешно используются в задачах классификации изображений. Однако их эффективность снижается за счет угроз применения нарушителем так называемых состязательных атак. Одной из возможных состязательных атак является патч-атака, изменяющая небольшую локальную область изображения с целью обмана классификатора. В докладе предложена модель такой атаки. Выполненная формализация позволит разработать эффективные меры защиты от патч-атак.

Дано: изображения $X \in R^{W \times H \times C}$, где W – ширина, H – высота, C – число каналов изображения;

$Y = \{0,1, \dots, N-1\}$ – пространство меток классификации;

$f: X \to Y$ – модель (классификатор).

Входной набор данных модели: $Z = X$ x Y.

Атакующий может модифицировать пикселы в некотором регионе изображения. Защитник знает оценку верхней границы размера площади возможной области искажений, но не знает, где она расположена.

Пусть патч моделируется бинарной маской $p \in P \subseteq \{0,1\}^{W \times H}$.

Тогда набор ограничений нарушителя $A(X)$ может быть выражен как

$$\{x' = (1-p) \odot x + p \odot x''\} | x, x' \in X, x'' \in R^{W \times H \times C}, p \in P,$$

где $\odot$ - операция поэлементного умножения, x' – измененное изображение x'' - патч нарушителя.

Рассмотрим более подробно действия нарушителя.

Пусть имеется алгоритм обучения A и его входное пространство $Z = X \times Y$ (декартово произведение пространства изображений и их меток). Для обучающего датасета $S \in Z$ и данного изображения $z = (x, y) \in Z$ определим функцию выхода модели $q(z; S)$ как некоторую метрику, оцениваемую на входе z после обучения модели на множестве S. Определим также результативность функции выхода модели, обученной на датасете S по отношению к датасету S`:

$$Perf(S \to S`) = \frac{1}{|S`|} \sum_{z \in S`} q(z; s).$$

При проведении бэкдор-атаки нарушитель наблюдает чистый датасет S и выбирает для внедрения триггера некоторую долю $\alpha \in (0,1)$ изображений этого датасета. Далее атакующий выполняет:

а) разделение датасета S на два множества S_p и S_C, где $|S_p| \leq \alpha|S|$ – множество атакуемых изображений;

б) выбирает функцию внесения триггера $\tau: Z \to Z$ (например, внедрение фиксированного набора бит и установление определенной метки). Выполняет преобразование $P = \tau(S_p)$ и замещает исходные изображения в S_p. Пусть $\tau(S`)$ для любого множества S` означает множество $\{\tau(z): z \in S`\}$. Тогда цель атакующего для заданного множества $S`$ разработать P и τ, удовлетворяющие двум свойствам:

1) эффективность. Отравленная модель должна быть уязвимой к триггеру. То есть, $Perf\left(S_C \cup P \to \tau(S`)\right)$ должна быть велика;

2) незаметность. Обученная на отравленных данных модель должна вести себя почти также, как и модель, обученная на чистых данных. То есть, $Perf(S_C \cup P \to S`) \approx Perf(S \to S`)$.

То есть цель нарушителя: для данной модели f, изображения x, истинной метки y найти изображение $x' \in A(X) \subseteq X$ такое, что $f(x') = y'$, где $y' \neq y$ – произвольная метка.

Цель защитника: разработать модель (алгоритм обнаружения)

$$g = (f, v): X \longrightarrow Y \times \{0,1\},$$

где $g(x) = \{f(x), v(x)\}$,

$f(x) \in Y$ – результат классификации,

$v(x) \in \{0,1\}$ – результат верификации («1» означает, что результат классификации верифицирован).

Верифицированное подмножество назовем областью робастности и обозначим: $X_{\text{роб}} = \{x \in X | v(x) = 1\}$. Это – та область, где патч-атака нарушителя будет неуспешна (так как обнаружена). Таким образом, либо $f(x) = f(x')$ либо $v(x) = 0$ (будет выполнено отбрасывание изображения).

Задачей защитника является максимизация отношения $r_{\text{роб}} = \frac{X_{\text{роб}}}{X}$ и точности классификатора в робастной области $acc_{\text{роб}} = \mathbf{E}_{x \in X_{\text{роб}}}[l(f(x), y)]$, где l – функция ошибки (0,1).

Список литературы

1. Jaydip Sen J., Dasgupta S. Adversarial Attacks on Image Classification Models – FGSM and Patch Attacks and their Impact / In Information Security and Privacy in the Digital World - Some Selected Topics [Working Title]. IntechOpen, Jul. 26, 2023. doi: 10.5772/intechopen.112442.

УДК 004.057.5, 004.92

А.А. БОРЗЯК, Р.С. СМИРНОВ
АО «Россети Цифра», Москва

РАЗРАБОТКА НАДЕЖНОГО ПО НА ПРИМЕРЕ ДВУХ ПРОГРАММ МОДЕЛИРОВАНИЯ И ВИЗУАЛИЗАЦИИ

В настоящее время в России активно проводится политика импортозамещения в области создания программного обеспечения (ПО). Цель работы – определение приемов написания надежного ПО. В статье анализируются две программы моделирования и визуализации. Определены факторы, повышающие надежность ПО.

Начиная с 2020 г., авторы принимали участие в разработке двух программ моделирования и визуализации. Первая программа MathPanel [1] написана на языке C# и предназначена для использования в учебном процессе путем обучения методам компьютерного моделирования и визуализации, программированию на языках C# и JavaScript. Для упрощения разработки моделей реализована поддержка скриптов на языке C# и Программный Интерфейс Приложения (ПИП – от английского API – Application Programing Interface). Также MathPanel может быть использована для визуализации научных результатов. Код MathPanel находится в репозитории https://github.com/aborziakX/MathPanel .

В настоящее время в России растет интерес к разработке кроссплатформенных приложений на языке C++ [2], при этом ключевым моментом становится использование свободного ПО с открытым исходным кодом. Для C++ доступны свободно распространяемые компиляторы под лицензией GNU GPL. При компьютерном моделировании сложных процессов традиционным является разбиение задачи на обработку в 3-х модулях, к которым относятся:

– препроцессор (задание исходных данных решаемой проблемы),

– процессор или решатель (собственно моделирование),

– постпроцессор (визуализация результатов моделирования).

Было проведено исследование доступных кроссплатформенных графических библиотек с открытым исходным кодом на предмет использования в препроцессоре. Выбор сделан в пользу FLTK (Fast Light Toolkit - быстрый и легкий инструментарий) [3]. Компиляция не требует дополнительных библиотек, большое число элементов интерфейса пользователя и утилита для OpenGl, более 60 примеров использования, есть коллектив, который делает обновления в репозитории git.

Используется в научных проектах.

С использованием FLTK был разработан препроцессор [4]. Гибкость его работы обеспечивается управляющим файлом beat.ini, который содержит секции:

[Features] #Физические свойства задачи моделирования,

[Parameters] #диалоги для выбора параметров моделирования,

[Contols] #параметры генерации.

Препроцессор в начале работы загружает файл beat.ini и формирует свои структуры данных. Появляется интерфейс пользователя, который содержит:

– вверху меню команд;

– слева расположена древовидная структура из секций, содержащих объекты;

– справа окно для визуализации условий задачи.

Затем можно приступить к определению геометрии задачи. Команды создания геометрических примитивов включают добавление: сферы, ящика, цилиндра, конуса, линии, датчика. После создания геометрического объекта его можно редактировать и задавать физические свойства. Когда геометрия задана и настроены параметры, можно сгенерировать ini-файл для конкретного проекта. Код препроцессора находится в репозитории https://github.com/aborziakX/grasp .

В процессе разработки были определены факторы, повышающие надежность ПО:

– использование библиотек с открытым исходным кодом,

– кроссплатформенная реализация,

– реализация авто-тестирования для уменьшения ошибок в новых сборках,

– повышение модульности приложения (микро-сервисы, обмен командами между модулями через клиент-серверное взаимодействие),

– документирование и применение «хороших практик программирования»,

– использование программ для нахождения уязвимостей в исходном коде.

Список литературы

1. Борзяк А.А., Топорков В.В., Емельянов Д.М., Самочёрнов О.И., Смирнов Р.С. Основы компьютерного моделирования и визуализации. Издательство «Лань», 2022, 244 с., ISBN 978-5-507-44951-4

2. Страуструп Бьёрн. Дизайн и эволюция языка-С++. ДМК Пресс, 2016. 446 с. ISBN: 978-5-97060-419-9

3. B. Spitzak et al., 2022. Fast, Light Toolkit (FLTK). Online: http://www.fltk.org/.

4. Борзяк А.А., Смирнов Р.С. Кроссплатформенная реализация препроцессора для моделирования систем // ИТНОУ. 2023. №1. С.20–25, ISSN: 2587-6309

УДК 004.032.26

А.М. БУЛЫГИН, К.Я. КУДРЯВЦЕВ
Национальный исследовательский ядерный университет «МИФИ», Москва

РАЗРАБОТКА АЛГОРИТМА – «ПЕРСОНАЛЬНЫЙ ТРЕНЕР»

Разработан алгоритм многоклассовой классификации упражнений в режиме реального времени и подсчёта количества повторений на основе разработки группы исследователей из MediaPipe [1]. В отличие от решений с постобработкой данных [1–3], решение переведено из оффлайн области в режим реального времени. Рассматриваются различные классификаторы и методы подсчёта количества упражнений для получения лучших значений точности, а количество упражнений увеличивается до восьми штук.

В последние 20 лет наблюдается стремительный рост виртуальной коммуникации за счёт бурного развития технологий [4]. Виртуальные ассистенты всё сильнее внедряются в нашу жизнь, так как позволяют решить большой спектр рутинных задач, на которых нет желания сосредотачивать своё внимание. Согласно статистике исследования Clutch 2019 года, около 27% людей используют виртуальных помощников для выполнения своих повседневных дел. [5].

В любом деле, где результата нельзя достичь мгновенно необходима последовательность в своих действиях, особенно при занятии спортом. В случае отсутствия возможности в определённый момент платить персональному тренеру, человеку приходится прекращать персональные тренировки, что может в перспективе негативно сказаться на достигнутом ранее результате [5]. Самостоятельные занятия для человека, несвязанного со спортом, в зависимости от техники выполнения упражнений могут, как улучшить здоровье, так и наоборот испортить его, вплоть до необратимых последствий. Таким образом, ощущается необходимость и актуальность разработки приложения, нацеленного на поддержание уровня здоровья человека, стеснённого социальными и экономическими условиями, с помощью алгоритма распознавания позы и циклических движений для подсчёта выполненных им упражнений с возможной рекомендацией относительно следующих шагов.

Для анализа различных видов классификаторов подготовлены датасеты, один из которых синтетически расширен в четыре раза с помощью изменения координат, отвечающих положениям различных частей тела в небольшом диапазоне (~2%). Количество классов в датасетах увеличено до восьми штук. Среди них присутствуют близкие по технике выполнения

упражнения, такие как тяга верхнего блока к груди и подтягивания, для анализа способности алгоритма машинного обучения к их правильной классификации. Координаты положения точек тела в пространстве не следует подавать на вход классификатору, в отличие от производных от них величин, так как избыточность входных данных может приводить к неправильному обучению классического метода машинного обучения.

В данной задаче на вход подаются хорошо структурированные числовые векторы, поэтому выбор классических методов машинного обучения более чем оправдан в рамках данной задачи. Посредством варьирования параметров различных классификаторов и использования, разных датасетов на основе точности, f1-score и матрицы ошибок делается выбор в пользу одного из них.

Для подсчёта количества повторений было предложено несколько подходов различных по своей методике. Первый подход, наиболее простой по своей идее и реализации, выбирает из всех возможных классов тот, который обладает максимальным значением вероятности. Второй и третий подходы, учитывающие первые два и три значения классов, дают наиболее близкое к эталону количество повторений для различных упражнений.

Предложенный алгоритм онлайн классификации позы человека и анализа циклических движений, основанный на оффлайн методе подсчёта повторений для одного класса упражнений MediaPipe Pose [1], может быть внедрён в системы, связанные с физической активностью человека, и может быть полезен как людям, не связанным со сферой спорта, так и профессиональным спортсменам и оздоровительными центрам в качестве системы контроля качества и количества выполненных упражнений.

Список литературы

1. Pose Classification [Электронный ресурс] // MediaPipe. – 2023. – URL: https://github.com/google/mediapipe/blob/master/docs/solutions/pose_classification.md (дата обращения: 02.09.2023).

2. G. Taware, R. Agrawal, P. Dhende, P. Jondhalekar, S. Hule, AI-based Workout Assistant and Fitness guide. // International Journal of Engineering Research & Technology (IJERT). – 2021. – № 10(11).

3. Building an AI for Real-Time Exercise Recognition using Computer Vision & Deep Learning // GitHub. – 2023. – URL: https://github.com/chrisprasanna/Exercise_Recognition_AI (дата обращения: 02.09.2023).

4. Руденко Е.С. Виртуальная коммуникация как психологический феномен. // Научный результат. Педагогика и психология образования. – 2020. – № 2. – С. 45–50.

5. Centers for Disease Control. Prevalence of no leisure-time physical activity-35 States and the District of Columbia, 1988–2002. // MMWR. – 2004. – № 53. – С. 82–86.

УДК 004.05

М.Ю. ТОЛСТЫХ
Московский государственный лингвистический университет

СРЕДСТВА ПРОТИВОСТОЯНИЯ ФЕЙКОВОЙ ИНФОРМАЦИИ КАК УГРОЗЕ ИНФОРМАЦИОННОЙ И НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Рассматривается фейковая информация как угроза национальной безопасности. В качестве оригинального решения предлагается модель верификации подозрительного контента, которая может применяться как система поддержки принятия решений при работе с дипфейками.

По мере изменения общего медийного ландшафта использование цифровых инструментов для информирования людей и активизации гражданского обсуждения замещается деструктивной работой злоумышленников в направлении умелой эксплуатации преимуществ социальных и цифровых платформ с целями обмана, введения в заблуждение или нанесения вреда отдельным категориям граждан, а также целым государствам путем создания или распространения фейков.

Под дипфейком обычно понимают видео, в которых лицо и (или) голос человека изменены с помощью программного обеспечения (ПО) таким образом, чтобы измененное видео выглядело аутентичным. Манипуляции с лицом могут быть разделены на следующие категории: синтез лица, обмен лицами, модификация черт лица и его выражения [1].

Для обнаружения поддельных синтетических изображений разработаны различные программные подходы, наиболее распространен подход, при котором используются слои внимания поверх карт признаков [2], чтобы выделить обработанные области лица. Их сеть выводит бинарное решение о том, является ли изображение реальным или поддельным.

Предлагается конструирование ПО, представляющего собой систему поддержки принятия решений (СППР), основанную на обучении нейронных сетей (НС), которая может быть интегрирована в процессы верификации подозрительного контента в форме изображений и видео.

Охарактеризуем этапы и содержание работ по обучению сетей, т.е. построению модели, в том числе математической, являющиеся базой предлагаемого программного решения задачи распознавания дипфейков.

Набор данных для построения и обучения модели содержит 1000 исходных достоверных видео с докладчиками. Для каждого

компонента применена одна из модификаций, реализуемых приложениями: Deepfakes, Face2Face, FaceSwap, NeuralTextures.

Для целей исследования выбран Deepfakes – датасет. Для выделения лица докладчика используется функционал «insightface» с доработкой в виде фреймофрков, предложенных на платформе «Github».

Конвейер обучения модели представляет набор итераций, используется его простейшая архитектура: вырезание лица; сложение трех изображений по каналам; решение задачи бинарной классификации с помощью сверточной НС ResNet50. Решение проблемы деградации выполнено путем внедрения глубокой остаточной структуры сети.

Результаты обучения приведены в табл. 1.

Таблица 1. Метрики качества модели

	Precision	Recall	F1-score
0 – фейк	0,59	0,85	0,69
1 – достоверное видео	0,73	0,40	0,52
Accuracy			0,62
Macro avg	0,66	0,62	0,61
Weighted avg	0,66	0,62	0,61

Эффективная и качественная работа по верификации потенциально недостоверной информации и опровержению фейков зависит от консолидации усилий общества и государства [3], востребованным также видится конструирование ПО, включающего в себя модели обучения НС для идентификации ключевых признаков, свидетельствующих об отсутствии достоверности информации.

В предложенной разработке СППР общая точность модели составила 62% с учетом обработки всех кадров видео. Для более высокого результата следует осуществить решение специфичных задач, связанных со значительно бóльшим временным окном или добавлением дополнительных признаков, таких, например, как звук, что может являться направлениями дальнейших исследований по заданной тематике.

Список литературы

1. Купка И. П. Дипфейк как информационное оружие современности / И. П. Купка, С.С. Щербаков // Динамика медиасистем. – 2023. – Т. 3, № 1. – С. 375–381.

2. Боровская Е.В. Основы искусственного интеллекта: учебное пособие / Боровская Е.В., Давыдова Н.А. – М.: Лаборатория знаний, 2020. – 128 с.

3. Муратова Н. Fake news: дезинформация в медиа: пособие / Н. Муратова, Н. Тошпулатова, Г. Алимова. – Ташкент: «Innovatsion rivojlanish nashriyot-matbaa uyi», 2020. – 104 с.

УДК 004.056

Н.Б. ЦВЕТКОВА

Институт государственной службы и управления РАНХиГС, Москва
Институт социально-политических исследований ФНИСЦ РАН, Москва

ВЗАИМОДЕЙСТВИЕ НАУКИ, ГОСУДАРСТВА И БИЗНЕСА В ПРОЦЕССЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ.

Цифровая трансформация — это процесс внедрения цифровых технологий во все сферы жизнедеятельности общества. Целью цифровой трансформации является содействие достижению большей синергии между структурами власти, бизнеса и гражданского общества, объединение этих структур в единую систему, которая бы усиливала эффект от их взаимодействия.

В контексте перехода к цифровому будущему [1] возникает необходимость поиска новых форм взаимодействия и выбора оптимальных механизмов и технологий цифровой трансформации. [2] Развитие цифровых технологий влияет на социальные отношения и политику государства. Эти изменения представляют собой адаптацию к современной жизни в информационном обществе. При внедрении новых технологий должны соблюдаться нравственные и этические принципы, обеспечиваться безопасность граждан [3]. В рамках национальной цели "Цифровая трансформация [4], поставлена задача достичь "цифровой зрелости" ключевых отраслей экономики и социальной сферы, в том числе здравоохранения, образования, государственного управления, проводятся мероприятия по цифровой трансформации государственных и муниципальных услуг [5].

Цифровая трансформация помогает сместить акценты на ускоренное развитие регионов, при повышении гибкости центров. Повышается прозрачность взаимодействия, ускоряются процессы позитивных изменении в обществе.

В настоящее время перед государством, бизнесом и научным сообществом стоят следующие задачи: 1) выявить передовой опыт обмена данными между властью и бизнесом (B2G), чтобы обеспечить эффективное и качественное предоставление государственных услуг, основанное на достоверных данных; 2) оценивать правовые, экономические и технические проблемы, препятствующие обмену данными между властью и бизнесом, и давать рекомендации по их устранению, чтобы способствовать обмену данными в общественных интересах.

Новая реальность в условиях экономических санкций диктует новые условия. Стали более востребованы удаленные сервисы, внедряются технологии искусственного интеллекта, которые ускоряют получение обратной связи при решении актуальных социальных проблем. «Портал Госуслуг» позволяет правительству решать сложные социальные задачи, осуществлять выплаты нуждающимся гражданам.

Распоряжением Правительства РФ утверждена концепция цифровой и функциональной трансформации социальной сферы на период до 2025 г. [6].

Создана цифровая платформа поддержки инфраструктурных проектов РОСИНФРА [https://rosinfra.ru/], с которой сотрудничают крупные финансовые и бизнес-структуры, включая Сбербанк, ВЭБ РФ.

Цифровизация позволяет удовлетворить потребности молодого поколения, которое успешно использует интернет. Используются инновационные социальные технологии в некоммерческом секторе, создана платформа для онлайн голосования.

Создание новых технологий не должно скомпрометировать надежность уже выстроенной системы управления. Работа с большими данными позволяет распознавать социальные проблемы и привлекать необходимые ресурсы для их решения, повышается контроль за использованием государственных и частных ресурсов. Цифровые платформы и приложения должны представлять ценность для максимального числа граждан. Меры государственного регулирования помогут установить приемлемый баланс между личной конфиденциальностью и общественной безопасностью.

Список литературы

1. Заседание дискуссионного клуба «Валдай», 2021 г. URL: http://www.kremlin.ru/events/president/news/66975.

2. Лапин А.В., Цветкова Н.Б. Экосистемный подход к исследованию деполяризации общества в условиях цифровой трансформации // Социально-политические науки. 2021. Т. 11. № 6. С.23–29. DOI: 10.33693/2223- 0092-2021-11-6-23-29.

3. Орлова И. В. Россия в XXI веке. Политика. Экономика. Культура. // Под ред. Ильичевой Л.Е., Комаровского В.С. М.: Аспект Пресс, 2016, 441 с.

4. О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента РФ № 474 от 21 июля 2020 г.

5. Об оценке эффективности деятельности высших должностных лиц (руководителей высших исполнительных органов государственной власти) субъектов Российской Федерации и деятельности органов исполнительной власти субъектов Российской Федерации: Указ Президента № 68 от 04 февраля 2021 г.

6. Распоряжение Правительства РФ от 20.02.2021 N 431-р (ред. от 08.05.2023) Об утверждении Концепции цифровой и функциональной трансформации социальной сферы, относящейся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, на период до 2025 г.

УДК 004.822

Д.В. ДЕМИДОВ, Л.М. МАРДЕР
Национальный исследовательский ядерный университет «МИФИ», Москва

МЕТОД СОПОСТАВЛЕНИЯ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ С ТРЕБОВАНИЯМИ РЕГУЛЯТОРА

Представлен метод сопоставления технической документации с требованиями нормативной документации по информационной безопасности. Метод предусматривает извлечение терминов в рассматриваемых документах с помощью информационно-поисковых тезаурусов, причём термины связаны между собой онтологическими отношениями.

Постановка задачи

Сертифицируемое программное обеспечение и аттестуемые программные комплексы проверяются на соответствие требованиям различной нормативной документации, вводимой приказами уполномоченных федеральных служб РФ. Процесс установления соответствия разносторонен, трудоёмок, состоит из нескольких этапов, вовлекает сторонние организации (испытательные лаборатории, органы по сертификации и др.), чреват рисками длительного устранения замечаний.

Актуальным является облегчение подготовки к сертификации и её прохождения путём применения организацией-заявителем автоматизированных методов проверки соответствия требованиям регуляторов, в частности метода сопоставления технической документации на сертифицируемый продукт с функциональными требованиями безопасности и требованиями доверия.

Как продуктовая, так и нормативная документация пишется на неформальном языке технической прозы, что исключает применение формальных методов доказательств соответствия при сертификации (за исключением высших уровней доверия, когда установление формального соответствия является явным требованием). Другие сложности сертификации описаны в [1]. Поэтому в основе метода — подходы к обработке естественного языка.

Описание метода

В методе предусмотрены три этапа:

1. Выделение терминов и онтологических отношений в текстах обоих сопоставляемых документов.

2. Построение информационно-поискового тезауруса [2, 3] для предметной области с одной стороны и для свода требований с другой стороны. В качестве базового представления требований регулятора рассматривается набор нормативных документов, по которым строится тезаурус, отражающий структуру нормативной базы и типологию требований. Каждое из требований далее интерпретируется как поисковый запрос. На практике интерес представляет и такое представление требований как опросник. Пункты опросников также можно интерпретировать как поисковые запросы.

3. Классификация фрагментов текста, описывающего реализацию требований, и их сопоставление с требованиями.

Первые два этапа направлены на создание возможности сопоставления фрагментов текста с учётом отношений между терминами, таких как выше-ниже, синонимия, аббревиатура–полный термин, ассоциация (в статистическом смысле) и потенциально ряд других.

На третьем этапе с целью фильтрации фрагменты текста классифицируются по двум классам: «является описанием реализации требований»/«не является». Непосредственно сопоставление конкретных текстовых фрагментов выполняется статистическими методами, в дальнейшем могут привлекаться методы структурного анализа синтаксических структур и семантических отношений. Результатом сопоставления является ранжированный перечень фрагментов технической документации, соответствующих тому или иному фрагменту требований.

Полученные результаты

Для предложенного метода разработаны программные средства построения тезауруса технического документа. Тезаурусы представляются в формате OWL[1].

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, pp. 31–36.

2. Добров Б.В. Иванов В.В. Лукашевич Н.В. Онтологии и тезаурусы: модели, инструменты, приложения. – ИНТУИТ, 2008. – 172 с.

3. Лукашевич Н.В. Тезаурусы в задачах информационного поиска. – Издательство Московского университета, 2011. – 396 с.

[1] https://www.w3.org/OWL/

УДК 004.852

Д.А. КРИВОВ, В.В. БОНДАРЕНКО
Самарский национальный исследовательский университет им. академика С.П. Королева

ОБ ОДНОМ СПОСОБЕ ОПРЕДЕЛЕНИЯ ПОЛА АВТОРА ПО КОРОТКОМУ ЭЛЕКТРОННОМУ СООБЩЕНИЮ

В данной работе авторами рассмотрена проблема определения пола автора электронного сообщения. Для решения данной проблемы разработана программа, которая на основе статистических методов может определять гендерную принадлежность автора текста. Для обучения программы и для обработки значительного объема данных разработан метод сбора и анализа большого количества электронных сообщений. На его основе проведен ряд тестов с целью нахождения наиболее результативного подхода к обучению программ определению требуемых сведений об авторе сообщения.

Введение

В современном мире одной из наиболее серьезных проблем является мошенничество в сети интернет [1]. Благодаря особенностям данной сети можно без особых трудностей скрыть всю информацию о своей личности. Именно этим пользуются злоумышленники и часто выдают себя за совершенно другого человека. Так, например, для получения доверия со стороны потенциальной жертвы преступник может притвориться красивой девушкой с целью дальнейшего получения денежных средств.

Однако у каждого пола человека существуют свои речевые особенности [2]. Например, женщины употребляют для общения некоторые слова намного чаще мужчин. Поэтому, если проанализировать большое количество сообщений от представителей разных полов, можно с достаточно высокой вероятностью определить гендерную принадлежность автора электронного сообщения. Это может быть полезно для определения потенциального злоумышленника.

Разработка программы для определения пола автора электронного сообщения

Для русского языка данная проблема до сих пор остается достаточно актуальной, именно поэтому было решено создать программу для определения личности предполагаемого злоумышленника. Разработанное приложение использует методологию машинного обучения, рабочим механизмом классификации выступает метод опорных векторов (SVM). Идея работы приложения, следующая: на вход подается какое-либо сообщение, далее идет обработка исходного текста сообщения и уже после этого используется

расстановка весов для каждого слова при помощи метода опорных векторов. Дальнейшее функционирование программы зависит от выбранного в начале режима работы приложения:

– если была поставлена задача обучения, то все представленные слова записываются в текстовый документ, после чего им расставляются веса в зависимости от выбранного пункта меню (мужчина/женщина). Также стоит упомянуть, что в случае, если данное слово уже присутствовало в файле с данными, то оно не будет снова записано, а лишь увеличится его вес;

– если же выбран режим тестирования программы, то в данной ситуации приложение начинает искать каждое из слов в файле с данными и суммировать все значения их весов. Затем полученные результаты сравниваются, и программа выдает заключение о том, кто написал поданное на вход сообщение, также при этом высчитывается вероятность правильного ответа. Она может принимать значения в промежутке от 50 до 100 процентов.

Программа реализована в виде чат-бота Телеграмм.

Результаты обучения программы

Основной проблемой при построении программы было отсутствие обучающих выборок на русском языке достаточного объема. Для формирования обучающей выборки были использованы видеоролики с «повседневными» диалогами. При этом вся речь сначала преобразовывалась в текст, а потом производились манипуляции, описанные ранее. Суммарно было обработано 100 видеофрагментов, а количество уникальных слов в памяти программы после обработки составило 7254 единицы. При этом после обучения программы и проведения тестирования, было получено, что точность работы программы составляет 81 процент.

Точность верных ответов в 81 процент является удовлетворительным результатом, однако ее и дальше можно увеличивать за счет использования предварительной фильтрации текста, а также изменяя значение весов наиболее часто употребляемых слов и у мужчин, и у женщин.

Список литературы

1. Самая серьезная проблема – обман в интернет-магазинах // Известия URL: https://iz.ru/842939/evgeniia-priemskaia/samaia-sereznaia-problema-obman-v-internet-magazinakh (дата обращения: 03.02.2023).

2. Doyle J., Keselj V. Automatic Categorization of Author Gender via N-Gram AnalySis. Proceedings of the 6th Symposium on Natural Language Processing, SNLP'2005, 2005. available at: http://web.cs.dal.ca/~vlado/papers/SNLP05J.pdf.

УДК 004.056

К.Д. СЧАСТЛИВЦЕВ, И.Ю. КОРКИН
Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS 11 ОТ ВНЕДРЕНИЯ КОДА В ПРОЦЕССЫ

Цель исследования: исследование возможности внедрения вредоносного кода в легитимные процессы операционной системы Windows 11. Результат исследования: операционная система Windows 11 уязвима к большому количеству популярных методов внедрения кода в процессы. Научная новизна: заключается в проведенном исследовании, анализ полученных результатов позволит разработать простое и удобное средство для защиты от внедрения кода в процессы.

Внедрение процессов в Windows, по-видимому, является хорошо изученной темой, поскольку в настоящее время известно и реализовано множество методов для внедрения из одного процесса в другой [1]. Вероятно, операционная система Windows 11 должна быть хорошо защищена от данных методов или, хотя бы, от самых популярных из них [2]. Данное исследование направлено на демонстрацию того, что все на самом деле не так.

Как правило, процесс внедрения делится на 3 этапа:

- Выделение памяти;
- Запись в память (с использованием примитива записи в память);
- Исполнение.

Рассмотрены реализации нескольких популярных техник внедрения кода, таких как внедрение загружаемой библиотеки при помощи функции CreateRemoteThread, загрузка потока в контексте пользователя, метод внедрения «Перезапись процесса», метод внедрения «Процесс двойник» [3], метод внедрения «Отраженная загрузка кода» [4, 5].

В методе загрузки потока в контексте пользователя используется функция RtlCreateUserThread, которая позволяет создать поток в контексте пользователя и выполнить любой код от его имени.

«Перезапись процесса» (Process Hollowing) – метод внедрения, в котором создается процесс в состоянии ожидания, из которого впоследствии удаляется весь код и заменяется на внедряемый.

«Процесс двойник» (Process Doppelganging). Суть метода заключается в создании «двойника» процесса, которому затем присваиваются характеристики и содержимое другого процесса.

«Отраженная загрузка кода» (Reflective Code Injection) – это метод внедрения кода с использованием техники отражения. Техника отражения – это способ вызова функций и методов в объектно-ориентированных языках программирования, при котором вызов происходит через специальный объект, который может отражать информацию о вызываемом методе или функции.

В качестве полезной нагрузки использовался код, который позволял получить информацию о глобальных переменных легитимного процесса, изменить значения данных переменных, получить некоторую информацию о системе пользователя, а также записывающий всю полученную информацию в отдельный файл.

В результате исследования четыре метода из пяти были успешно выполнены, со стороны операционной системы и встроенного антивируса Microsoft Defender не последовало никаких действий, что свидетельствует о том, что методы внедрения кода, такие как загрузка потока в контексте пользователя, метод внедрения «Перезапись процесса», метод внедрения «Процесс двойник», метод внедрения «Отраженная загрузка кода», исправно работают в операционной системе Windows 11. Из полученных результатов следует, что необходимо разработать ПО, способное обнаруживать и предотвращать внедрение кода в процессы пользователя в операционной системе Windows 11.

Список литературы

1. Ten process injection techniques: A technical survey of common and trending process injection techniques [Электронный ресурс] // Elactic: сайт. – URL: https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process (дата обращения: 20.08.2023).

2. D. Pogonin, I. Korkin. Microsoft Defender Will Be Defended: MemoryRanger Prevents Blinding Windows AV // Proceedings of the 15th Annual ADFSL 2022 Conference on Digital Forensics, Security and Law, Florida, USA. – 2022

3. SynAck targeted ransomware uses the Doppelgänging technique // SecureList: сайт. – URL: https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/ (дата обращения: 21.05.2023).

4. Process Injection Techniques used by Malware [Электронный ресурс] // Medium: сайт. – URL: https://medium.com/csg-govtech/process-injection-techniques-used-by-malware-1a34c078612c (дата обращения: 11.05.2023).

5. Process Injection Techniques [Электронный ресурс] // GitHub: сайт. – URL: https://github.com/MahmoudZohdy/Process-Injection-Techniques (дата обращения: 10.05.2023).

Направление

Защищенные компьютерные системы и технологии

Руководитель секции – Иванов М.А., д.т.н.,
заведующий кафедрой №12

УДК 004.056

С.А. ПЕТРЕНКО[1], А.С. ПЕТРЕНКО[2]

[1]*Университет Иннополис, Иннополис*

[2]*Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИИ РФ В УСЛОВИЯХ АТАК С ПРИМЕНЕНИЕМ КВАНТОВОГО КОМПЬЮТЕРА

Показано, что объекты КИИ РФ уже не обладают требуемой устойчивостью для целевого функционирования в условиях ранее неизвестных квантовых атак злоумышленников. Предложена новая технология (модели, методы и средства) обеспечения квантовой устойчивости объектов КИИ РФ, которая в отличие от известных технологий информационной безопасности позволяет упреждать приведение упомянутых объектов к существенным или катастрофическим последствиям в условиях роста квантовой угрозы безопасности.

Введение

Актуальность темы заключается в необходимости обеспечения требуемой устойчивости объектов КИИ РФ в условиях роста квантовой угрозы безопасности, и недостаточности известных технологий обеспечения безопасности, надежности и отказоустойчивости для противодействия ранее неизвестным атакам злоумышленников с применением квантового компьютера [1]. Достижения американской компании IBM, а также ряда других производителей квантовых компьютеров, убедительно свидетельствуют о реалистичности, так называемой, «квантовой угрозы» [2,3]. По этой причине в ряде стран мира уже начали подготовку к противодействию будущим квантовым кибератакам.

Постановка задачи

Целью исследований является разработка технологии обеспечения требуемой устойчивости объектов КИИ РФ в условиях ранее неизвестных атак злоумышленников с применением квантового компьютера.

Для достижения поставленной цели исследований потребовалось решить следующие основные задачи:

1) Разработать методы анализа квантовой устойчивости объектов КИИ РФ на основе модифицированных квантовых алгоритмов Шора и Гровера,

позволяющих получить реальные оценки теоретической и практической стойкости криптопримитивов.

2) Предложить методы синтеза постквантовых криптопримитивов для объектов КИИ РФ на основе разделов математики, потенциально содержащих сложные вычислительные задачи, для которых не известны эффективные алгоритмы решения. В том числе, на основе теории решеток, многочленов от многих переменных, теории кодирования, изогений на эллиптических кривых, алгебры октонионов, многочленов Чебышева, теории Кос и др.

3) Выработать методы решения задач выбора оптимальных технологий и программ обеспечения квантовой устойчивости объектов КИИ РФ в детерминированных условиях. Определить содержание и особенности реализации основных этапов решения задач синтеза технологий и комплексного планирования обеспечения квантовой устойчивости объектов КИИ РФ в условиях классических и квантовых атак злоумышленников.

4) Разработать архитектуру, инструментальные средства и программное обеспечение синтеза технологий и комплексных планов обеспечения квантовой устойчивости блокчейн объектов КИИ РФ в условиях классических и квантовых атак злоумышленников.

Заключение

В результате была создана новая технология (модели, методы и средства) обеспечения квантовой устойчивости объектов КИИ РФ, которая в отличие от известных технологий информационной безопасности позволяет упреждать приведение упомянутых объектов к существенным или катастрофическим последствиям в условиях роста квантовой угрозы безопасности.

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. Alexei Petrenko, Applied Quantum Cryptanalysis (научная монография «Прикладной квантовый криптоанализ»), ISBN: 9788770227933, e-ISBN: 9788770227926, River Publishers, 2023. – 256 p. (SCOPUS), https://doi.org/10.1201/9781003392873, https://www.riverpublishers.com/book_details.php?book_id=1028.

3. Петренко А.С., Романченко А.М. Перспективный метод криптоанализа на основе алгоритма Шора. Защита информации. Инсайд. 2020. № 2 (92). С. 17–23., https://www.elibrary.ru/item.asp?id=42615393.

УДК 004.056

В.Г. ГРИБУНИН[1], Р.В. ДЗВИНКО[2], В.Д. ПАСТУХОВ[1]

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

[2]*НПЦ «Бизнесавтоматика», Москва*

СОВРЕМЕННЫЕ ПОДХОДЫ К СТЕГАНОГРАФИЧЕСКОМУ АНАЛИЗУ

Использование нарушителем методов стеганографии является одной из угроз информационной безопасности. Для противодействия этой угрозе используются средства стегоанализа, ориентированные на выявление факта наличия скрытой информации. В докладе рассмотрено использование в этих средствах методов машинного обучения (МО) и методов обучения глубоких нейронных сетей (ГНН), показаны их достоинства и недостатки, сделаны выводы и представлены предложения по перспективным исследованиям в данной области.

Введение

Одной из угроз информационной безопасности является скрытие (хранимой, передаваемой) информации нарушителем от законного контроллера. Использовать для этой цели методы стеганографии может даже неквалифицированный нарушитель, с учетом широкого распространения в Интернете соответствующих бесплатных средств. При этом скрываемая информация помещается незаметным (для любых средств анализа) образом в другие файлы, существенно большего объема, называемые контейнерами. В качестве них обычно выступают файлы, имеющие избыточность (видео, аудио, изображения). Особенно большое количество информации может быть скрыто в файлах изображений. Например, в сделанной смартфоном фотографии можно достаточно безопасно разместить 80 кбайт информации.

Поэтому развиваются методы стегоанализа, и в особенности, стегоанализа изображений формата JPEG. Целью этих средств является выявление с некоторой вероятностью факта наличия скрытой информации в контейнерах при допустимой вероятности ложной тревоги (хотя возможно и использование других метрик качества). За 25 лет исследований был достигнут существенный прогресс в данной области, и в настоящее время наличие стеганографии успешно определяется при внедрении до 0.1 бит/пиксел изображения.

Можно выделить два основных направления исследований в стегоанализе: использование МО и использование ГНН. Эти два

направления рассмотрены в следующих разделах. В конце рассмотрен новый подход к стегоанализу, хотя и не основанный на ГНН, но родившийся в ходе изучения особенностей работы сверточных нейронных сетей (СНС).

Стегоанализ на основе «классического» машинного обучения

Стегоанализ на основе МО состоит из трех этапов:

1) Снижение влияния изображения-контейнера на результаты стегоанализа. Так как изображение в среднем является низкочастотным, то на этом этапе часто применяют высокочастотную фильтрацию.

2) Формирование векторов признаков от получившегося шумового остатка. Здесь наибольшее значение имеет так называемая «пространственно-богатая модель» (SRM) [1], заключающаяся в вычислении линейных и нелинейных зависимостей между пикселями и статистик высокого порядка (всего формируется вектор из 34671 признака).

3) Классификация. На данном этапе обычно используется классификатор на основе машин опорных векторов (SVM).

Стегоанализ на основе глубокого обучения

Успехи ГНН в классификации изображений обусловили внимание к ним для решения задач стегоанализа. Было предложено множество архитектур, в большинстве из них используются СНС, среди которых наилучшими считаются SRNet, Yedroudj-Net, Zhu-Net [2]. При использовании глубокого обучения, рассмотренные выше, этапы 2 и 3 объединены. Качество стегоанализа выше, чем у средств, построенных на основе МО.

Вместе с тем, обучение классификаторов требует большого числа изображений и серьезных вычислительных ресурсов. Также много ресурсов требуется и во время работы стегоанализатора. Поэтому в докладе рассмотрен подход к стегоанализу, использующий идеи метода PixelHop [3]. Полученные результаты не уступают лучшим из опубликованных результатов для стегоанализаторов на основе ГНН, тогда как обучение и функционирование стегоанализатора требует существенно меньших ресурсов.

Список литературы

1. Fridrich J., Kodovský J. Rich Models for Steganalysis of Digital Images // IEEE Transactions on Information Forensics and Security. – Vol. 7. – №3. - June 2012. – pp. 868–882.

2. Kheddara H., Hemis M., Himeurc Y., Megías D., Amira A., Deep Learning for Diverse Data Types Steganalysis: A Review / Preprint submitted to Elsevier. – Aug, 2023. https://arxiv.org/pdf/2308.04522.pdf.

3. Yang Y., Magoulianitis V., Kuo C.-C. Jay. E-PixelHop: An Enhanced PixelHop Method for Object Classification // APSIPA ASC. – 2021. – pp. 1475–1482.

УДК 004.056

О.И. АТАКИЩЕВ[1], В.Г. ГРИБУНИН[1], И.Л. БОРИСЕНКОВ[2], М.В. ЛЫСАЧЕВ[3], В.Е. АНАНЬЕВ[1]

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

[2]*Секция прикладных проблем при Президиуме РАН, Москва*

[3]*АО «Консист- ОС», Москва*

ОСОБЕННОСТИ ПРИМЕНЕНИЯ МЕТАГРАММАТИЧЕСКОГО ПОДХОДА ПРИ СОЗДАНИИ ПЕРСПЕКТИВНЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассмотрены особенности применения метаграмматического подхода при решении задач создания перспективных сложноструктурированных систем информационной безопасности различного назначения. Особое внимание уделено решению задач структурно- параметрического синтеза сложноструктурированных систем информационной безопасности и программ их создания в условиях динамичного изменения условий эксплуатации и нечеткого задания исходных данных на основе комбинированных сигнатурно- метаграмматических методов и методов метаграмматического анализа иерархий.

Современный этап развития организационно-технических систем информационной безопасности (ИБ) различного назначения характеризуется ростом множества нарушителей и угроз безопасности, существенным повышением уровня требований к подобным системам, их сложности, необходимостью их оперативного создания и модификации в условиях динамично изменяющейся обстановки и нечеткого задания исходных данных.

Выполнение требований к системам ИБ (СИБ) и средствам ИБ (СрИБ) в этих усложняющихся, зачастую нечетко заданных условиях, может быть достигнуто путем оптимального планирования создания СИБ с поэтапной адаптацией их сложной и ресурсоемкой структуры, состава используемых СрИБ под динамично изменяемые условия эксплуатации, нарастающее множество угроз, а также с учетом необходимости адекватного ситуации внедрения в СИБ новых технологий (методов, механизмов и средств) ИБ.

В условиях динамично изменяющейся обстановки при наличии жестких ресурсных ограничений по развитию систем рассматриваемого

класса, актуализируется проблема научно обоснованного выбора решений по созданию новых и совершенствованию существующих СИБ.

Эта проблема характеризуются все большей сложностью, что приводит к существенному увеличению науко- и ресурсоемкости ее решения, определяет необходимость дальнейшего развития научно-методического аппарата создания сложноструктурированных СИБ.

В докладе рассмотрены существующие подходы к решению подобных проблем их достоинства и недостатки.

Рассмотрены особенности предложенного и развиваемого метаграмматического подхода (МГП) к решению данной проблемы.

В основе МГП лежит формализация системы правил структурно-параметрического синтеза СИБ в виде метаграмматик (МГ): $G_{мг}=<\{G_i\}, W_{мг}>$, содержащих множества грамматик различного вида$\{G_i\}$ и схему их согласования $W_{мг}$. Структуризация продукционных правил формирования вариантов СИБ в виде МГ позволяет снизить сложность продукционных моделей, применить эффективные методы генерации и выбора вариантов создания СИБ на основе метаграмматического разбора.

В зависимости от условий решаемых конкретных задач предложено использовать различные классы МГ. В докладе детально рассмотрены особенности предложенных модификаций МГП-комбинированных подходов на основе Ки-МГ (сигнатурно-метаграмматический подход) и нечетких МГ (метаграмматический анализ иерархий) [1–2]. В первом случае в МГ используются Ки-грамматики и правила согласования, во втором – нечеткие грамматики с ориентированными на них методами грамматического совместного метаграмматически-графового разбора и методов разбора метаграмматик, совмещенных с методом анализа иерархий Саати.

Показаны преимущества данных модификаций при решении ряда конкретных задач создания сложноструктурированных СИБ критической инфраструктуры.

Список литературы

1. Атакищев О.И., Борисенков И.Л., Грибунин В.Г., Смирнов Д.В. Коллегиальные метаграмматики для моделирования динамично изменяемых программ создания систем информационной безопасности. Вестник компьютерных и информационных технологий, 2020, № 4(190), с. 29–43.

2. Атакищев О.И., Грибунин В.Г., Лысачев М.Н., Смирнов Д.В. Метаграмматический подход анализа иерархий и особенности его применения при создании систем обеспечения информационной безопасности атомных станций малой мощности. Известия Института инженерной физики. 2023, № 1(67), с. 82–88.

УДК 004.056

И.Ю. ЖУКОВ[1, 3], С.К. МУРАВЬЕВ[2],
Т.И. КОМАРОВ[1, 3], Н.А. ЧЕПИК[3,4]

[1]*«АО «РАМЭК-ВС», Санкт-Петербург*

[2]*ООО «НПП «Криптософт», Пенза*

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

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

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВСТРОЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Комплексный анализ реализации импортозамещения в сфере вычислительного оборудования показывает острую необходимость разработки доверенного встроенного программного обеспечения. По результатам исследований предложен подход по созданию отечественной защищенной иерархии доверия, формируемой прошивкой материнской платы в момент старта компьютера («корня доверия») до предоставления защищенных облачных сервисов (формирование «цепочки доверия»).

Встроенное ПО представляет собой прошивки, которые программным образом реализуют часть функций аппаратного обеспечения. Одним из наиболее важных и влияющих на безопасность компонентов вычислительной системы являются прошивки материнских плат, которые чаще всего функционируют согласно спецификации UEFI (Unified Extensible Firmware Interface) [1].

UEFI-совместимая прошивка материнской платы является первым программным компонентом, который стартует при включении компьютера и обеспечивает инициализацию аппаратного обеспечения, а затем, в зависимости от сценария использования, загружает последующие программные компоненты.

Именно на начальном этапе загрузки прошивки должны быть предприняты меры по обеспечению безопасности – необходимо проинициализировать программный или аппаратный корень доверия, после чего последовательно осуществлять проверку всех загружаемых в дальнейшем компонентов. Если прошивкой с самого начала работы компьютера не обеспечивается должный уровень безопасности, то это открывает дорогу для различных вредоносов, в т.ч. bootkit-ов, которые

могут направить всю дальнейшую работу системы по сценарию, который нужен злоумышленнику [2].

В настоящее время. практически вся национальная критическая информационная инфраструктура функционирует на импортных решениях, несмотря на действующие программы импортозамещения. В большинстве случаев осуществляется контрактная сборка рабочих станций и серверов на территории Российской Федерации, без значимых изменений аппаратного и встроенного программного обеспечения.

При этом, используемые импортные средства вычислительной техники и их прошивки имеют собственные механизмы обеспечения безопасной загрузки (например: TPM [3]), которые построены с использованием зарубежных стандартов и криптоалгоритмов, что исключает их широкое применение на территории Российской Федерации.

Для решения обозначенной проблемы предлагается разработать дополнительные требования к процессу безопасной загрузки. В соответствии с данными требованиями, предлагается разработать открытые спецификации, которые разовьют идеи, заложенные в аппаратно-программные средства доверенной загрузки (АПМДЗ), а также адаптируют и улучшат идеи, применяемые в зарубежных технологиях. В соответствии с разработанными спецификациями предлагается реализовать отечественные программно-аппаратные решения, которые будут представлять собой, с точки зрения функциональности, гибрид классических АПМДЗ и модулей TPM, что позволит реализовать отечественную иерархию доверия для всей ИТ-инфраструктуры.

Реализация указанных предложений позволит существенным образом повысить уровень безопасности большого количества вычислительных систем (в т.ч. отечественных ГИС, ведомственных систем) и, как минимум, в области встроенного ПО перехватить инициативу и развивать собственные решения, а не следовать в фарватере зарубежных производителей.

Список литературы

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

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

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

УДК 004.056

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

СТОХАСТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Отмечается важная роль стохастических методов при решении задач защиты информации, главный результат применения которых – это внесение непредсказуемости в работу защищаемого цифрового объекта и средств обеспечения его безопасности. Базовым элементом в этой ситуации становится непредсказуемый генератор псевдослучайных чисел.

Любая атака на компьютерные системы начинается с исследования атакуемого объекта либо на модели, либо на реальной системе. У нападающей стороны всегда есть резерв времени для поиска уязвимостей в целевой вычислительной системе, при этом ему достаточно обнаружить только одно слабое место в ее защите, чтобы провести успешную атаку. Задача защищающейся стороны значительно сложнее, ей надо выявить и ликвидировать все слабые места в системе, при этом анализ ее защищенности необходимо проводить постоянно и на всех уровнях: элементная база, архитектура, системное ПО, сетевое ПО, прикладное ПО; учитывая, что задачи защиты информации надо решать в динамике, а не в статике.

Кроме того, защита практически никогда не знает, кто ее будет атаковать и когда, что является целью атакующего и какие у него возможности. При этом задачи защиты информации очень часто решаются по остаточному принципу, когда продукт, система или технологии уже созданы, при этом используются реактивные методы защиты, которые развиваются лишь по мере появления новых угроз информационной безопасности и новых механизмов проведения атак на компьютерные системы.

В этой ситуации положение защиты выглядит безнадежным и на вопрос, каким образом она может получить преимущество перед нападением, казалось бы, единственным правильным ответом будет – никогда. Однако выход есть и этот выход – использование стохастических методов защиты информации, которыми принято называть методы, основанные на использовании генераторов псевдослучайных чисел и хеш-генераторов [1–3]. Примеров эффективного применения стохастических

методов защиты накопилось множество [1, 4–6], при этом надо отметить их универсальность, так как они могут использоваться совместно с любым другим методом защиты, автоматически повышая его качество.

Стохастические методы защиты информации являются методами двойного назначения. Первыми, еще в прошлом веке их стали применять создатели компьютерных вирусов (КВ) (пермутирующие, полиморфные, метаморфные КВ), затем уже в 21 веке разработчики других типов вредоносных программ (AdmMutate, Ransomware и пр.).

Наиболее перспективными направлениями использования генераторов псевдослучайных чисел, которые начали развиваться в последние годы, являются Logic Encryption, Design Obfuscation (механизм скрытых функций, многовариантная логика и др.), Moving Target Defense, Control Flow Integrity. При этом последние две технологии являются попытками защититься от атак, основанных на эксплуатации уязвимостей ПО, т.е. речь по сути дела идет о создании стохастического процессора.

Таким образом, актуальной научной задачей является разработка непредсказуемых и статистически безопасных генераторов псевдослучайных чисел (в некоторых случаях с нестандартными графами переходов), ориентированных на использование в задачах защиты информации, и их интеграция в структуру вычислительных систем и их элементов.

Список литературы

1. Осмоловский С.А. Стохастические методы передачи данных. – М.: Радио и связь, 1991. – 240 с.
2. Осмоловский Стохастические методы защиты информации. – М.: Радио и связь, 2003. – 319 с.
3. Осмоловский С.А. Стохастическая информатика: инновации в информационных системах. − М.: Горячая линия–Телеком, 2012. – 320 с.
4. Wenbo Mao. Modern Cryptography: Theory and Practice. Prentice Hall, 2003.
5. М.А. Иванов. Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи. // Вопросы кибербезопасности. – 2019. – № 3(31). – С. 45−50. DOI: 10.21681/2311-3456-2019-3-45-50.
6. Иванов М.А. Основы криптографии. В 2 частях. – М.: ГУУ, 2023.

УДК 004.056

Г.А. ВРАЖНОВ[2], М.А. ИВАНОВ[1, 2], М.А. ХОРОШАЕВ[2]

[1]*Государственный университет управления», Москва*

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

ГЕНЕРАТОРЫ ($M – 2^n + 1$)-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Предлагается генератор псевдослучайных чисел, диаграмма переключений которого состоит из двух циклов длиной ($2^{2n} – 2^n$) и 2^n. Отличительной особенностью генератора является возможность организации самоконтроля правильности функционирования за счет предсказания значения свертки содержимого элементов памяти. Генератор ориентирован на реализацию механизма скрытых функций вычислительных систем и их элементов.

Самым распространенным классом ГПСЧ являются генераторы, функционирующие в конечных полях $GF(2^n)$. Область использования ГПСЧ этого типа чрезвычайно широка, это помехоустойчивое кодирование, встроенное тестирование цифровых устройств на БИС, скремблирование информации, защита информации. Если характеристический многочлен степени N является примитивным над $GF(2^n)$, генератор формирует M-последовательность, где $M = 2^{nN} – 1$. Диаграмма переключений генератора M-последовательности состоит из двух циклов, т.е. имеет вид $(2^{nN} – 1)$-1.

Если в качестве характеристического многочлена выбран многочлен вида $\varphi(x) = (x + 1)\lambda(x) = x^2 + a_1x + a_0$, где $\lambda(x)$ – многочлен первой степени, примитивный над $GF(2^n)$, диаграмма переключений устройства состоит из 2^n циклов длиной $2^n – 1$ и 2^n циклов длиной 1, т.е. имеет вид $(2^n – 1)(2^n)$-$1(2^n)$. Таким образом, несмотря на наличие 2^n элементов памяти максимальная длина формируемой последовательности равна $2^n – 1$, что сильно меньше потенциально возможной 2^{2n}.

Предлагается решение, позволяющее увеличить длину формируемой последовательности до величины $2^n (2^n – 1) = (2^{2n} – 2^n)$, т.е. в 2^n раз большей, чем в известном устройстве. Диаграмма переключений генератора включает в себя всего лишь два цикла длиной $(2^{2n} – 2^n)$ и 2^n, т.е. имеет вид $(2^{2n} – 2^n)$-2^n. Математическая модель устройства имеет вид:

$$Q_1(t + 1) = a_0Q_2(t),$$
$$Q_2(t + 1) = ((Q_1(t) + (a_0 + a_1)Q_2(t)) \boxplus c_1) + a_0Q_2(t),$$

где + сложение в GF(2^n), ⊞ – сложение по модулю 2^n, $Q_i(t)$ и $Q_i(t + 1)$ – содержимое i-го регистра ГПСЧ соответственно в моменты времени t и $(t + 1)$, $i = 1, 2$.

На рис. 1 показана схема генератора для случая $\varphi(x) = x^2 + a_1x + a_0$. Устройство состоит из двух n-разрядных регистров, двух блоков сложения в GF(2^n), двух блоков умножения в GF(2^n), блок сложения по модулю 2^n, генератор имеет группу c_1 управляющих входов (количество которых равно n). На рис. 1 показаны также вид диаграммы переключений устройства при $n = 2$, 3 и 4. Количество возможных значений на управляющих входах, при которых генератор приобретает требуемые свойства, равно количеству чисел, меньших и взаимно простых с числом 2^n.

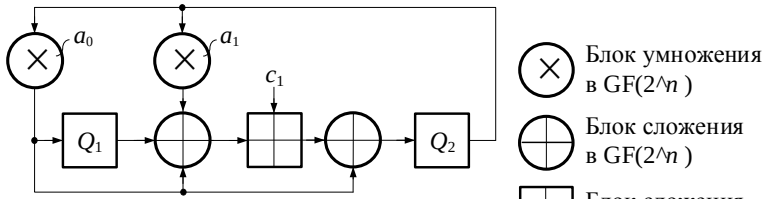

Диаграмма переключений генератора

$n = 2 \rightarrow$ 12-4

$n = 3 \rightarrow$ 56-8

$n = 4 \rightarrow$ 240-16

•••

Рис. 1. Схема генератора ($M – 2^n + 1$)-последовательности.

Отличительной чертой генератора ($M – 2^n + 1$)-последовательности является то, что свертка в GF(2^n) содержимого регистров устройства в процессе его работы меняет свое значение предсказуемым образом. Иначе говоря, за счет выбора характеристического многочлена особого вида и предсказания значения свертки содержимого элементов памяти можно организовать самоконтроль правильности функционирования ГПСЧ. При этом в отличие от других генераторов, обладающих подобным свойством, в данном случае процедура определения вида управляющих сигналов, обеспечивающих диаграмму переключений вида $(2^{2n} – 2^n)$-2^n тривиальна.

Генераторы ориентированы на реализацию механизма скрытых функций после интеграции ГПСЧ в структуру защищаемого цифрового устройства.

УДК 004.056

М.А. КОНДАХЧАН[2], М.А. ИВАНОВ[1, 2], А.В. СТАРИКОВСКИЙ[1]

[1]*Государственный университет управления», Москва*

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

НЕЛИНЕЙНОЕ ТРЕХМЕРНОЕ МНОГОРАУНДОВОЕ ПРЕОБРАЗОВАНИЕ ДАННЫХ 3DGOST

Рассматривается 3D стохастическое преобразование, предназначенное для реализации стохастических алгоритмов обработки данных. Особенностью преобразования является высокая степень параллелизма на уровне элементарных операций.

Главный результат применения генераторов псевдослучайных чисел (ГПСЧ) в задачах защиты информации (ЗИ) – внесение непредсказуемости в работу защищаемой вычислительной системы и ее элементов. Методы ЗИ, основанные на использовании непредсказуемых и статистически безопасных ГПСЧ, принято называть стохастическими [1, 2].

Предлагается 3D многораундовое стохастическое преобразование, ориентированное на реализацию стохастических алгоритмов обработки данных. Особенности преобразования:

– представление входного, выходного блоков данных, всех промежуточных результатов в виде трехмерного массива 8 × 8 × 8 бит; формирование по входному блоку данных M разрядностью 512 бит блока данных S той же разрядности в соответствии с выражением $S := M$, после этого выполнение трех раундов преобразования блока данных S соответственно параллельно плоскостям $y0z$, $x0z$, $x0z$; введение понятия слоя данных (Layer, L_{ji}), представляемого в виде двухмерного массива 8 × 8 бит, при этом $S = L_{x0} \| L_{x1} \| \dots \| L_{x7} = L_{y0} \| L_{y1} \| \dots \| L_{y7} = L_{z0} \| L_{z1} \| \dots \| L_{z7}$; где $\|$ – операция конкатенации; L_{xi} – слои данных, параллельные плоскости $y0z$; L_{yi} – слои данных, параллельные плоскости $x0z$; L_{zi} – слои данных, параллельные плоскости $x0y$; $i = 0, 1, ..., 7$; стохастическое преобразование (Mix) каждого слоя данных L_{xi}, объединение преобразованных слоев в преобразованный блок S в первом раунде; стохастическое преобразование (Mix) каждого слоя данных L_{yi}, объединение преобразованных слоев в преобразованный блок S во втором раунде; стохастическое преобразование (Mix) каждого слоя данных L_{zi}, объединение

преобразованных слоев в преобразованный блок S в третьем раунде; операции преобразования (перемешивания) слоя данных L_{ji} (Mix) реализованы в виде шести итераций сети Фейстеля, обеспечивающих полное рассеивание и перемешивание информации;

– 512-разрядный ключ K представляется в виде трехмерного массива 8 × 8 × 8 бит; вводится понятие слоя ключа (KeyLayer, KL_{ji}), представляемого в виде двухмерного массива 8 × 8 бит, при этом $K = KL_{x0} \parallel KL_{x1} \parallel \ldots \parallel KL_{x7} = KL_{y0} \parallel KL_{y1} \parallel \ldots \parallel KL_{y7} = KL_{z0} \parallel KL_{z1} \parallel \ldots \parallel KL_{z7}$, $j \in \{x, y, z\}$; слои KL_{x0}, KL_{x1}, …, KL_{x7} используются в первом раунде преобразования состояния (блока данных) S в качестве раундовых ключей при преобразовании слоев данных соответственно L_{x0}, L_{x1}, …, L_{x7}; слои KL_{y0}, KL_{y1}, …, KL_{y7} используются во втором раунде преобразования состояния (блока данных) S в качестве раундовых ключей при преобразовании слоев данных соответственно L_{y0}, L_{y1}, …, L_{y7}; слои KL_{z0}, KL_{z1}, …, KL_{z7} используются в третьем раунде преобразования состояния (блока данных) S в качестве раундовых ключей при преобразовании слоев данных соответственно L_{z0}, L_{z1}, …, L_{z7}; каждый 64-разрядный слой ключа KL_{ji} делится на два 32-разрядных подключа k_1 и k_2, которые используются при выполнении итераций преобразования Mix слоя данных L_{ji} в следующей последовательности k_1, k_2, k_2, k_1, k_1, k_2 (шаг вперед, шаг назад и шаг вперед).

Каждая из 6 итераций преобразования Mix может являться, например, раундом ГОСТ 28147-89 [3].

Предлагаемое стохастическое преобразование ориентировано на реализацию функции выхода при построении ГПСЧ на основе использования двухступенчатой структуры Counter Mode.

Статистическое тестирование по методике НИСТ подтвердило статистическую безопасность преобразования.

Список литературы

1. Осмоловский Стохастические методы защиты информации. – М.: Радио и связь, 2003. – 319 с.

2. Осмоловский С.А. Стохастическая информатика: инновации в информационных системах. − М.: Горячая линия–Телеком, 2012. – 320 с.

3. Винокуров А. ГОСТ не прост..., а очень прост! // Монитор. – 1995. – №1. – С. 60-73.

УДК 004.056

С.В. ДВОРЯНКИН[1], Р.А. УСТИНОВ[2]

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

[2]*Финансовый университет, Москва*

ФОРМИРОВАНИЕ НОВОГО ПОДХОДА К ОЦЕНКЕ ЗАЩИЩЕННОСТИ АКУСТИЧЕСКОЙ (РЕЧЕВОЙ) ИНФОРМАЦИИ

Целью настоящей работы является изучение возможностей применения методов оценки качества изображений для сравнения спектрограмм акустических (речевых) сообщений и формирование нового подхода к оценке защищенности акустической (речевой) информации. Предлагаемый подход позволяет достаточно просто (с вычислительной точки зрения) и быстро провести анализ безопасности средств (систем) защиты речевой информации без использования соответствующих инструментальных методов.

Постановка задачи

Основной задачей настоящей работы является формирование нового подхода к оценке защищенности акустической (речевой) информации (АРИ), основанного на оценке качества изображений.

Анализ критериев оценки качества изображений

Для решения поставленной задачи были проанализированы следующие критерии оценки качества изображений: MSE, PSNR, Норма Минковского, UQI, VIF, SSIM, MSSIM, CW-SSIM.

Анализ проводился на изображениях спектрограмм (рис. 1) различных речевых сообщений (РС), оригинальных и синтезированных, с использованием технологии образного анализа-синтеза [1].

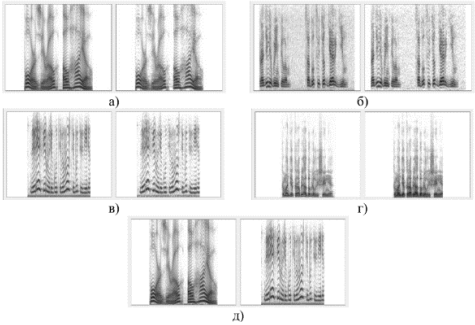

Рис 1. Спектрограммы оригинальных и синтезированных РС (а-г) и различных РС (д)

Результаты анализа показали, что наибольшей адекватностью и точностью обладает критерий CW-SSIM. При сравнении спектрограмм рис. 1а–1г оригинальных и синтезированных РС значения CW-SSIM = 0,987…0,988. Для различных спектрограмм рис. 1д значение CW-SSIM = 0,467.

Новый подход к оценке защищенности АРИ

Предлагаемый подход к вычислению показателя защищенности АРИ заключается в следующем. На первом этапе осуществляется построение спектрограммы оригинального РС. Далее выполняется преобразование над РС или его спектрограммой. На завершающем этапе проводится сравнение спектрограмм оригинального и преобразованного РС с использованием критерия CW-SSIM. Интерпретация результатов предлагаемого подхода представлена в табл. 1.

Таблица 1. Цели и критерии эффективности систем защиты АРИ

Цель защиты	Критерий эффективности защиты (W_n – речевая разборчивость)	Критерий эффективности защиты с использованием CW-SSIM
Скрытие факта ведения переговоров	$W_n \leq 10\ \%$	$CW-SSIM \leq 0{,}1$
Скрытие предмета переговоров	$W_n \leq 20\ \%$	$CW-SSIM \leq 0{,}2$
Скрытие содержания переговоров	$W_n \leq 30\ \%$	$CW-SSIM \leq 0{,}3$

Заключение

В результате проведенной работы был предложен подход к оценке защищенности АРИ, основанный на использовании критерия CW-SSIM. Данный подход позволяет достаточно просто (с вычислительной точки зрения) провести экспресс анализ безопасности систем (средств) защиты АРИ без применения сложной вычислительной аппаратуры.

В качестве дальнейших исследований в указанном направлении целесообразно провести апробацию предлагаемого подхода на большем количестве РС, а также оценить возможность использования вместо спектрограмм РС графические представления фонетической функции Пирогова.

Список литературы

1. Дворянкин С.В., Дворянкин Н.С., Устинов Р.А. Развитие технологий образного анализа-синтеза акустической (речевой) информации в системах управления, безопасности и связи // Безопасность информационных технологий. Том 26, № 1. 2019. С. 64–76.

УДК 004.239

А.Д. ЕСАКОВ
ООО «НТЦ МакроСистемы», Москва

ИССЛЕДОВАНИЕ И МОДИФИКАЦИЯ МИКРОПРОЦЕССОРНОГО ЯДРА SCR1 С АРХИТЕКТУРОЙ RISC-V ДЛЯ ИНТЕГРАЦИИ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ОТЕЧЕСТВЕННЫХ АЛГОРИТМОВ

Работа посвящена разработке аппаратных механизмов защиты информации, использующих алгоритмы стохастического преобразования, а также исследованию и модификации микропроцессорной системы на основе процессорного IP-ядра для интеграции данных механизмов с целью обеспечения защиты информации в системе от атак с выполнением произвольного кода. В результате работы механизмы защиты реализованы и интегрированы в микропроцессорную систему для ПЛИС, выполнено тестирование механизмов проведением атаки, измерены потери производительности системы.

Распространённым видом атак на информационные системы являются атаки с выполнением произвольного кода. Как правило, такие атаки проводятся путём записи в память подготовленных нарушителем данных, которые выполняются компьютером как код, что позволяет нарушителю выполнять несанкционированные действия [1]. Большинство механизмов защиты от этих атак основано на логическом разделении страниц памяти данных и кода или на методах анализа кода программ, однако эти методы носят частичный характер и предоставляют защиту лишь от отдельных уязвимостей [2–4].

Перспективным методом защиты от таких атак является защита на основе подвижных целей. При использовании этого метода в состояние вычислительной системы вносится случайное изменение, затрудняющее нарушителю подбор необходимой для атаки информации [5]. Например, в архитектуре Morpheus реализован вариант данного метода, в котором изменение генерируется и вносится в систему периодически. Этот вид защиты также имеет в некоторой степени свойство превентивности [4, 6].

В данной работе реализованы механизмы защиты информации с подвижными целями, основанные на тегировании кода и данных в памяти и периодическом стохастическом преобразовании адресного пространства процессора и представления команд и данных в памяти при помощи алгоритма ГОСТ 34.12-2018 «Кузнечик». При преобразовании физические

адреса и представления команд и данных вычисляются на основе логических адресов и представлений с помощью алгоритма стохастического преобразования, ключ которого меняется с определённым периодом. Предполагается, что к возможным уязвимостям системы относятся недостатки, связанные с внедрением произвольного кода, неполнотой проверки входных данных, неконтролируемой форматной строкой либо переполнением буфера памяти.

Микропроцессорная система реализована на ПЛИС Xilinx Zynq-7000 и состоит из IP-ядер микропроцессора SyntaCore SCR1 с архитектурой RISC-V, оперативной памяти, алгоритма стохастического преобразования «Кузнечик» и интерфейса памяти. Проведено тестирование системы с механизмами защиты путём выполнения программы, реализующей атаку с переполнением буфера входных данных.

Разработанные механизмы можно использовать для повышения эффективности защиты информации в микропроцессорных системах от атак с выполнением произвольного кода и некоторых других атак с перехватом потока управления программ. В отличие от других типов механизмов защиты, реализованные в работе механизмы охватывают весь класс атак с выполнением произвольного кода, а не только отдельные их виды. Кроме того, данные механизмы опережают зарубежные аналоги по характеристике потерь производительности системы. Также стохастическое преобразование адресного пространства, применяемое в работе, вносит в расположение защищаемой информации в памяти больше неопределённости, чем в аналогичных механизмах, за счёт обеспечения не только абсолютного, но и относительного смещения данных от их логических адресов в памяти.

Список литературы

1. Conti M. et al. Losing control: On the effectiveness of control-flow integrity under stack attacks. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. – 2015. – С. 952–963.

2. Lhee K. S., Chapin S. J. Buffer overflow and format string overflow vulnerabilities // Software: practice and experience. – 2003. – Т. 33. – №. 5. – С. 423–460.

3. Johnson P. Intrinsic Propensity for Vulnerability in Computers? Arbitrary Code Execution in the Universal Turing Machine. arXiv preprint arXiv:2105.02124. – 2021.

4. Harris A. et al. Morpheus II: A RISC-V Security Extension for Protecting Vulnerable Software and Hardware. 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). – IEEE, 2021. – С. 226–238.

5. Jajodia S. et al. (ed.). Moving target defense: creating asymmetric uncertainty for cyber threats. Springer Science & Business Media, 2011. – Т. 54.

6. Gallagher M. et al. Morpheus: A vulnerability-tolerant secure architecture based on ensembles of moving target defenses with churn. Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems. — 2019. – С. 469–484.

УДК 004.056

А.И. СТРЕЛЕЦ, М.Н. ЁХИН, И.А. ЛОГВИНЕНКО
Национальный исследовательский ядерный университет «МИФИ», Москва

АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ ЦИФРОВЫХ УСТРОЙСТВ В МНОГОПОЛЬЗОВАТЕЛЬСКОЙСИСТЕМЕ ВИРТУАЛЬНЫХ СТЕНДОВ

В современных информационных и вычислительных системах проблеме аутентификации пользователя отведено важное место и существует целый ряд решений, обеспечивающих безопасную аутентификацию. Однако большинство этих способов аутентификации предполагают, что субъектом аутентификации являются люди. В системе виртуальных стендов, предназначенной для многопользовательской удаленной работы студентов и преподавателей с различными цифровыми устройствами, субъектами аутентификации выступают не только люди, но и цифровые устройства – FPGA, SoC и др. При этом, уровень развития средств информационной безопасности в решениях производителей цифровых устройств либо низок, либо такие средства отсутствуют вовсе. Это приводит к необходимости разработки средств аутентификации и авторизации, предназначенных для работы с цифровыми устройствами.

Современные информационные и вычислительные системы отличаются высокой архитектурной сложностью и обилием составных компонентов. Всё это увеличивает объем оборудования системы, доступного злоумышленнику для атаки. Наиболее простой способ защиты от атаки – это физическая недоступность системы из сети интернет. В случае с рабочими местами пользователей в лаборатории именно изолированность служит самой надежной защитой, поскольку вся работа происходит в локальном режиме на компьютерах в лаборатории. Пользователю доступен компьютер на рабочем месте, цифровое устройство подключено к компьютеру через USB, а доступ в интернет осуществляется через стандартные порты или отсутствует вовсе. Проблема защищенности рабочего места в такой конфигурации эквивалентна проблеме защищенности обычного рабочего места пользователя и имеет массу стандартных решений [1]. Иначе обстоит дело, если возникает необходимость удаленного доступа к цифровым устройствам в лаборатории.

Учебный процесс в лабораториях с цифровыми устройствами выстроен таким образом, что пользователи (студенты) используют цифровые устройства, установленные в лаборатории. Это накладывает

ограничения на образовательный процесс, делая невозможным удаленные курсы или доступ в нерабочее время. Для решения этой проблемы была разработана многопользовательская система со специальными виртуальными стендами для удаленного подключения студентов к устройствам через интернет. Однако использование этой системы привело к возникновению дополнительных векторов атаки через сеть. Система является веб-сервисом, к которому подключаются студенты, преподаватели, а также цифровые устройства. Аутентификация пользователей осуществляется стандартными средствами на основе пароля. Помимо людей, к данной системе также подключаются и обмениваются информацией устройства из лаборатории. Эти устройства также являются субъектами аутентификации, не являясь при этом людьми. Стандартные средства аутентификации – аутентификация на основе пароля, двухфакторная аутентификация или на основе токенов не являются применимыми в данном случае, поскольку подразумевают использование пароля, который необходимо хранить отдельно от устройства [2].

Наиболее перспективным способ аутентификации устройств в данном случае является аутентификация на основе ключей доступа. Такой подход позволяет избежать передачи пароля сторонний приложениям или злоумышленнику [3]. Однако, тот факт, что субъектом аутентификации является устройство, а не пользователь, добавляет свои особенности. Например, ключ может храниться внутри устройства в специальных разделах памяти на FPGA.

Таким образом, актуальной задачей является разработка способа аутентификации на основе ключей доступа для случаев, когда субъектом аутентификации являются цифровые устройства лаборатории, и интеграция этого способа аутентификации в многопользовательскую систему виртуальных стендов.

Список литературы

1. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей. Authentication: From Passwords to Public Keys First Edition. – М.: Вильямс, 2002. – 432 с.

2. Шнайер Б.Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.

3. Иванов М.А. Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи. // Вопросы кибербезопасности. – 2019. – № 3(31). – С. 45–50. DOI: 10.21681/2311-3456-2019-3-45-50.

УДК 004.891.3

Е.Ю. ШТАНОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

CHATGPT В ОБУЧЕНИИ АСПИРАНТОВ

В данной работет сравнивается процент генерации текста с помощью чат-бота ChatGPT в реферативных работах аспирантов 1-го курса по философии в рамках сдачи кандидатского минимума. В ходе работы анализируются выборки за 2021 и 2022 гг. Проверка студенческих работ реализуется с помощью инструментов с открытым исходным кодом, объединенных в одну программу.

Введение

30 ноября 2022 г. была опубликована первая версия ChatGPT – «чат-бота с искусственным интеллектом». ChatGPT – языковая модель, для тренировки которой использовались методы обучения с учителем и обучения с подкреплением. Популярность данная модель обрела благодаря корректным ответам практически на любой вопрос – её можно «попросить» написать, как сочинение, так и программный код [1].

Постановка задачи

Возможность автоматизации ручного труда, в том числе по написанию рефератов, не могла быть проигнорирована студентами высшей школы [2]. Поскольку одним из этапов сдачи кандидатского минимума по философии является написание реферативных работ, к обязанности преподавателя, помимо проверки на плагиат, добавляется необходимость выявления сгенерированного ИИ текста. Все породило запрос на создание автоматизированного инструмента выявления сгенерированного текста.

Основная часть

В рамках данной работы были использованы три инструмента:

1. roberta-base-openai-detector;
2. roberta-large-openai-detector;
3. open-ai-classificactor (OAIC).

Из перечисленных инструментов первые два являются моделями ИИ на базе ChatGPT, обученные на выялвние сгенерированного текста (отличаются объемом обучающей выборки) [3]. Третий инструмент предоставляется компанией OpenAI (разработчиком ChatGPT). Также при анализе собирается ряд статистической информации – энтропия и количество слов в реферате.

С помощью разработанного инструмента были проанализированы 115 рефератов 2022 г. (данные работы были написаны до ChatGPT) и 140 работ 2023 г.. При анализе особое внимание обращалось на работы, у которых возникало превышение по исследуемым параметром. Статистика за 2022 г. приведена в табл. 1, статистика по 2023 г. в табл. 2.

Таблица 1. Результаты 2022 г.

Tool	Roberta Base	Roberta Large	Open AI
Минимум	5.85	50.09	46.7
Максимум	99.97	89.52	94.8
Среднее	79.97	60.7	79.05
Среднеквадратичное откл.	21.9	8.14	9.43
Границы нормализации	-3.83; 0.91	-1.3;3.53	1.66;-1.21

Таблица 2. Результаты 2023 г.

Tool	Roberta Base	Roberta Large	Open AI
Минимум	2.63	50.09	58.3
Максимум	99.83	86.79	91.7
Среднее	84.04	60.95	80.43
Среднеквадратичное откл	23.0	9.22	7.55
Границы нормализации	-0.81; 0.15	-0.12;0.29	0.24;0.12

Заключение

Использование выбранных данных инструментов позволило выявить 38 рефератов, полностью или частично созданных с использованием ИИ.

Список литературы

1. Leshchev, S.V.: Artificial Intelligence Limitations: Blockchain Trust and Communication Transparency. Studies in Computational Intelligence 1032 SCI, 249–254 (2022).

2. Alshater, M.: Exploring the Role of Artificial Intelligence in Enhancing Academic Performance: A Case Study of ChatGPT, https://ssrn.com/abstract=431235

3. Selwyn, N. (2022). The future of AI and education: Some cautionary notes. European Journal of Education, 57(4), 620–631.

УДК 004.056

П.А. ТЕПЛЮК, А.Г. ЯКУНИН

Алтайский государственный технический университет им. И.И. Ползунова, Барнаул

АНАЛИЗ МОДЕЛЕЙ ПОВЕРХНОСТИ АТАКИ ДЛЯ ФАЗЗИНГА ЯДРА LINUX

Одним из эффективных методов обнаружения уязвимостей в ядре Linux является фаззинг-тестирование. В число важных задач, необходимых для проведения эффективного фаззинг-тестирования, входит определение поверхности атаки. В работе проанализированы существующие модели поверхности атаки ядра операционной системы (ОС); выбрана наиболее подходящая модель для определения фаззинг-целей в ядре Linux.

Введение

Широкое распространение ОС на базе ядра Linux в качестве основы системного ПО приводит к росту количества напрямую зависимых от его безопасности информационных систем [1], в т.ч. разрабатываемых в защищенном исполнении.

Как следует из утверждённой ФСТЭК России «Методике выявления уязвимостей и недекларированных возможностей в программном обеспечении» [2], одним из этапов разработки безопасного ПО является выполнение динамического анализа кода, в том числе с применением фаззинг-тестирования [3]. Важной задачей для эффективного тестирования методом фаззинга является определение поверхности атаки [4].

Постановка задачи

Для описания поверхности атаки в ядре Linux необходимо обозначить универсальную модель безопасности, покрывающую надёжность всего работающего ядра, а затем более конкретные модели, охватывающие локальные атаки из пользовательского пространства. Целью работы является анализ существующих моделей определения поверхности атаки применительно к фаззингу ядра Linux. В [5] предлагаются 3 общие модели поверхности атаки ядра: GenSec, IsolSec и StaticSec.

Модель GenSec покрывает все возможные сбои ядра, включая их в поверхность атаки. Допускается, что злоумышленник может быть как локальным, так и удалённым, т.е. он имеет учётную запись в целевой системе и может взаимодействовать со всеми аппаратными устройствами. Также злоумышленник имеет некоторый контроль над

привилегированными приложениями. Данная модель безопасности является довольно обширной, поэтому учитывать все будущие действия во время функционирования ОС при её применении очень сложно.

Модель IsolSec отражает общую модель поверхности атаки в многопользовательских системах, а также в других системах, в которых предполагается, что злоумышленник изначально не имеет доступа к привилегированным процессам. Согласно этой модели, злоумышленник может повысить свои привилегии, например, используя внедрение кода в некоторые загружаемые модули (Loadable Kernel Module – LKM) или уязвимости в интерфейсе системных вызовов.

Модель изоляции StaticSec схожа с IsolSec, однако её отличие состоит в том, что в StaticSec злоумышленник не может модифицировать LKM.

Заключение

Рассмотренные модели поверхности атаки ядра Linux предполагают различный уровень привилегий в системе, доступный злоумышленнику. При решении задачи фаззинг-тестирования ядра Linux, определение поверхности атаки поможет более точно сформировать список фаззинг-целей. Программные дефекты, потенциально, могут присутствовать в различных разделах исходного кода ядра Linux, поэтому фаззинг-тестирование должно охватывать как можно больше подсистем и модулей. Поскольку целями фаззинга могут быть не только системные вызовы, но и, например, внешние интерфейсы, работающие с аппаратными средствами [6], то для его применения наиболее подходящей является модель GenSec.

Список литературы

1. Международный проект по разработке ядра Linux [Электронный ресурс]. Режим доступа: http://samag.ru/archive/article/4534#f-01, свободный (дата обращения: 27.08.2023).

2. Информационное сообщение ФСТЭК России от 10 февраля 2021 г. [Электронный ресурс]. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/info rmatsionnye-i-analiticheskie-materialy/informationnoe-soobshchenie-fstek-rossii-ot-10-fevralya-2021-g-n-240-24-647, свободный (дата обращения: 28.08.2023).

3. Козырский, Б. Л. Использование фаззинга для поиска уязвимостей в программном обеспечении / Б. Л. Козырский, Т. И. Комаров, М. А. Иванов // Безопасность информационных технологий. – 2014. – Т. 21, № 4. – С. 33–43. – EDN TSEIMN.

4. DevSecOps: Фаззинг исходного кода [Электронный ресурс]. Режим доступа: https://dsec.ru/wp-content/uploads/2020/12/dseconair_b.-ryutin-p.-knyazev_fazzing_ishodnogo_koda.pdf, свободный (дата обращения 10.09.2023).

5. Quantifiable Run-time Kernel Attack Surface Reduction [Электронный ресурс]. Режим доступа: https://www.ibr.cs.tu-bs.de/users/kurmus/papers/kurmus-dimva14.pdf, свободный (дата обращения 01.09.2023).

6. USB Hacking [Электронный ресурс]. Режим доступа: https://github.com/xairy/usb-hacking, свободный (дата обращения 10.09.2023).

УДК 004.056

С.А. РАКОВСКИЙ
МИРЭА – Российский технологический университет, Москва

ПРЕСТУПЛЕНИЯ В OPENSOURCE: РАССЛЕДУЕМ ТРОЯНЫ В PYTHON PACKAGE INDEX

Проведен поиск пакетов, добавленных и в скором времени удалённых в Python Package Index за последнее время. Среди них найдены пакеты, которые были удалены, в том числе по причине наличия вредоносной или нежелательной активности. Найдены общие паттерны в метаинформации, к которым прибегают злоумышленники в рамках публикации своих пакетов.

Введение

Нет ни одного месяца, когда бы компании, занимающиеся безопасностью процессов разработки, не сообщали о том, что в открытых хранилищах кода были найдены всё новые и новые вредоносные пакеты. Сам факт обнаружения – хорошая информация, ведь кто-то отслеживает деятельность злоумышленников в opensource. Однако данные исследования обычно являются частью коммерческого продукта, поэтому оценить состоятельность подходов мы можем только по результатам, то есть по количеству найденных пакетов.

Аналитики, проводящие исследования открытых проектов, отмечают, что Python в последнее время находит всё большую популярность, а для некоторых направлений, таких как искусственный интеллект, уже стал наиболее значимым языком программирования [1]. За последние несколько лет разные группы исследователей обращали внимание на Python Package Index в поисках паттернов, являющихся уникальными для вредоносного кода [1], сравнивали различные реализации сканеров безопасности [2], изучали атаки с использованием опечаток в названиях пакетов [3–5].

Однако даже под неусыпным надзором компаний и исследователей вредоносному программному обеспечению удаётся оставаться незамеченным на протяжении нескольких недель, что создает угрозу компрометации разработчиков, инфраструктуры организаций, конечных пользователей продукта.

Ход исследования

За лето 2023 г. пользователями PyPI было создано 24126 новых пакетов, 3084 (12,8%) из которых были удалены за тот же период. Среднее время жизни удалённых пакетов – 83 часа, медиана – 19 часов. Далее

последовало сравнение заимствования метаинформации из 8000 популярных пакетов с учетом пересечения разработчиков. Обнаружено 110 пакетов (3.6% от числа удаленных пакетов), заимствующих информацию без прямой связи с разработчиком. Среди этих пакетов 73 (66%) копируют информацию для связи с разработчиком из популярных пакетов и полное описание проекта, 50 (45%) – ссылку на домашнюю страницу (и, соответственно, информацию о популярности проекта на GitHub), 30 (27%) используют обе техники одновременно. Также среди 38 пакетов (1.2 от общего числа) прослеживается использование техники typosquatting (использование названия, схожего с оригинальным пакетом, в надежде, что разработчик опечатается при наборе названия устанавливаемого пакета) – wheel1, requosts и другие пакеты. Показатели {min, avg, mean, max} для пакетов, заимствующих информацию из популярных проектов, составило {0.01, 70, 250, 1134} часов, и пакетов, которые используют схожие с популярными наименования – {0.01, 109, 339, 967} часов.

Заключение

Исследование показало, что злоумышленники могут использовать техники, которые целыми днями остаются незамеченными современными подходами по их обнаружению. Низкое время обнаружения некоторых пакетов показывает, что текущий мониторинг создаваемых пакетов, реализуемый коммерческими решениями и исследователями, неэффективен с точки зрения времени реагирования. Проблема может заключаться не только во времени реагирования на новый вредоносный пакет, но и во времени уведомления администраторов PyPI и последующего за этим удаления.

Список литературы

1. Liang G. et al. Malicious packages lurking in user-friendly python package index //2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). – IEEE, 2021. – С. 606–613.

2. Vu D. L., Newman Z., Meyers J. S. Bad Snakes: Understanding and Improving Python Package Index Malware Scanning //2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE). – IEEE, 2023. – С. 499–511.

3. Vu D. L. et al. Typosquatting and Combosquatting Attacks on the Python Ecosystem //5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020. – Institute of Electrical and Electronics Engineers Inc., 2020. – С. 509–514.

4. Truong M. T. Typosquatting Attacks and Mitigations: diss. – University of Applied Sciences, 2023.

5. Vu D. L. et al. Towards using source code repositories to identify software supply chain attacks //Proceedings of the 2020 ACM SIGSAC conference on computer and communications security. – 2020. – С. 2093–2095.

УДК 004.056

П.М. КУРЧАВОВ
МИРЭА – Российский технологический университет, Москва

ФОРМАЛИЗАЦИЯ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ИНФРАСТРУКТУРНОГО ДЕСТРУКТИВИЗМА

Представлена формализация процесса обеспечения целостности КИИ, выполненное на базе исследование взаимосвязи ее элементов. Определены антропорфические виды межобъектных взаимодействий, влияющие на целевую функцию целостности информации. Рассмотрена роль категорий значимости объектов КИИ при построении базовой матричной модели взаимодействия объектов КИИ.

Введение

В настоящее время количество предприятий, являющихся субъектами критической информационной инфраструктуры (КИИ), становится все больше. Согласно ФЗ №187 [1] КИИ функционируют в сферах: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка и т.п. Для обеспечения безопасности существует ряд подходов, реализующих обеспечение целостности, большинство из которых не способны покрыть весь кластер задач.

Постановка задачи

Нарушение инфраструктурной целостности может снизить уровень безопасности как отдельного элемента системы, так и системы в целом [2], увеличивая тем самым появление инфраструктурного деструктивизма, который подразумевает под собой саморазрушение инфраструктуры субъекта [3]. Для предотвращения деструктивного влияния на субъекты критической информационной инфраструктуры необходимо формализовать процесс обеспечения целостности КИИ, для разработки методики, решающей эту задачу.

Решение поставленной задачи

Для решения поставленной цели система должна быть рассмотрена с точки зрения структурного анализа.

В рамках формализации процесса были рассмотрены примеры полиморфизма уязвимостей [4], а именно тот факт, что уязвимости в системе могут оказывать сильное влияние на окружающую их систему, а

также и на другие уязвимости в системе. Таким образом, можно сделать вывод о возможности изучения структуры системы взаимодействующих объектов, не столько с точки зрения ее функциональных элементов, но и со стороны уязвимостей и потенциальных угроз, которые могут появляться с ней со временем, в процессе функционирования и масштабирования. Примером такого взаимодействия является «конкуренция», которая подразумевает наличие конкурируещего за ресурсы взаимодействия. Это происходит в том случае, когда для реализации основного функционала необходимо использование одних и тех же ресурсов системы, что приводит к борьбе за них, тем самым понижая эффект деструктивного воздействия на систему, от данных уязвимостей.

В ходе исследования рассматривается базовая модель, в которой в отношении «элемент – критерий» выполнен по принципу 1 к 1. Данная модель представлена в логической форме:

$$((x \vee y) \vee (x \wedge y)) \wedge (x \leftrightarrow y)\,(a \wedge x),$$

где a – переменные, отображающие соответствие категории значимости; x и y – переменные, отображающие функциональную стабильность характеристик элемента. Данная модель является фрагментом универсальной логической модели оценки целостности системы.

Заключение

В данной работе представлен фрагмент процесс формализации системы обеспечения целостности критической информационной инфраструктуры с учетом взаимодействия уязвимостей в структуре объектов. Реализация данной модели позволит выйти на методику оценки целостности КИИ в условиях инфраструктурного деструктивизма. Данные способы являются вспомогательными на пути построения методики по оценке целостности критической информационной инфраструктуры, но при этом составляют её основу.

Список литературы

1. О безопасности критической информационной инфраструктуры Российской Федерации // Федеральный закон от 26.07.2017 N 187-ФЗ.

2. Основы информационной безопасности. Часть 1: Виды угроз [Электронный ресурс]: Хабр URL: https://habr.com/ru/company/vps_house/blog/343110/.

3. Максимова, Елена Александровна. Инфраструктурный деструктивизм субъектов критической информационной инфраструктуры. / МИРЭА – Российский технологический университет. – М.: Издательство Волгоградского государственного университета – 2021. – С. 170–180 – ISBN 978-5-9669-2147-7.

4. Буйневич Михаил Викторович. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде / Ч. 1. Типы взаимодействий / М.В. Буйневич, К.Е. Израилов // Защита информации. Инсайд. – 2019. – № 5. – С. 78–85.

УДК 004.056

Д.В. КИРИЛЛОВ
Самарский национальный исследовательский университет им. академика С.П. Королева

МЕТОДИКА РАЗРЕШЕНИЯ КОНФЛИКТОВ В МОДЕЛЯХ УПРАВЛЕНИЯ СИСТЕМ КОНТРОЛЯ ДОСТУПА

В работе рассматривается проблема разрешения конфликтов в моделях управления системами контроля доступа, использующих динамический или отложенный механизмы назначения, отзыва и проверки полномочий, а также предлагается методика разрешения таких конфликтов.

Механизмы разграничения и управления доступом, а также модели управления такими механизмами, предусматривающие отложенную реализацию решений по предоставлению или отзыва полномочий [1], характеризуются проблемой возникновения конфликтов среди элементов, определяющих данные решения [2]. Причиной этого является то, что правила, порождающее те или иные действия связанны с изменением полномочий, могут семантически пересекаться между собой. При этом пересекающиеся правила могут порождать противоположные действия по отношению к одним и тем же субъектам/объектам/полномочиям, либо другим элементам. Конфликты приводят к возникновению ситуаций неопределенности, в которых система управления доступом либо не может принять однозначное решение о том, какое действие необходимо выполнить, либо выполняемое действие может не соответствовать ожидаемому. Для предотвращения таких ситуаций или минимизации вероятности их возникновения, необходимо, с одной стороны, разработать методику предотвращения и разрешения конфликтов и реализовывать управляющие механизмы систем разграничения доступа с учетом данной методики.

Рассмотрим основные положения методики. Первым шагом необходимо определить предполагаемые источники конфликтов – например, для модели событийно-обусловленного делегирования полномочий, источником являются с правила, определяющие действия по делегированию или отзыву полномочий.

Вторым шагом, необходимо провести декомпозицию источников конфликтов, в том случае, если они имеют сложную структуру – в рассматриваемом примере, в результате декомпозиции мы получаем два

компонента – события и условия. Данные компоненты в их сочетаниях и порождают потенциальные конфликты.

Третьим шагом, необходимо реализовать методы семантического сопоставления правил и их компонентов между собой, для того чтобы в дальнейшем иметь возможность определить, пересекаются семантически компоненты правил или нет.

Четвертым шагом, необходимо определить, при каких условиях возможно возникновение конфликтов и типизировать их. В рассматриваемой в качестве примера модели, такие ситуации возможны:

1) В контексте одного правила – когда семантически пересекаются два или более событий, или элементы правил, использованные в логически противоречивых конструкциях

2) В контексте различных правил – когда, существует более одного правила, семантически пересекающихся по своему содержимому, при этом действия, порождаемые этими правилами не согласованы между собой (противоположны по смыслу)

Пятым шагом, определить механизм ранжирования потенциальных конфликтов по категориям – опасные и неопасные. К опасным относятся такие конфликты, которые порождают потенциальной реализации угроз безопасности, к неопасным – не ведущие к потенциальной реализации угроз безопасности.

На следующем шаге необходимо определить механизм разрешения конфликтов, который будет использоваться в том случае, если конфликт все-таки возникает. В рамках данного механизма должны быть заданы действия, которые необходимо предпринять при возникновение конфликтов системой, методы приоритезации таковых действий, механизмы протоколирования и уведомления.

При применении данной методики, возможно обеспечить с одной стороны минимизацию вероятности возникновения конфликтов, с другой стороны, так как полностью избежать конфликтов в целом невозможно, в случае если конфликтные ситуации возникают, методика позволяет минимизировать негативные последствия от их возникновения.

Список литературы

1. Кириллов Д.В. Основные принципы событийно-обусловленного делегирования и отзыва полномочий в системах контроля доступа на основе ролей // Вестник Уфимского государственного авиационно-технологического университета. 2009. – Т. 12. № 1. – С. 218–225.

2. Adi, K., Bouzida, Y., Hattak, I., Logrippo, L., Mankovskii, Typing for Conflict Detection in Access Control Policies. //E-Technologies: Innovation in an Open World. MCETECH 2009. Lecture Notes in Business Information Processing, vol 26. Springer, Berlin, Heidelberg

УДК 004.056.5

Ф.А. СУХОНОСОВ, И.В. ВАХНЕНКО, Д.Р. ИГНАТЬЕВ
Южно-Российский государственный политехнический университет им. М.И. Платова (ЮРГПУ НПИ), Новочеркасск

ТАРГЕТИРОВАННЫЕ КОМПЬЮТЕРНЫЕ АТАКИ, КАК ОСНОВНАЯ ОПАСНОСТЬ ДЛЯ РАБОЧИХ СТАНЦИЙ

Целью данного доклада является изучение и анализ таргетированных атак на информационные системы предприятий. Для достижения данной цели проведен анализ терминологии предметной области, исследованы особенности информационных систем предприятий и таргетированных атак.

Информация имеет большое значение в жизнедеятельности любой компании, вне зависимости от ее формы собственности. В условиях современного мира защита сведений, составляющих какую-либо тайну (коммерческую, банковскую, профессиональную и т.д.) является актуальным вопросом, требующим вклада самых разных ресурсов, в том числе – человеческих.

Каждый год сопровождается улучшением инструментов и методов управления бизнесом, развитием инфраструктуры и внедрением новых достижений и технологий. Неполадки в сети, интернете или взаимодействии с другими компаниями могут привести к полному или частичному нарушению рабочих процессов, что в свою очередь может привести к финансовым потерям.

За последние годы отмечается смещение акцента с массовых атак на более целенаправленные, направленные на конкретные цели и субъекты. Предсказать такого рода атаки достаточно сложно, но возможность их обнаружения все же существует. В связи с этим, для выявления таргетированных атак необходимо анализировать множество событий информационной системы, используя существующие подходы к обнаружению.

Таргетированные или целевые атаки – это атаки, подразумевающие нацеленность на определенный объект, представляющий собой коммерческие или муниципальные организации и ведомства [1].

Главный мотив или главная проблема таких атак состоит в хищении секретной информации для достижения преследуемых замыслов и целей.

Отличительной характеристикой таргетированных атак является нацеленность на определенную организацию или ведомство [2].

Нацеленные атаки проходят через определенные этапы, которые тщательно прорабатываются и точно выполняются, без отклонений.

Таргетированные атаки делятся на сетевые и системные [3]. Сетевые атаки заключаются в захвате контроля над системой или повышения привилегий для осуществления управления. Также зачастую они направлены на кражу персональных данных, сбои в функционировании системы или нарушению ее работы, к таким атакам относятся парольные атаки, IP-спуфинг, SQL-иньекция или уязвимость нулевого дня.

Системные атаки – атаки, использующие уязвимости в системных программах – ошибки, недочеты, к ним относятся DDoS атаки, сетевые черви и различные вирусы [4].

Пример таргетированной атаки можно было наблюдать на зимней олимпиаде в Пхенчхане. Olympic Destroyer парализовал работу IT- систем: были отключены экраны, не было сети Wi-Fi, не работал официальный веб-сайт Олимпиады, из-за чего болельщики не могли распечатать билеты, а также была нарушена работа горнолыжных подъемников. После стало ясно, что данная атака была предварительно спланирована и продолжалась в течение значительного периода времени.

Для защиты рабочих станций от таких атак необходимо принимать ряд мер. Во-первых, важно обеспечить регулярные обновления операционных систем и прикладного программного обеспечения. Во-вторых, необходимо использовать надежные антивирусные программы и фаерволы. Кроме того, важно обучать пользователей основам безопасности информации.

Список литературы

1. APT Таргетированные или целевые кибератаки «Развитая устойчивая угроза» / Tadviser – 2019 – Tadviser, 2019 - Режим доступа: http://www.tadviser.ru/index.php/ Милославская Н.Г., Толстой А.И. Управление информационной безопасностью. М.: НИЯУ МИФИ, 2020. – 536 с.

2. Кривцова К.А. Таргетированные атаки. К.А. Кривцова // Наука и молодёжь: новые идеи и решения. Материалы X международной научно-практической конференции молодых исследователей: Сб. статей. – Волгоград, 2016. – С. 197–-199.

3. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы. / Современные тенденции технических наук: материалы международной научной конференции – Уфа, 2011. – С. 8–13;

4. Маркина Т.А. Средства защиты вычислительных систем и сетей: Учебное пособие. – СПб: Университет ИТМО, 2016. – 71 с.

УДК 004.056

Л.Я. ДОБКАЧ
АО «Центр эксплуатации объектов космической наземной инфраструктуры», Москва

РАСЧЁТ СЛОЖНОСТИ УНИФИЦИРОВАННОЙ СИСТЕМЫ УГЛУБЛЁННОГО ОБНАРУЖЕНИЯ КИБЕРУГРОЗ

Отсутствие унифицированного образца системы расширенного обнаружения и реагирования (XDR) приводит к трудностям с определением эффективности этой новой технологии. Если же рассматривать в качестве образца архитектуру XDR на основе сетевой системы обнаружения вторжений и системы обнаружения и реагирования на конечных узлах (EDR), то становится возможным найти сложность соответствующего алгоритма. Для описываемой системы получена оценка сверху, исходя из которой возможно проектирование типичных XDR-систем.

Введение

Развитие информационных технологий включает в себя увеличение новых видов атак и средств их выявления и противодействия. Одним из современных видов комплексных средств защиты информации от компьютерных атак стали XDR-технологии, которые пока не получили унифицированного вида.

В то же время разные XDR-решения отличаются большей или меньшей эффективностью в вопросах своевременного обнаружения атак. Формализация хотя бы одного образца этого вида СЗИ позволит лучше проектировать системы безопасности в организациях.

Предлагается рассмотреть архитектуру XDR на основе сетевой системы обнаружения вторжений (СОВ) и системы обнаружения и реагирования на конечных узлах (EDR), использующих ансамбли искусственных нейронных сетей (ИНС) и методов машинного обучения [1]. Следует рассчитать сложность такой системы для подтверждения целесообразности её использования в качестве образца обсуждаемой технологии.

Расчёт сложности компонентов

Среди методов машинного обучения наилучшие показатели сложности показывают логистическая регрессия и стохастический градиентный спуск — $O(m \times n)$ [2], а также деревья решений — $O(n \times m \log m)$ [3].

В ансамбле трёх ИНС важную роль играют размер и количество слоёв. Для 4-х слойной ИНС сложность можно определить как $O(n_i \cdot n_{h1} + n_{h1} \cdot$

$n_{h2} + n_{h2} \cdot n_o)$, что соотносится по порядку со сложностью алгоритмов машинного обучения. Тогда самым затратным по производительности компонентом оказываются деревья решений.

Результаты эксперимента

Фактическое время может существенно отличаться от определённой выше оценки сверху на настоящем наборе данных. В эксперименте использовались подготовленные выборки из CICIDS 2017 [4].

Поскольку различные компоненты ансамбля ИНС были настроены на классификацию в целом и двух наиболее более редких классов, их размеры разнились между собой. Наиболее медленной стала ИНС3, которая предназначена для лучшего выявления атак класса Infiltration, т.к. она тратила порядка 350 мс в среднем на одно событие. Заметных потерь времени при обработке деревьями решений замечено не было.

Заключение

Оценка производительности при классификации событий не превышает $O(n \times m \log m)$, причём наиболее затратными по времени оказываются деревья решений. Описанную архитектуру можно дополнительно ускорить путём распараллеливания вычислений компонентами ансамблей.

Таким образом, данная реализация представляется целесообразной в качестве эффективного образца XDR-технологии, хотя и допускает иные варианты её воплощения.

Список литературы

1. 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 информационных технологий, 2022, т. 19, № 7 (217), с. 48–56.

2. Sarker I. H. CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet of Things. 2021, vol. 14, art. no. 100393.

3. Abspoel M., Escudero D., Volgushev N. Secure training of decision trees with continuous attributes. Cryptology ePrint Archive. 2020, art. no. 1130.

4. Васильев И.Н. Исследование методов обнаружения и устранения киберугроз для корпоративных сетей. Облачные и распределенные вычислительные системы в электронном управлении (ОРВСЭУ-2022) в рамках национального суперкомпьютерного форума (НСКФ-2022). 2022, с. 92–99.

КИБ-2023
КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Интеллектуальное управление сетевой безопасностью

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

УДК 004.056

С.С. ВЕЛИГОДСКИЙ, Н.Г. МИЛОСЛАВСКАЯ
Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ ПОДХОДОВ К ОЦЕНКЕ УРОВНЯ ЗРЕЛОСТИ ЦЕНТРОВ УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ

Подробно анализируются различные подходы к оценке уровня зрелости центров управления сетевой безопасностью (ЦУСБ). Выделяются их достоинства и недостатки, на основе которых формулируются требования к разработке собственного подхода.

В областях деятельности, трудно поддающихся формализации с использованием измеримых характеристик, к которым относится и обеспечение информационной безопасности (ОИБ), устоявшейся практикой является проведение их оценки на основе сравнения с моделью оценки, в роли которой часто выступает модель зрелости (Maturity Model). До сих пор не существует общепринятого определения того, как выглядит «зрелая технология», «зрелый процесс» или «зрелая организация». Различные модели зрелости воплощают в себе разные концепции и пути достижения зрелости [1].

Определим модель оценки уровня зрелости объекта оценки (далее для краткости – модель зрелости) как структурированный набор элементов, объединяющий информационную потребность (знания (сведения), необходимые для управления целями, задачами, рисками и проблемами [2]) установления уровня зрелости соответствующих объектов оценки с их атрибутами (свойствами или характеристиками объекта, которые могут быть определены количественно или качественно вручную или автоматическими средствами [2, 3]). Объектами оценки уровня зрелости могут выступать, например, процессы или отдельные услуги по ОИБ, а также подразделения, осуществляющие управление рисками и инцидентами информационной безопасности (ИБ). В нашем случае – это ЦУСБ для информационно-телекоммуникационной сети (ИТКС) типовой организации. В работе за основу принято описание ИТКС и ЦУСБ ИТКС организации, введенное в [1].

Продолжая исследования, начатые в работе [4], приведем результаты анализа и сравнения моделей зрелости первых типов ЦУСБ – групп реагирования на инциденты информационной безопасности (ГРИИБ) и центров мониторинга безопасности (ЦМБ).

Для анализа и сравнения выбраны следующие модели:

- модель ГРИИБ Мэттью Гардинера (Matthew Gardiner);
- Security Incident Management Maturity Model (SIM3) Дона Стиквурта (Don Stikvoort);
- Incident Management Capability Assessment (IMCA) Института программной инженерии Университета Карнеги-Меллон;
- HP Security Operations Maturity Model (HP SOMM) компании Hewlett-Packard;
- модель зрелости возможностей ЦМБ SOC-CMM Роба ван Оса (Rob van Os);
- подход к оценке уровня зрелости компании Nettitude;
- модель зрелости ЦМБ компании Huntsman;
- модель зрелости ЦМБ компании Cybereason;
- SOC – Use Case Maturity Model/Cube (SOC-UCMM);
- подход к оценке уровня зрелости ЦМБ Раджива Шуклы (Rajeev Shukla);
- подход к оценке уровня зрелости, предложенный компанией PricewaterhouseCoopers;
- Security Operations Maturity Model (SOMM) компании LogRhythm;
- модель зрелости ЦМБ компании Accenture.

Выделяются их достоинства и недостатки, на основе которых формулируются требования к разработке собственного подхода.

Список литературы

1. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. М.: Горячая линия-Телеком, 2021. – 432 с.

2. ISO/IEC/IEEE 15939:2017 Systems and software engineering — Measurement process. 2017. 39 p.

3. ГОСТ Р ИСО/МЭК 27004–2021 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. М., Стандартинформ, 2021. 46 с.

4. Милославская Н.Г., Сагиров Р.А. Обзор моделей зрелости процессов управления информационной безопасностью // Безопасность информационных технологий. – 2015. – Том 22, № 2. – С. 119–125.

УДК 004.056.5

В.И. ВАСИЛЬЕВ, А.М. ВУЛЬФИН, А.Д. КИРИЛЛОВА
Уфимский университет науки и технологий

АВТОМАТИЗАЦИЯ МОДЕЛИРОВАНИЯ СЦЕНАРИЕВ АТАК НА ПРОМЫШЛЕННЫЕ СИСТЕМЫ

Рассматривается проблема обеспечения информационной безопасности промышленных систем автоматизации. Разработана архитектура интеллектуальной системы поддержки принятия решений и программная реализация средств автоматизации моделирования сценариев проведения атак и оценки рисков информационной безопасности, применение которых позволяет повысить эффективность выбора контрмер на этапах проектирования и внедрения комплексных систем защиты информации.

Сегодня существенно выросли требования регуляторов, направленные на повышение информационной безопасности (ИБ) промышленных систем автоматизации. Необходимо обеспечить автоматизацию процессов обработки больших объемов, накапливаемых в современных системах обеспечения ИБ данных о состоянии промышленных систем, что позволит в конечном итоге повысить оперативность оценки рисков ИБ и будет способствовать повышению защищенности этих объектов в условиях воздействия возможных потенциальных угроз ИБ [1, 2].

В [3] разработана методика количественной оценки рисков ИБ промышленной системы на основе иерархии моделей и алгоритма построения сценариев атак, отличающаяся нечетким когнитивным моделированием сценариев атак в выделенных зонах промышленного объекта, что позволяет выполнить оценку рисков ИБ и оптимальное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений. Автоматизация моделирования сценариев атак позволяет извлечь информацию о слабых местах инфраструктуры, наиболее опасных уязвимостях и потенциальных слабостях компонент системы, выявить наиболее успешные сценарии атак и оценить их последствия для промышленного предприятия.

Предлагается разработать инструментальные средства автоматизации моделирования сценариев атак на промышленную систему в составе интеллектуальной системы поддержки принятия решений (ИСППР) на этапе оценки рисков ИБ.

Разработана логическая модель данных, описывающая структуру и взаимосвязь основных сущностей предметной области, используемой для

создания хранилища данных об угрозах, уязвимостях и сценариях их реализации на основе взаимодействия с внешними базами знаний БДУ ФСТЭК, NVD и MITRE.

Разработанное ПО обеспечивает поддержку принятия решений при работе с открытыми базами угроз, уязвимостей и шаблонов атак, что позволяет специалистам, зная конкретные уязвимости объекта, получить наглядную графовую модель реализации атаки [4, 5]; анализ сценариев атак с требуемым уровнем детализации и оптимизации весовых коэффициентов НКК при помощи методов машинного обучения для распределения ресурсов контрмер.

На рис. 1 представлен фрагмент архитектуры ИСППР в нотации диаграммы компонентов UML с реализацией паттерна MVC.

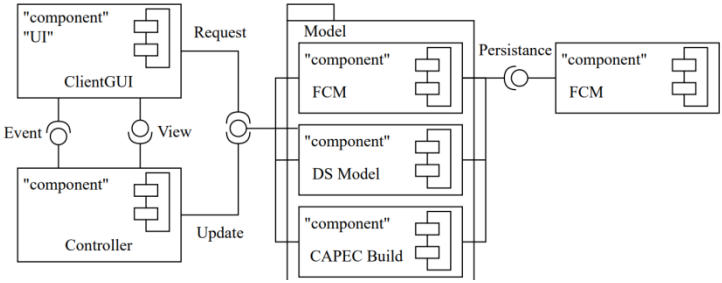

Рис. 1. Фрагмент архитектуры ИСППР (диаграмма компонентов UML)

Разработанные инструментальные средства автоматизации моделирования сценариев атак в составе ИСППР позволяют повысить достоверность и обоснованность качественных и количественных оценок рисков ИБ с учетом воздействия факторов неопределенности.

Список литературы

1. Зегжда Д.П. и др. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации. Вопросы кибербезопасности. 2018. Т. 2(26). с. 2–14

2. . Alshamrani A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials. 2019, Т. 2(21), с .1851–1877.

3. Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining. Системы управления, связи и безопасности. 2021. Т. 3. с. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134.

4. Bakhtavar E. et al. Fuzzy cognitive maps in systems risk analysis: a comprehensive review. Complex & Intelligent Systems. 2021. Т. 7(2). с. 621–637.

5. Amirkhani A., Nasiriyan-Rad H., Papageorgiou E.I. A novel fuzzy inference approach: neuro-fuzzy cognitive map. International Journal of Fuzzy Systems. 2020. Т. 22(3). с. 859–872.

УДК 519.254.1

Д.В. ИВАНОВ
Самарский национальный исследовательский университет им. академика С.П. Королева

МОДЕЛИ С РАЗНОСТЯМИ ДРОБНОГО ПОРЯДКА ВЫЯВЛЕНИЯ АНОМАЛИЙ ТРАФИКА

В работе предлагается комплекс моделей трафика компьютерных сетей на основе уравнений с разностями дробного порядка. Разработаны методы структурно-параметрической идентификации моделей трафика компьютерных сетей с длинной памятью при наличии ошибок в переменных на основе генетических алгоритмов, позволяющие выявлять аномалии трафика.

Моделирование трафика компьютерных сетей является важной и актуальной задачей. Для моделирования трафика компьютерных сетей широко используются методы анализа временных рядов. Было установлено, что трафик компьютерных сетей имеет ряд особенностей таких как самоподобие и наличие длинной памяти. [1, 2]. Самой известной моделью, позволяющей моделировать эффекты длинной памяти является модель FARIMA (fractionally difference autoregressive integrated moving average) [3, 4]. Обзор методов по выявлению аномалий трафика приведен в статье [5]. Как следует из обзора для выявления аномалий трафика на сегодняшний день используются только модели ARFIMA и GARMA (generalized autoregressive moving average) [6, 7].

Применение модели ARFIMA и GARMA сопряжено с рядом сложностей:

1. Предполагается, что на первом шаге точно, оценивается порядок дробного интегрирования. После чего может быть оценена целочисленная ARMA модель. В случае погрешности, оценки параметра дробного интегрирования ARMA модель может иметь длинную память, что обычно не учитывается и может сильно искажать модель.
2. Оценивание даже целочисленной модели ARMA на много сложнее чем оценивание авторегрессий высокого порядка.
3. Из классов моделей ARMA, авторегрессии, авторегрессия с аддитивным шумом, наилучшей разрешающей способностью для в задачах спектрального анализа в задачах спектрального анализа обладает авторегрессия с аддитивным шумом.

Применение метода наименьших квадратов для идентификации моделей с ошибками в переменных с длинной памятью приводит к крайне

неточным результатам. В работе предлагаются методы структурно-параметрической идентификации комплекса моделей с длинной памятью с ошибками переменных на основе метода обобщенных полных наименьших квадратов и генетических алгоритмов [8].

Разработанные алгоритмы и программное обеспечение используются для усовершенствования алгоритмов обнаружения DDOS-атак.

Параметры идентифицированных моделей применяются в семействе детекторов, использующих:

1) ошибку прогнозирования процесса.
2) порядок дробной разности, связанный с показателем Херста как $\alpha = H - 0.5$.
3) спектральное представление, полученное на основе оцененной авторегрессии.

Высокая точность разработанных методов оценивания авторегрессий с разностями дробного порядка позволяет улучшить показатели распознавания различных DDOS-атак в компьютерных сетях.

Список литературы

1. Leland W.E., Taqqu M.S., Willinger W., Wilson D.V. On the self-similarnature of ethernet traffic // IEEE/ACM Transactions of Networking. – 1994. – № 2(1). –P. 1–15.

2. Цыбаков Б.С. Модель телетрафика на основе самоподобного случайного процесса// Радиотехника. – 1999. – 5. – С. 24–31.

3. C.W. Granger; R. Joyeux. An introduction to long-memory time series models and fractional differencing. // Time Ser. Anal. – 1980. – №1. – P. 15–29.

4. Hosking, J.R.M. Fractional differencing. // Biometrika. — 1981. — № 68, pp. 165–176.

5. Husák, J. Komárková, E. Bou-Harb and P. Čeleda, Survey of Attack Projection, Prediction, and Forecasting in Cyber Security // IEEE Communications Surveys & Tutorials. — 2019. – № 21(1), pp. 640–660. doi: 10.1109/COMST.2018.2871866.

6. Z. Zhan, M. Xu, S. Xu, Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study // IEEE Transactions on Information Forensics and Security. – 2013. – № 8. – P. 1775–1789.

7. T.R. Pillai, S. Palaniappan, A. Abdullah, H. M. Imran, Predictive modeling for intrusions in communication systems using GARMA and ARMA models// 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW). – 2015.

8. D. Ivanov, A. Zhdanov. Symmetrical augmented system of equations for the parameter identification of discrete fractional systems by generalized total least squares // Mathematics. – 2021. – Vol. 9. – No 24. – DOI 10.3390/math9243250

9. D. V. Ivanov, V. V. Engelgardt, I. L. Sandler. Genetic algorithm of structural and parametric identification of Gegenbauer autoregressive with noise on output // Procedia Computer Science: 8, Xiamen, 27–28 января 2018 года. – Xiamen, 2018. – P. 619–625.

УДК 004.056

М.М. МУНТЯН, И.Г. СИДОРКИНА
Чувашский государственный университет им. И.Н. Ульянова, Чебоксары

СКАНИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ В ЭКОСРЕДЕ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье приведены условия для реализации сканирования сетевой инфраструктуры при помощи методов искусственного интеллекта, а также условия и «проблемные места» в эксплуатировании компонентов предлагаемого для сканирования аналитического модуля.

Введение

В настоящее время отдельного внимания заслуживает выстраивание качественной линии обороны в сетевой инфраструктуре. В дополнение к сканерам уязвимостей и системам мониторинга в [1] описывается структура нового интеллектуального модуля для таких систем. В данной работе предложено использовать экосреду, осуществляющую модификацию входных данных путем фильтрации событий безопасности для фокусировки систем мониторинга на задачах по идентификации уязвимостей и угроз безопасности информации в инфраструктуре.

Существование экосреды в условиях вспомогательного модуля

Экосреда – совокупность средств информационной системы, направленная на решение задач мониторинга. Применительно к вспомогательному модулю – это разграничение компонентов модуля (разбиение функций по компонентам), определение ограничений и «узких мест» при функционировании.

Основываясь на [1] важным условием экосреды является реализация ИИ именно в аналитическом модуле, а не в программном агенте. В противном случае возникает существенный рост требований к аппаратному обеспечению, что делает функционирование системы не эффективным. Фактически это формирует потребность в использовании специализированных ЭВМ [2]. Помимо этого, естественным препятствием для использования программного агента на практике являются вопросы связанные со сбором информации о состоянии инфраструктуры в сегменте (проблема ip-адресов). Пути решения этой проблемы состоит из трех возможных вариантов: организации совпадения логических и физических адресов сети, передачи программному агенту

адресов логической сети напрямую, использование управляемых коммутаторов для самостоятельного определения сети и «соседей» [3-4]. Также целесообразным является проведение сегментации инфраструктуры для реализации параллельного сбора и первичного анализа информации.

В результате, использование предлагаемой экосреды направлено на дополнение систем мониторинга интеллектуальной составляющей, а также способствует ускорению процесса анализа за счет организации параллельной обработки событий в разных частях инфраструктуры. Например, если MaxPatrol SIEM может обрабатывать до 60 тысяч событий в секунду [5], то применение модуля в условиях экосреды позволит снизить общий объем поступающих событий и увеличит объем обрабатываемых событий безопасности. При этом интеллектуальная составляющая позволит определять те участки инфраструктуры, которые могут быть подвержены аналогичным уязвимостям и угрозам, а также позволит определить пути борьбы с ними.

Заключение

Предложенная экосреда позволяет выделить необходимость модернизации аппаратного обеспечения, а также сегментирования инфраструктуры, устанавливает правила разработки компонентов вспомогательного модуля. Помимо этого, экосреда способствует повышению уровня ориентированности SIEM-систем на анализ событий безопасности, а также позволяет снизить нагрузку на ресурсы инфраструктуры за счет минимизации участия человека и перехода на децентрализованное функционирование.

Список литературы

1. Мунтян М.М., Сидоркина И.Г. «Интеграция сканеров уязвимостей в системы мониторинга рисков информационной безопасности», Н. Новгород, 2023.

2. Evergreen. «Нейронные сети для вашего бизнеса: какое железо «потянет»?». – Текст: электронный. – URL: https://evergreens.com.ua/ru/articles/neural-networks-hardware.html.

3. Антон Кириллов. «Физическая и логическая топология компьютерной сети (звезда, кольцо, full и partial mesh) и их сравнение. Учимся читать диаграммы Cisco. – Текст: электронный. – URL: https://zametkinapolyah.ru/kompyuternye-seti/topologii-kompyuternoj-seti.html#1113.

4. ITT Solutions. Особенности применения управляемых и неуправляемых коммутаторов. – Текст: электронный. – URL: https://habr.com/ru/companies/zyxel/articles/525178/.

5. Positive Technologies. MaxPatrol SIEM. – Текст электронный: – URL: https://www.ptsecurity.com/ru-ru/about/news/maxpatrol-siem-teper-obrabatyvaet-do-60-000-sobytij-v-sekundu/.

УДК 004.056

В.В. БАРАНОВ, А.П. КОРЧАГИНА, И.Н. ЦЫГУЛЕВ
Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова, Новочеркасск

ПРОАКТИВНЫЕ МЕТОДЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ЭЛЕМЕНТОВ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ЦИФРОВЫХ КАРТ БЕЗОПАСНОСТИ

В работе проведено обоснование актуальности разработки моделей и методов оценки защищенности элементов распределенных информационных систем (РИС) на основе цифровых карт безопасности (ЦКБ). Разработаны ЦКБ элементов РИС, имеющих графическую часть и информационно-расчетную, связанную с международными базами данных уязвимостей и ошибок. Разработана методика определения предпочтительности сценариев ККА и степени их критичности.

Введение

Проактивность в области управления ИБ заключается в раскрытии и упреждении замысла нарушителей, опережении его действий по реализации угроз безопасности информации (УБИ). Научная ценность исследования заключается в том, что представленные модели, алгоритмы и методики являются универсальным инструментом, применимым для оценки защищенности РИС со структурой любой сложности.

Методы исследования

Проведен анализ общедоступных баз данных, включающих описание и классификацию общих шаблонов атак CAPEC ™ [1]. Среди общих механизмов проведения атак выделено 9 групп. Каждый шаблон атаки содержит информацию о том, как выполняются определенные этапы атаки, и содержит рекомендации по способам их локализации.

Базы данных CVE, CWE отражают полный перечень известных уязвимостей и ошибок в программном и аппаратном обеспечении [3, 4]. Система оценки уровня опасности последствий реализации уязвимостей CVSS позволяет определить их категории – высокий, средний и низкий и численные значения такой оценки.

Применение простых компьютерных атак (ПКА) не всегда достигает цели, поэтому применяются различные последовательности, объединённые единым замыслом по достижению цели. Они представляют

собой шаблон комплексной компьютерной атаки (ККА). В ее структуре выделены три этапа: подготовительный, основной и завершающий.

Составлены онтологические структурно-функциональные модели (ОС-ФМ) комплектующих элементов РИС на уровнях базовой эталонной модели взаимодействия открытых систем (ЭМВОС), представленные как объекты деструктивного воздействия (ДВ).

Для определения параметров ДВ применяется их вероятностная оценка методом нейро-байесовских сетей (НБМ) [5, 6]. Для обучения НБМ необходима база данных оценки предпочтительности альтернативных сценариев событий ИБ. Для этого в работе был использован метод многокритериальной оценки (MCDM) PROMETHE-SAPEVO-M1.

Рассмотренные методы будут применены для построения ЦКБ РИС и их элементов. Под ЦКБ в работе понимается ОС-ФМ элемента структуры РИС, отражающая комплектующие его узлов на уровнях ЭМВОС, реализуемые ими функциональные процессы, типы ДВ на них и сопряженная с ней информационно-расчетная система, позволяющая определить предпочтительные сценарии реализации УБИ. Данные ЦКБ будут выступать средством проактивного моделирования сценариев реализации УБИ для конкретных исходных данных.

Заключение

Модели и методы оценки защищенности элементов РИС могут быть использованы для проактивного управления событиями ИБ, существенно снижая время составления модели и обеспечивает высокие показатели достоверности принятых решений при оценке защищенности РИС.

Список литературы

1. CAPEC (Common Attack Pattern Enumeration and Classification) – стандарт описания классов атак и их иерархических отношений. https://capec.mitre.org

2. MITRE ATT&CK Matrix – формальное описание техник и тактик реализации кибератак. https://attack.mitre.org. (дата обращения: 12.01.2023).

3. Перечисление общих недостатков (CWE). [Электронный ресурс]. URL: https://cwe.mitre.org/data/definitions/1194.html. (дата обращения: 12.01.2023).

4. Распространенные уязвимости и риски (CVE). [Электронный ресурс]. URL: https://cve.mitre.org// (дата обращения: 12.01.2023).

5. Cognitive model for assessing the security of information systems for various purposes Baranov V.V., Shelupanov A.A. Symmetry. 2022. Т. 14. № 12. С. 2631.

6. Методика и алгоритмы расчета защищенности элементов распределенных информационных систем в условиях деструктивного воздействия / Баранов В.В., Шелупанов А.А. Доклады Томского государственного университета систем управления и радиоэлектроники. 2022. Т. 25. № 4. С. 88–100.

УДК 004.056

В.Е. МОРОЗОВ
ООО «Либрасофт», Минск

БЛОКИРОВКИ В DLP-СИСТЕМАХ: PRO ET CONTRA

Анализируется проблема использования блокировки информации в DLP-системах, обсуждаются достоинства и недостатки режимов работы данных систем с блокировкой и без, рассматриваются пути снижения временных затрат и ресурсоемкости блокировок, дается классификация блокировок, описываются некоторые подходы к реализации блокировок на примере программного комплекса «КИБ СёрчИнформ».

Идея блокировки трафика, выходящего за пределы защищаемого периметра и нарушающего заданные политики безопасности, далеко не нова. В соответствии с изначальной концепцией DLP весь исходящий поток информации в организации должен обязательно проходить через установленную «в разрыв» DLP-систему, автоматически проверяющую трафик на предмет возможного наличия нарушений. Недостатк данного подхода – то, что блокировка информации на условной границе между организацией и внешним миром помогает бороться лишь с последствиями нарушений, но не защищает от инсайдерских атак, и способствует демаскировке системы. Его плюс – то, что блокировка позволяет «физически» предотвратить утечку (пусть и не во всех случаях). Следствием подобной двойственности является тот факт, что современные комплексные DLP-системы реализуют два возможных режима работы: а) с использованием блокировки, б) без блокировки. В последнем случае акцент делается на мониторинге информационных потоков и проактивном характере мер по недопущению утечек [1].

Традиционный взгляд на работу DLP-системы предполагает, что сначала данные надо перехватить при помощи агента либо на уровне шлюза, затем осуществить парсинг (извлечь текст и атрибуты), отправить данные на хранение в базу данных, после чего их проиндексировать. Индексатор создаст удобную структуру для текстового поиска (индекс), по которому проведёт проверку соответствующий программный модуль. По результатам проверки принимается решение о блокировке. Блокировка возможна на разных уровнях: на конечной точке, при передаче информации по сети либо при использовании интеграции, например, с почтовым сервером. Наибольшая гибкость обеспечивается при использовании агентского перехвата.

В общем случае блокировки целесообразно разделять на контентные (по содержимому сообщения) и контекстные (по атрибутам сообщения). Первые отличается высоким временем срабатывания, ресурсоёмкостью, но в то же

время гибкостью в настройках правил, вторые – быстротой срабатывания, нетребовательностью к ресурсам и отсутствием указанной гибкости.

Существующие пути снижения упомянутых ресурсных издержек заключаются либо в переносе функционала сервера на клиентскую машину (при этом максимизируются требования к ресурсам пользовательского ПК), либо в отказе от проверки по содержимому и осуществлении проверки только по атрибутам (низкая ресурсоемкость и простота реализации). Компромисс – наделение агента функционалом индексатора, который позволяет проводить индексациютолько для некоторых, наиболее важных каналов. Урезание аналитических возможностей позволяет уменьшить ресурсоемкость: становится возможным реализовывать мгновенную блокировку по контенту, и при этом не требуется большого количества ресурсов пользовательского ПК.

В качестве примера рассмотрена конкретная реализация блокировок в программном комплексе «КИБ СёрчИнформ». В соответствии с описанным выше подходом в агент встроен miniSearchServer, который позволяет проводить индексацию. В консоли EndpointController возможна настройка правил контроля использования файлов пользователями/компьютерами/ приложениями. Настройки правил позволяют обнаружить файл по значениям его атрибутов, по содержимому файла, по метке, присваиваемой модулем FileAuditor просканированным файлам. Имеются 4 группы настроек, которые обеспечивают возможность добавление правила доступа к файлам соответствующего типа: файлы по классификации (FileAuditor), мессенджеры (DLP), печать по контенту (DLP), сайты по контенту (DLP). Также доступна блокировка сетевого трафика HTTP(S) на основании передаваемого текста, выбранных пользователей, хостов, URI, POST, GET и других атрибутов, что позволяет реализовать безопасные схемы работы с веб-почтой, чатами, форумами, облачными хранилищами.

Если в приоритете быстрое реагирование на инциденты, подойдет режим работы с блокировками — главное предотвратить утечку, обстоятельства не важны [2]. С другой стороны, если мы не хотим нарушать бизнес-процесс и при этом стремимся обнаруживать нарушения на раннем этапе, лучшим выбором будет комбинация блокировок и мониторинга.

Список литературы

1. Данкевич, А. Включайте голову, прежде чем включать блокировку в DLP / А. Данкевич. – Текст: электронный // InformationSecurity / Anti-Malware : [сайт]. – 2017. – URL: https://www.anti-malware.ru/practice/solutions/lock-dlp (дата обращения: 12.09.23).

2. Минасян, Г. Наблюдать нельзя блокировать. А как вообще использовать DLP? / Г. Минасян. – Текст: электронный // InformationSecurity / itWeek [сайт]. – 2020. – URL: https://www.itweek.ru/security/article/detail.php?ID=211478 (дата обращения: 12.09.23).

УДК 004.056

Д.Н. СТОДЕЛОВ, Н.Г. МИЛОСЛАВСКАЯ
Национальный исследовательский ядерный университет «МИФИ», Москва

ВОПРОСЫ ПОИСКА ИНФОРМАЦИИ ОБ ОРГАНИЗАЦИЯХ ПО ОТКРЫТЫМ ИСТОЧНИКАМ

Рассматриваются вопросы поиска новых подходов к обеспечения информационной безопасности (ИБ) функционирования организаций в условиях цифровой трансформации, способных минимизировать угрозы несанкционированного доступа (НСД) к ресурсам организации, представляющим коммерческую тайну.

Стремительное развитие цифровых технологий ставит перед организациями новые задачи обеспечения ИБ (ОИБ). Сегодня бизнес тесно связан с современными технологиями, но, используя их возможности, он одновременно подвергается угрозе НСД к ресурсам, составляющим коммерческую тайну, что может нанести им значительный финансовый и репутационный ущерб. Таким образом, актуальной задачей является разработка принципиально новых, научно-обоснованных подходов к решению задач безопасной работы в цифровой среде.

Современные информационные системы отличаются сложностью, разнообразием и непостоянством, ввиду чего на этапе разработки обеспечения их ИБ практически невозможно учесть все уязвимости [1]. Общепринятым подходом в настоящий момент и в сложившейся обстановке является принцип отслеживания поведения злоумышленников, систематизация шаблонов их поведения и выбор на основе накопленных данных предупреждающих мер по предотвращению компьютерных атак.

Одним из эффективных подходов является разработка комплекса мер ОИБ на основе матрицы MITRE ATT&CK [2]. Предложенная в 2013 г. по сути глобальная база знаний дает сведения о средствах и методиках, наиболее частно используемых злоумышленниками для получения НСД к данным, представляющим коммерческую тайну организации. В ней представлена совокупность тактик и техник для информационных систем организации (Enterprise), промышленных систем управления (Industrial Control Systems, ICS) и мобильных устройств (Mobile) [3]. Началом является «рекогносцировка» (reconnaissance) – процесс поиска «чувствительных данных» об организации по открытым источникам. Это email-адреса сотрудников организации, DNS-имена и IP-адреса, домены и

субдомены, факты компрометации почтовых адресов, открытые порты и сервисы на них, публичные эксплойты для найденных сервисов, коммерческие документы, имеющихся в свободном доступе, реализованные меры ОИБ и т.п. [4].

С одной стороны, становится очевидным необходимость системного анализа тех угроз, которые могут возникнуть на этапе рекогносцировки, а с другой – актуальность разработки научно-обоснованных подходов к оценке готовности организаций противостоять подобным угрозам. Требуется разработка методик, позволяющих оценить общую степень защищенности организации с позиций используемых технологий (от вида базы данных до архитектуры в целом). Важен и поиск шаблонов поведения злоумышленников на этапе рекогносцировки с использованием модходов искусственного интеллекта (технологий «больших данных» (Big Data), машинного обучения (ML), нейросетей (DL)) [5] с последующей разработкой соответствующих программных продуктов, направленных на повышение защищенности организаций от киберугроз.

Разработка новых методов борьбы с НСД к ресурсам организации, базирующихся на анализе степени защищенности за счет «чувствительной информации», находящейся в открытом доступе, – не только актуальна, но и стратегически важна. При отсутствии реальных возможностей полностью скрыть «цифровой след» бизнес-структур необходимы научно-обоснованные методики и программные продукты, способные минимизировать возможные угрозы, который он генерирует.

Список литературы

1. Кондаков С.Е., Рудь И.С. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы кибербезопасности. 2021. № 5 (45), с. 12–18.

2. Веревкин С.А., Федорченко Е.В. Сравнительный анализ баз данных MITRE ATT&CK и CAPEC // Известия ТулГУ. Технические науки. 2023. № 4, с. 29–39.

3. Борисов В.И., Федорченко Е.В. Метод нормализации полей внешних источников репозитория данных о кибератаках MITRE CTI // ИВД. 2023. № 6 (102).

4. Miloslavskaya N. et al. Security Architecture of Network Security Centers as Part of Modern Intranets //Procedia Computer Science. 2022. Т. 213. С. 58–63.

5. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность // International Journal of Open Information Technologies. 2022. № 9, с. 135–146.

УДК 004.056.5

А.М. РУСАКОВ

МИРЭА – Российский технологический университет, Москва

ОЦЕНКА РИСКОВ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ ИНФРАСТРУКТУРНОГО ГЕНЕЗА НА ОСНОВЕ СПЕКТРАЛЬНОЙ ТЕОРИИ ГРАФОВ

В научной работе предлагается один из возможных подходов для оценки рисков деструктивных воздействий инфраструктурного генеза на основе спектральной теории графов. Экспериментальным путем было показана зависимость спектра графа информационной структуры и рисков информационного деструктивизма. Показано, что применение спектральной теории графов к анализу информационных инфраструктур позволяет повысить информационную безопасность информационных инфраструктур на стадии их проектирования за счет прогнозирования риска от эффекта инфраструктурного деструктивизма.

В последние десятилетия роль информационной инфраструктуры в обеспечении устойчивого развития различных отраслей цифровой экономики стала неоспоримой. Однако недостаточное внимание к оценке рисков деструктивных воздействий на информационные инфраструктуры приводит к серьезным последствиям, которые могут негативно повлиять на функционирование и развитие социально-экономических систем. Однако с ростом значимости информационной инфраструктуры возрастает и угроза деструктивных воздействий на нее.

Под инфраструктурным деструктивизмом в данном случае будем понимать накопление различных эффектов деструктивных воздействий (кибератак, вирусов и т.д.) которое приводит к невозможности функционирования информационной инфраструктуры в штатном режиме. Различные решения данной задачи уже имеются в исследовании [1, 2].

В данной работе предлагается использовать специальную спектральную теорию графов для анализа структурной сложности информационной инфраструктуры с целью определения ее энергетической составляющей [3, 4].

Спектральная теория графов позволяет судить о свойствах графа по свойствам матриц, связанных с ним (смежности, лапласиана, инцидентности) [5]. Коспектральные графы не обязательно должны быть изоморфными, но изоморфные графы всегда коспектральны. Графы, как правило, определяются своим спектром. Граф называется определяемым

его спектром, если любой другой график с таким же спектром поскольку изоморфен.

Далее используя дополнительную авторскую методику оценки рисков инфраструктурного деструктивизма, было показано что спектр графа является решающим фактором для классификации информационных инфраструктур с позиции деструктивных воздействий инфраструктурного генеза. Применяя данный подход, стало возможным оценить схожесть графов информационных инфраструктур и тем самым выделять различные категории рисков инфраструктурного деструктивизма.

Выводы

В результате проведенного исследования можно сделать вывод о том, что при работе с информационными инфраструктурами важно учитывать не только их структуру (так как изоспектральные графы необязательно изоморфны), но и требуется дополнительное исследование, как влияет спектральная природа информационной инфрастуктуры на ее отказоустойчивость по многим критериям, в том числе и в сфере информационной безопасности. Применение спектральной теории графов к анализу информационных инфраструктур позволяет повысить информационную безопасность информационных инфраструктур на стадии их проектирования за счет прогнозирования эффекта инфраструктурного деструктивизма.

Список литературы

1. Максимова Е.А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры / Е.А. Максимова // 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. Максимова Е. А. Оценка инфраструктурных рисков деструктивного характера на субъекте критической информационной инфраструктуры / Е.А. Максимова, В.В. Баранов, Н.П. Садовникова // Системный синтез и прикладная синергетика: сборник научных работ X Всероссийской научной конференции, пос. Нижний Архыз, 28 сентября – 02 2021 года. – Ростов-на-Дону, Таганрог: Южный федеральный университет, 2021. – С. 164–169. – DOI: http://dx.doi.org/10.18522/syssyn-2021-29.

3. Русаков А.М. Исследование структурных свойств информационных систем на основе спектральной теории графов / А.М. Русаков, Н.А. Юшкова // Наукосфера. – 2023. – № 6-1. – С. 192–199. – DOI: http://dx.doi.org/10.5281/zenodo.8055586.

4. Козлов С. В. Интерпретация инвариантов теории графов в контексте применения соответствия Галуа при создании и сопровождении информационных систем // International Journal of Open Information Technologies. 2016. Т. 4. №. 7. С. 38–-44.

5. Qiu L., Ji Y., Wang W. On a theorem of Godsil and McKay concerning the construction of cospectral graphs // Linear Algebra and its Applications. 2020. Т. 603. С. 265–274.

УДК 004.056

М.П. КАРПЕНКО, А.Ю. СИМАЧЕВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА В SIEM- И SOAR-СИСТЕМАХ ДЛЯ ПОВЫШЕНИЯ ИХ РЕЗУЛЬТАТИВНОСТИ В УПРАВЛЕНИИ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исследована возможность применения искусственного интеллекта (ИИ) в SIEM-системах и SOAR-системах в целях повышения их результативности в управлении инцидентами информационной безопасности (УИИБ). Проанализированы актуальные области применения ИИ в рамках SIEM и SOAR.

Исследуется применимость ИИ в системах управления информационной безопасностью (SIEM) и автоматизации реакции на инциденты (SOAR) для повышения результативности систем SIEM и SOAR в решении задач обеспечения информационной безопасности (ИБ).

Новизна проведенного исследования заключается в интеграции различных подходов использования ИИ на всех этапах управления инцидентами ИБ.

Цель исследования состоит в определении применимости ИИ для создания типологии инцидентов ИБ, создания правил сработки систем обнаружения инцидентов ИБ и их автоматического преобразования в формализованное описание. Такие системы способны обрабатывать данные и выполнять задачи значительно быстрее, чем любой человек, что позволяет повысить общую производительность и безопасность труда. В частности, в области ИБ технологии ИИ предоставляют возможность создавать решения существенно более высокой эффективности [1].

В данном исследовании проведен анализ возможности использования ИИ с целью генерации потенциальных сценариев инцидентов ИБ. Далее планируется разработать алгоритмы и модели, способные анализировать агрегированные данные в системе SIEM, SOAR и на основе этого анализа предсказывать возможные угрозы ИБ. Применение ИИ в SIEM-системах позволяет достигнуть очень высокого уровня автоматизации. В отличие от SIEM, ИИ в SOAR помогает не только проводить анализ угрозы информационной безопасности, но и автоматически реагировать на них надлежащим образом.

Важной частью анализа данных является определение наиболее эффективные стратегий реагирования на инциденты, основанных на

информации о состоянии SOAR и SIEM систем. Также определена ключевая роль специалистов по ИБ и ИИ в совместной разработке правил и стратегий реагирования.

В исследовании определена и обоснована необходимость внедрения различных ИИ на разных этапах обработки инцидентов ИБ [2], что подчеркивает важность совместного взаимодействия человеческого и искусственного интеллекта в этой области.

В настоящее время количество атак продолжает расти, а ландшафт угроз меняется с молниеносной скоростью, поэтому особое внимание уделено интеграции ИИ в системы управления инцидентами информационной безопасности (SIEM) и автоматизации управления инцидентами (SOAR) с целью повышения эффективности их работы, основанной на автоматизации процессов обнаружения и управления инцидентами ИБ, снижению времени реагирования на инциденты. Дает возможность сотруднику ИБ рассматривать угрозы, исключая ошибки второго рода (ложная сработка), что снижает нагрузку на системы и персонал [3].

Результатами применения ИИ для формулировки и разработки правил и стратегий реагирования на инциденты ИБ, стало снижение времени реагирования на инциденты, повышение эффективности в расследовании ИБ-инцидентов, обнаружение угроз, уменьшение ложных сработок рассматриваемых специалистом. Исходя из данных о текущем состоянии системы, ИИ смог предположить о новых возможных угрозах.

Список литературы

1. Артамонов В.А., Артамонова Е.В. Искусственный интеллект в системах безопасности // Защита информации. Инсайд. – 2022. – № 5. – С. 2–11.

2. ИИ в ИБ // хакер.ru [Электронный ресурс]. – URL: https://xakep.ru/2021/07/21/nn-in-ib/

3. MaxPatrol O2 // ptsecurity.com [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/products/mp-o2/#how-the-meta-product-works

Направление

Промышленная кибербезопасность

Руководитель секции – Дураковский А.П., к.т.н., доцент,
директор аттестационно–испытательного центра НИЯУ МИФИ

УДК 681.3.06 (075.32)

А.И. КОСТОГРЫЗОВ

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

ОБОСНОВАНИЕ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ В СИСТЕМНЫХ ПРОЦЕССАХ НА ОСНОВЕ ВЕРОЯТНОСТНОГО ПРОГНОЗИРОВАНИЯ РИСКОВ

Целью настоящей работы является аналитический обзор авторских риск-ориентированных методов и моделей, доведенных до реализации в стандартах системной инженерии, для решения прикладных задач обоснования противодействия угрозам применительно к системам различного назначения. Указаны основные решаемые задачи для прогнозирования рисков и обоснования эффективных предупреждающих мер по снижению этих рисков или их удержанию в допустимых пределах.

Система определена как комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей (согласно ISO/IEC/IEEE 15288 и его российскому аналогу – национальному стандарту ГОСТ Р 57193 «Системная и программная инженерия. Процессы жизненного цикла систем»). Под риском понимается сочетание вероятности нанесения ущерба и тяжести этого ущерба (по ГОСТ Р 51898).

Применение вероятностных методов и моделей позволяет построить функцию распределения (ФР) времени до нарушения качества (безопасности) системы и ее критичных элементов. Ориентируясь на построенную ФР, учитывающей характеристики угроз, функции контроля и восстановления приемлемого качества (безопасности) после нарушений или обнаружения признаков возможных нарушений (например, с помощью моделей [1–5]), возможно извлечение знаний, позволяющих:

– рассчитать реальную зависимость вероятности нарушения качества системы и составных подсистем от характеристик разнородных угроз и предпринимаемых мер противодействия угрозам;

– оценить точность прогнозирования по сравнению с упрощенной экспоненциальной аппроксимацией ФР, учитывающей лишь частоту нарушений;

– определить период эффективного функционирования, в течение которого нарушений качества не ожидается (по критерию непревышения

допустимых рисков) – для определения упреждающих противодействий угрозам за время, не превосходящее данного периода;

– выделить зоны прогнозных периодов времени, когда возможны нарушения требований допустимого риска – для определения упреждающих противодействий угрозам или обоснованное уточнение риска для этих зон (в т.ч. избегание рисков или смягчение требований из-за неизбежного резкого возрастания рисков в приемлемых пределах).

Предложенные риск-ориентированные методы и модели для решения прикладных задач обоснования противодействия угрозам применительно к системам различного назначения ориентированы на:

– прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы, интерпретация и анализ приемлемости получаемых результатов, включая сравнение с допустимыми рисками;

– определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество и/или безопасность рассматриваемой системы;

– определение и обоснование в жизненном цикле системы упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства качества и/или безопасности рассматриваемой системы при задаваемых ограничениях в задаваемый период прогноза.

Вышеизложенные идеи доведены до реализации на уровне типовых требований системной инженерии (см. ГОСТ Р 59329 – ГОСТ Р 59357, ГОСТ Р 59989 – ГОСТ Р 59994).

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. Акимов В.А., Костогрызов А.И., Махутов Н.А. и др. /Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности. М.: МГОФ «Знание», 2015. – 936 с.

3. 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.

4. Kostogryzov A., Korolev V. (2020) Probability, combinatorics and control. Probabilistic methods for cognitive solving problems of artificial intelligence systems operating in specific conditions of uncertainties. IntechOpen, 2020, pp. 3-34. https://www.intechopen.com/books/probability-combinatorics-and-control

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

УДК 681.3.06 (075.32)

А.А. НИСТРАТОВ

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

ПРОГНОЗИРОВАНИЕ РИСКОВ ПО ЦИФРОВОМУ ДВОЙНИКУ, СОПРОВОЖДАЕМОМУ В ПРОЦЕССЕ ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ ОБЪЕКТА

Сопровождение цифровых двойников промышленных объектов во времени позволяет использовать накапливаемые исходные данные. Цель работы заключается в выработке методического подхода к вероятностному прогнозированию рисков для упреждающего противодействия разнородным угрозам, в т.ч. угрозам кибербезопасности. Предложены вероятностные модели, методы их применения и интерпретации получаемых результатов прогнозирования рисков на примере сопровождаемого цифрового двойника фрагментов магистральной трубопроводной сети.

Сопровождение цифрового двойника заключается в актуализации данных реального состояния эксплуатируемого объекта с целью прогнозирования рисков и упреждающего противодействия угрозам, в т.ч. угрозам кибербезопасности.

В настоящей работе применяются вероятностные модели [1–5] и методы на конкретном примере сопровождаемого цифрового двойника фрагментов магистральной трубопроводной сети. В приложении к фрагменту магистральной трубопроводной сети цифровой двойник описывает: характеристики фрагмента трубы (диаметр, толщину, проектное давление, покрытие, внутритрубное устройство и др.), проектную и рабочую документацию на строительство трубопроводной сети с привязкой ко времени, характеристики среды эксплуатации (месторасположение, характеристики местности, например – болото, переходы через водные преграды, автомобильные и железнодорожные пути и др.). Т.е. цифровые двойники фрагментов магистральных трубопроводных сетей, по сути, сами представляют собой распределенные компьютерные системы, подлежащие прагматичному использованию в интересах бизнеса.

Необходимыми исходными данными для прогнозирования рисков являются: логическая структура для анализа (выделяются критичные фрагменты); по каждому составному фрагменту (в общем случае): частота возникновения угроз; среднее время развития угроз; период между

диагностиками; длительность диагностики; среднее время восстановления целостности.

Допустимый уровень риска согласно требованиям ГОСТ Р 55999-2014, ГОСТ Р 59991-2022 полагается не выше 0.1, что соответствует вероятности успешного функционирования трубопроводной сети не ниже 0.9. По результатам прогнозирования рисков на уровне зависимости функции распределения времени нарушения целостности сопровождаемого цифрового двойника фрагментов магистральной трубопроводной сети разработаны рекомендации по обоснованию осуществления необходимых периодов внутритрубого, в т.ч. в условиях коррозионной агрессивности грунтов.

Эти рекомендации служат дополнением к техническим мерам, востребуемым по итогам регулярного внутритрубного диагностирования реальных сетей.

Предложенные в работе вероятностные модели, методы их применения и интерпретации получаемых результатов прогнозирования рисков в приложении к сопровождаемым цифровым двойникам обладают аналитической новизной. Их применение обеспечивает прослеживаемость прогнозных рисков от влияющих факторов. Это предоставляет возможности для системного дополнения технических мер, востребуемых по итогам регулярного диагностирования объекта, и способствует повышению безопасности его эксплуатации.

Список литературы

1. Kostogryzov A., Nistratov G., Nistratov A. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management. Total Quality Management and Six Sigma, InTech, 2012, pp. 127–196, http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management

2. Vsevolod Kershenbaum, Leonid Grigoriev, Petr Kanygin and Andrey Nistratov / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, pp. 55–79. http://dx.doi.org/10.5772/intechopen.74963

3. Kostogryzov A., Nistratov A., Nistratov G. Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, 2020, vol 1201. Springer, pp. 352–364. https://www.springer.com/gp/book/9783030468941

4. Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In "Safety and Reliability of Systems and Processes", Gdynia Maritime University, 2020. pp. 153–174. DOI: 10.26408/srsp-2020.

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.

УДК 004.056

В.Г. ИВАНЕНКО[1], Н.Д. ИВАНОВА[2]

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

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

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП

Цель исследования: формирование предложений к алгоритму анализа рисков информационной безопасности (ИБ) АСУ ТП. На основании национальных и международных нормативно-методических документов и практики обеспечения информационной безопасности в статье определен перечень факторов и характеристик рисков ИБ АСУ ТП, что позволяет проводить анализ рисков на основании результатов уже проведенного анализа безопасности АСУ ТП. В результате разработан алгоритм анализа рисков ИБ АСУ ТП, ориентированный на объекты защиты и их уязвимости.

При формировании подхода к анализу рисков информационной безопасности (ИБ) автоматизированных систем управления технологическим процессом (АСУ ТП) важно учесть, что обеспечение ИБ АСУ ТП должно быть ориентировано на защиту функциональных компонентов, выполняемых ими функций, а также на защиту самого технологического объекта управления.

На основе анализа определений государственных и международных стандартов можно выделить два основных фактора риска: величина тяжести последствий от наступления опасного события и вероятность его наступления. В свою очередь, фактор вероятности наступления нежелательного события может быть характеризован по параметрам уязвимостей системы и ее компонентов и потенциала нарушителя.

Тяжесть последствий от успешной реализации угрозы ИБ на АСУ ТП может характеризоваться классом защищенности АСУ, в соответствии с приказом ФСТЭК России № 31 [1] определяемого степенью возможного ущерба от нарушения целостности, доступности, конфиденциальности информации, обрабатываемой в АСУ ТП. Также для АСУ ТП, являющихся объектами критической информационной инфраструктуры, тяжесть последствий от успешной реализации угрозы ИБ может характеризоваться с помощью показателей критериев значимости объектов КИИ РФ.

Уязвимости АСУ ТП могут характеризоваться метриками из стандарта Common Vulnerability Scoring System (CVSS) [2], являющимся открытым стандартом оценки уязвимостей.

Для определения характеристик потенциала нарушителя может быть использован стандарт ГОСТ Р ИСО/МЭК 18045-2013 [3], который предлагает методику определения потенциала нападения нарушителя, ориентированную на имеющиеся в системе уязвимости, что согласуется с определенным ранее подходом.

В общем случае предлагаемый алгоритм анализа рисков АСУ ТП включает следующую последовательность действий. После проведенной идентификации рисков оценка последствий от реализации угроз ИБ производится на основании ранее проведенного категорирования уязвимых объектов защиты. В рамках анализа ущерб из-за отказов компонентов определяется тяжестью ущерба отказа соответствующей системы согласно положениям Постановлением Правительства № 127 [4] в части категорирования объектов КИИ, заключающимся в присвоении определенной категории значимости объектам по результатам анализа «сверху-вниз». Для каждого компонента АСУ ТП на основании ранее проведенной идентификации рисков ИБ АСУ ТП формируется перечень уязвимостей и проводится их анализ на основании метрик стандарта CVSS [2]. Далее для каждой уязвимости оцениваются необходимые возможности нарушителя для ее успешной эксплуатации в соответствии со стандартом ГОСТ Р ИСО/МЭК 18045-2013 [3]. В результате проведенного анализа рисков ИБ АСУ ТП КИИ формируется сопоставление объектов защиты, уязвимостей и возможностей нарушителей, а также определяются их характеристики.

Предлагаемый подход к анализу рисков ориентирован на объекты защиты и их уязвимости, что позволяет реализовать детальный анализ рисков в условиях неопределенности видов возможных нарушителей и их мотивов.

Список литературы

1. Приказ ФСТЭК от 14.03.2014. № 31. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14- marta-2014-g-n-31 (дата обращения: 14.09.2023).

2. Common Vulnerability Scoring System version 3.1: Specification Document. – URL: https://www.first.org/cvss/specification-document/ (дата обращения: 14.09.2023).

3. ГОСТ Р ИСО/МЭК 18045-2013. – Введ. 28.08.2013. – URL: https://gostexpert.ru/data/files/18045-2013/65454.pdf (дата обращения: 14.09.2023).

4. Постановление Правительства Российской Федерации от 08.02.2018 № 127. – URL: http://publication.pravo.gov.ru/Document/View/0001201802130006 (дата обращения: 14.09.2023).

УДК 004.056

А.Н. ВАВИЧКИН, А.П. ДУРАКОВСКИЙ, Е.А. СИМАХИН
Национальный исследовательский ядерный университет «МИФИ», Москва

ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ И ВИБРАЦИОННЫМ КАНАЛАМ

Помещения, предназначенные для ведения конфиденциальных переговоров, содержащих сведения ограниченного доступа, подвергаются аттестационным испытаниям по требованиям безопасности информации. В докладе рассматриваются подходы к оценке защищенности речевой информации от утечки по акустическим и вибрационным каналам в соответствии новыми требованиями ФСТЭК России.

Работы по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, регламентируются приказом ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» и другими нормативными документами ФСТЭК России [1].

Наибольшую опасность непосредственного прослушивания речевой конфиденциальной информации, циркулирующей в помещениях для переговоров, представляют акустические и виброакустические каналы (воздуховоды, окна, трубопроводы, ограждающие конструкции).

Большинство коммерческих (и не только) компаний арендуют помещения в бизнес-центрах, где границей контролируемой зоны являются ограждающие конструкции помещения переговорной комнаты (защищаемое помещение), за которыми могут находиться конкуренты-злоумышленники. В данном случае невозможно обеспечить защиту речевой информации от прослушивания только пассивными методами, и требуется средства активной защиты помещений от утечки речевой информации. Для системы акустического и вибрационного зашумления применяют генераторы белого или розового шума в комплекте с набором акустических, электромагнитных и/или пьезоэлектрических вибропреобразователей [2].

Основной проблемой, от которой зависит эффективность защиты речевой информации, является выбор мест установки этих датчиков

(рис.1) [3], регулировка генератора по частотному диапазону, соответствующему ширине спектра речевого сигнала, по уровню шумов.

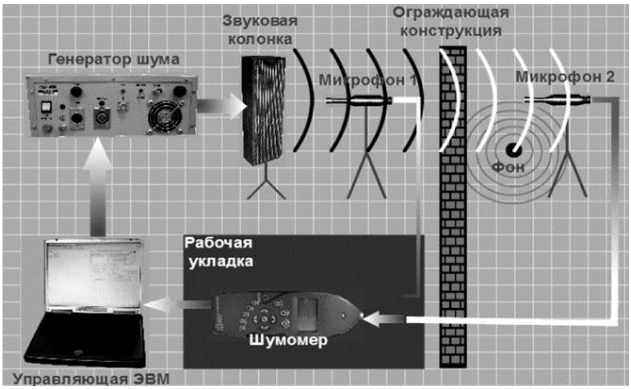

Рис. 1. Схема измерения уровня сигнала и фона в контрольной точке с использованием системы «Шёпот» [3]

Необходимо учитывать, что паразитные акустические шумы вносят дискомфорт, нарушают ведение нормальных переговоров в защищаемом помещении, и часто руководители просто отключают генераторы шума.

Не надо стремиться установить максимальное зашумление [4], минимальную защиту речевой информации можно обеспечить, когда уровень помехи приблизительно в три раза превышает уровень сигнала во всем частотном диапазоне или соотношение сигнал/помеха составляет минус 10 дБ. И этот результат должен повториться при многократных измерениях в контрольной точке.

Список литературы

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

2. Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации. Учебное пособие. – М.: НИЯУ МИФИ, 2015. – 152 с.

3. Бурлаков М.Е. Осипов М.Н. Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум: учебное пособие. – Самара: Издательство Самарского университета, 2021 – 96 с.

4. Дворянкин, Сергей В.; Антипенко, Антон О. Применение фазовых характеристик голосовых вокализмов в решении задач защиты речевой информации. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 21-33, апр. 2021. doi: http://dx.doi.org/10.26583/bit.2021.2.02.

УДК 004.057.5, 004.92

Р.С. СМИРНОВ
АО «Россети Цифра», Москва

РИСКИ ИСПОЛЬЗОВАНИЯ ОС LINUX С ВКЛЮЧЕННЫМ МЕХАНИЗМОМ ОБНОВЛЕНИЯ ВСТРОЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (СЕРВИС LINUX VENDOR FIRMWARE SERVICE) НА ПРЕДПРИЯТИЯХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ТЭК

В статье рассматривается проблема использования не верифицированных источников программного обеспечения (ПО) в среде ОС Linux, в частности сервиса LVFS, в схеме работы которого, с помощью разработанного сервиса мониторинга, выявлены потенциальные уязвимости, приведены примеры и представлен сам сервис. Также рассматривается вопрос использования ОС Linux на предприятиях ТЭК и изменение принципиальной схемы обновления ПО для устранения аналогичных проблем.

В 2015 г. одним из разработчиков Gnome, был создан сервис обновления т.н. встроенного программного обеспечения (далее «прошивок») устройств для операционной системы (далее ОС) Linux, который изначально предназначался для использования компанией Dell [1] Со временем сервис Linux Vendor Firmware Service (далее LVFS) набрал популярность [2] и на данный момент включен в большинство самых распространенных дистрибутивов ОС Linux – Ubuntu, Debian, RedHat и других построенных на их базе в т.ч. отечественных таких AstraLinux и Alt Linux ([3–4]), которые соответственно используются на предприятиях ТЭК. В рамках программы импортозамещения закупки дистрибутивов Linux осуществляются крупными компаниями такими как Росатом, Русгидро, СО-ЕЭС, АО СИБЭК и др. (в статье проведен анализ закупок на платформе zakupki.gov.ru).

Автором разработан сервис мониторинга размещаемых в LVFS прошивок и проанализирована его работа за определенный период, в рамках мониторинга было выявлено безвозвратное удаление ранее размещенных файлов и метаданных, также по схеме обновления сделан вывод о потенциальной уязвимости к целевой атаке со стороны владельцев LVFS (или т.н. MitM) с использованием метаданных агента.

Исходный код сервиса мониторинга доступен по адресу http://github.com/SmirnovRoman/FWMonitor [6].

Помимо использования ОС Linux на предприятиях ТЭК на АРМ сотрудников, существует проблема отсутствия единых подходов (стандартов) к обновлению встроенного программного обеспечения и для оборудования (стандарты по электромобилям и «электрозаправкам» IEC 63110-1:2022, освещение IEC 62386-105:2020, общие подходы по безопасности, без детализации – ISO/IEC 27019:2017, для Интернета Вещей – RFC9019).

Предлагается схема с дополнительным уровнем верификации – автоматической, с использования антивирусов, специализированного программного обеспечения и глубоким анализом содержимого пакетов обновления (например, разбор UEFI капсул) или полуавтоматической верификации с привлечением экспертов. Для отслеживания изменений целесообразно включение технологии распределенного реестра [7] на протяжении всего цикла размещения «прошивок», от вендора до конечной системы. В перспективе возможно проведение работ по доработке стандартов при их российской локализации для включения в них предполагаемого функционала дополнительной верификации и повышения прозрачности всего процесса обновления «прошивок».

Список литературы

1. Официальный сайт LVFS - https://fwupd.org/ (дата обращения 22.08.2023).
2. Michael Larabel 31.05.2022 Phoronix Media URL https://www.phoronix.com/news/LVFS-Fwupd-52-Million (дата обращения 22.08.2023).
3. БЮЛЛЕТЕНЬ № 2023-0426SE17 (оперативное обновление 1.7.4) – https://wiki.astralinux.ru/pages/viewpage.action?pageId=263044494 (дата обращения 22.08.2023)
4. Официальный репозиторий ALT Linux, версия c10f1, URL: http://ftp.altlinux.org/pub/distributions/ALTLinux/c10f1/branch/files/x86_64/RPMS/fwupd-1.8.10-alt1.x86_64.rpm (дата обращения 22.08.2023).
5. Michael Larabel 01.12.2021 Phoronix Media URL https://www.phoronix.com/news/LVFS-40-Million-Downloads (дата обращения 22.08.2023).
6. Репозиторий ПО FWMonitor – http://github.com/SmirnovRoman/FWMonitor (дата обращения 22.08.2023).
7. A. Yohan and N. -W. Lo, "An Over-the-Blockchain Firmware Update Framework for IoT Devices," 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 2018, pp. 1–8, doi: 10.1109/DESEC.2018.8625164.

УДК 004.056

С.С. ДОЛЖЕНКОВ, Е.А. МАКСИМОВА
МИРЭА – Российский технологический университет, Москва

ПРИМЕНЕНИЕ ПОДХОДОВ РИСК-МЕНЕДЖМЕНТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРИ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЯХ ИНФРАСТРУКТУРНОГО ГЕНЕЗА

В статье предлагается авторский подход к минимизации рисков в области Информационной безопасности (ИБ) субъектов критической информационной инфраструктуры (КИИ) при деструктивных воздействиях инфраструктурного генеза. Подходы к управлению ИБ субъектов КИИ должны быть основаны на научных принципах и методологиях, что позволит обеспечить максимальный уровень защиты от распространения угроз и минимизировать возможные последствия. Целью данного исследования является исследование технологии риск-менеджмента в контексте управления ИБ КИИ при деструктивных воздействиях инфраструктурного генеза.

Субъекты КИИ подвержены деструктивным воздействиям инфраструктурного генеза, которые способны нанести серьезный ущерб информационной безопасности (ИБ) организации и национальной безопасности в целом [1].

В настоящее время ИБ становится все более важной проблемой для организаций, особенно для тех, чья деятельность попадает под действие ФЗ-187. Субъекты КИИ должны уделять особое внимание рисковым факторам и принимать соответствующие меры для минимизации негативных последствий деструктивных воздействий инфраструктурного генеза [3].

КИИ охватывает важные объекты и системы, которые играют ключевую роль в функционировании государственных структур, экономики и общества в целом. Эти системы могут быть подвержены различным деструктивным воздействиям, таким как кибератаки, технические сбои, естественные и техногенные катастрофы.

Деструктивные воздействия могут включать в себя кибератаки, хакерские атаки, вирусы, вредоносные программы и другие формы атак на информационные активы. Последствия таких атак могут быть разрушительными для субъектов КИИ [1].

Риск-менеджмент включает в себя процессы и методы, которые позволяют организациям определить и оценить риски, разработать стратегии по их управлению и оптимизации [2]. В контексте управления ИБ, риск-менеджмент помогает выявить и снизить возможные угрозы информационным активам, связанным с деструктивными воздействиями и инфраструктурного генеза. Основные принципы методологии риск-менеджмента включают следующие:

Идентификация и классификация рисков: важно определить все возможные риски, связанные с деструктивными воздействиями ~~и~~ инфраструктурного генеза, и классифицировать их по уровню критичности и вероятности возникновения [3].

Анализ рисков: необходимо провести анализ потенциальных угроз ИБ и их последствий для субъектов КИИ. Это позволит определить наиболее критические уязвимости и разработать соответствующие меры защиты.

Оценка рисков**:** осуществление оценки вероятности возникновения рисков и их потенциального воздействия на объекты КИИ. На основе этой оценки можно определить приоритеты в области ИБ.

Методология поддержки процессов управления ИБ является основой для реализации риск-менеджмента. Она включает в себя шаги по идентификации информационных активов, выявлению угроз

Основная цель риск-менеджмента в контексте обеспечения ИБ КИИ – минимизировать риск возникновения проблем и ущерба, связанного с нарушением ИБ. Правильное и эффективное применение риск-менеджмента позволяет руководителям субъектов управлять рисками, связанными с ИБ.

Список литературы

1. Максимова Е.А. Инфраструктурный деструктивизм субъектов критической информационной инфраструктуры. – Москва - Волгоград: Волгоградский государственный университет, 2021. – 181 с. – ISBN 978-5-9669-2147-7. – EDN ZZTOKE.

2. Абрамова Е.Д. Риск-менеджмент, основа управления рисками. Формирование конкурентной среды, конкурентоспособность и стратегическое управление предприятиями, организациями и регионами. : Сборник статей VIII Международной научно-практической конференции, Пенза, 15–16 мая 2023 г. / Под научной редакцией О.А. Лузгиной. – Пенза: Пензенский государственный аграрный университет, 2023. – С. 10-14. – EDN CYBQHX.

3. Максимова, Е.А. Метод оценки инфраструктурной устойчивости субъектов критической информационной инфраструктуры / Е.А. Максимова, М.В. Буйневич // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 1(43). – С. 50-63. – DOI 10.14529/secur220107. – EDN PMNVFF.

УДК 004.051

Д.И. ПРАВИКОВ, В.А. МУРАШКИН
РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва

ОПТИМИЗАЦИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ПРЕДПРИЯТИИ ТЭК

В работе рассматривается вопрос автоматизации процессов управления информационной безопасностью в сфере ТЭК и внедрения систем поддержки принятия решений для новой категории должностных лиц, которая была учреждена Указом Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Основное внимание уделяется необходимости обеспечения эффективного решения задач, направленных на обеспечение информационной безопасности объектов КИИ.

Для организации управления на предприятиях ТЭК процессом управления информационной безопасности необходимо научно-методическое и техническое обеспечение. В работе предлагается процесс управления информационной безопасностью на предприятиях ТЭК, приведенный на рис. 1.

Рис. 1. Объекты управления

Эффективная система мониторинга должна обеспечивать возможность настраивать уведомления в случае возникновения определенных событий, что позволяет оперативно реагировать на потенциальные угрозы. Кроме того, такая система должна предоставлять средства визуализации данных в удобном для анализа формате, например, в виде графиков, таблиц и диаграмм.

При оценке эффективности системы обеспечения информационной безопасности важно учитывать различные метрики, такие как время реакции на события, количество выявленных угроз и рисков, степень автоматизации обработки событий и другие параметры. Эти метрики позволяют оценить эффективность работы системы мониторинга и настроить ее для наиболее эффективной защиты информации.

Выводы

В работе предложено создание системы критериев оценки эффективности обеспечения безопасности автоматизированных систем управления на предприятиях ТЭК.

С теоретической точки зрения, в ряде научных публикаций [1-3], эффективность защиты информации рассматривается как «степень соответствия результатов защиты информации цели защиты».

С точки зрения руководства предприятий ТЭК, основным показателем эффективности системы обеспечения безопасности является минимизация или исключение убытков, связанных с простоями предприятия. Эти простои могут быть вызваны различными факторами, включая угрозы информационной безопасности. Таким образом, эффективное обеспечение безопасности играет важную роль в обеспечении непрерывной работы предприятий ТЭК и защите их активов.

Список литературы

1. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2022. – 166 с. Управление информационной безопасностью. М.: НИЯУ МИФИ, 2020. – 536 с.

2. Карташевский И.В., Байдаков В.С. Управление информационной безопасностью современного предприятия. // Наука, техника и образование. – 2021. – С. 30–32.

3. Лившиц И.И., Лонцих П.А. Формирование метрик для измерения результативности систем менеджмента информационной безопасности. // Вестник ИрГТУ № 5 (112). – 2016.

УДК 004.056

А.П. ДУРАКОВСКИЙ, Е.А. СИМАХИН
Национальный исследовательский ядерный университет «МИФИ», Москва

ОЦЕНКА ВЕРОЯТНОСТИ ПОЯВЛЕНИЯ ОШИБКИ ПРИ ПРОВЕДЕНИИ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В рамках аттестационных испытаний, подтверждающих соответствие объекта информатизации (ОИ) требованиям по защите информации, кроме проверки регламентирующих документов на ОИ, экспертам органа по аттестации необходимо провести комплекс инструментальной оценки эффективности защиты информации от утечки по техническим каналам и от утечки за счет несанкционированного доступа. При оценке защищенности ОИ вероятно наличие непреднамеренных ошибок, обусловленное как вследствие недостаточной квалификации, так и чрезмерной длительностью инструментальных измерений, может привести к ложному заключению о соответствия ОИ требованиям защиты информации.

Оценку вероятности появления ошибки при проведении любой из проверок, проводимых в рамках аттестации ОИ, можно провести, предположив, что эксперт органа по аттестации или испытательной лаборатории, непреднамеренно совершает ошибку и в результате формирует вывод о соответствии системы защиты ОИ требованиям по безопасности информации с результатом «успех» или «отказ». Для определения возможных исходов данной бинарной задачи, применим метод проверки статистических гипотез [1] и примем в качестве нулевой гипотезы «Положительное решение» – H_0, а в качестве альтернативной гипотезы «Отрицательное решение» – H_1. Причем положительное решение принимается в том случае, если система защиты ОИ соответствует требованиям по безопасности информации и сотрудник не заметил ошибку. Отрицательное решение принимается в том случае, если на этапе проведения проверки удалось обнаружить непреднамеренную ошибку, в том числе ее наличие на любом предыдущем этапе работы.

Совершение непреднамеренной ошибки, содержащей не достоверную информацию, приводит к ошибке 2 рода относительно реального уровня защищенности ОИ. Каждый последующий тип работ может выявлять непреднамеренные ошибки предыдущего типа работ.

С учетом наличия группы экспертов при принятии решений, результаты могут быть подвержены определенным предубеждениям, а

также личностным или групповым проблемам и конфликтам, которые могут значительно подорвать эффективность, а также обладать низкой степенью достоверности результатов. Для минимизации этого к экспертам выдвигаются требования [2]:

1) эксперты должны обладать детальными знаниями в области, которую их просят оценить, и иметь не менее десяти лет практики в своей конкретной области или работе;

2) эксперты должны быть знакомы с теорией вероятности, в противном случае они не смогут выразить свой опыт в последовательной количественной форме.

Трудозатраты, которые могут быть потрачены на поиск группы экспертов, соответствующих критериям отбора, объективно превышают время проведения дополнительного оцениваемой деятельности одним экспертом. Сравнение методов оценки надежности человека (метод APJ, метод HEART) [3] показывает, что наиболее подходящим методом является HEART.

Вычисление значения вероятности ошибки человека проводится согласно выражению: $HEP = GEP \prod_{i=1}^{n}(r(i) * (w(i) - 1) + 1)$,

где GEP - номинальная вероятность ошибки,

$r(i)$ – коэффициент важности между сочетаниями условий,

$w(i)$ – весовой коэффициент (вес условия, приводящего к ошибке),

n – количество вариантов условий, приводящих к ошибкам.

В [3] предлагается метод расчёта значения нижней $\underline{GEP}(t_{fact})$ и верхней $\overline{GEP}(t_{fact})$ границ интервала номинальной вероятности GEP в зависимости от фактического времени t_{fact}, в течение которого человек работает в рамках выбранной деятельности, с учетом определения величины интенсивности ошибок человека $\lambda(t)$ за время $t^* < t_{fact}$.

Список литературы

1. Ивановский Р. Теория вероятностей и математическая статистика. Основы, прикладные аспекты с примерами и задачами в среде Mathcad. – 528 с. – URL: https://pdf.11klasov.net/7825-teorija-verojatnostej-i-matematicheskaja-statistika-ivanovskij-ri.html . (дата обращения: 11.09.2023).

2. Кирван Б. A guide to practical human reliability assessment = Руководство по практической оценке надежности персонала // ResearchGate – 2017 – С. 587. DOI:10.1201/9781315136349

3. Ахмеджанов Ф.М., Крымский В.Г. Алгоритм оценки надежности человека-оператора на основе модифицированной методики HEART // Электротехнические и информационные комплексы и системы №1 том 15 – 2019. – С. 60–69. DOI: 10.17122/1999-5458-2019-15-1-60-69

УДК 004.056

Е.А. СИМАХИН, А.П. ДУРАКОВСКИЙ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПРАКТИЧЕСКИЙ СПОСОБ ПРОВЕДЕНИЯ ИССЛЕДОВАНИЙ ПЭМИН ИНТЕРФЕЙСА DISPLAY PORT

Важнейшим этапом анализа побочных электромагнитных излучений и наводок (ПЭМИН) интерфейсов средств вычислительной техники (СВТ) является обнаружение частот информативных сигналов. С развитием технологий передачи информации некоторые широко используемые интерфейсы не имеют однозначного подхода к проведению таких исследований. Авторами предлагается практический способ исследования интерфейса DisplayPort.

Оценка возможности обнаружения частот информативного сигнала при проведении специальных исследований технических средств является одним из важнейших этапов анализа защищенности информации от утечки за счет ПЭМИН [1]. Однако, нет однозначного подхода к проведению таких исследований высокоскоростного интерфейса передачи данных – DisplayPort. В [2] авторами был проведен анализ их практической применимости при проведении исследований ПЭМИН в реальных условиях. Результаты анализа представлены в табл. 1.

Таблица 1. Результаты анализа применимости на практике

Содержание подхода	Результат	Применимость на практике
Анализ EDID	Уточнение характеристик монитора	Да
Выбор режима(ов) работы монитора	Исключение не контролируемой смены количества активных линий	Нет
Определение количества активных линий	Определение тактовой частоты передачи на линию	Нет
Передача данных при работе режима Link Training	Отключение скремблера	Нет
Разработка ПАК на базе ПЛИС		Нет, (стороннее устройство в составе СВТ)
Использование AMD Radeon Software, HDCP-stipper	Отключение HDCP	Нет
Анализ преобразования модуляции SSFM	Отключение SSFM	Нет
Анализ порядка передачи символов	Формирование тестовой последовательности	Да

По результатам проведенного анализа можно сделать вывод, что для анализа ПЭМИН интерфейса DisplayPort в настоящий момент специалистам доступно: провести анализ характеристик жидкокристаллического монитора и анализ порядка передачи данных.

Для доступа к необходимому функционалу разработано дополнительное специальное программное обеспечение (СПО), контролирующее в реальном режиме времени работу интерфейса посредством взаимодействия с драйвером устройства. Исходя из архитектуры интерфейса, данное СПО содержит: модуль изменения необходимых параметров в DPCD; модуль управления питанием; модуль формирования тестовой последовательности; модуль пересылки тестовой последовательности. Фрагмент интерфейса СПО, в части изменения необходимых параметров, формирования и пересылки тестов приведен на рис. 1.

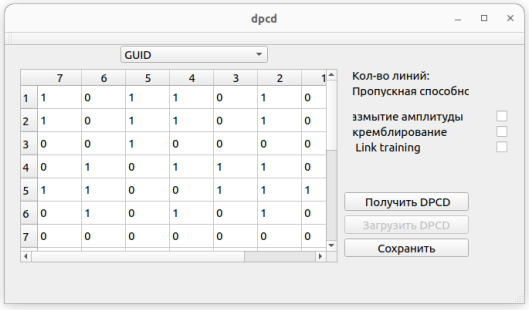

Рис. 1. Внешний вид разработанного СПО

Специалист однозначно может идентифицировать исследуемый интерфейс, определять режим работы интерфейса, анализ характеристик его работы и изменять их параметры в соответствии с требуемым режимом работы, не оказывая влияния на четкость изображения.

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: 11.09.2023).

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.

.

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

ОРТОМОРФНЫЕ ПРЕОБРАЗОВАНИЯ РЕГИСТРОВ СДВИГА НАД ПОЛЕМ $GF(2^m)$

В настоящее время ортоморфизмы используются при синтезе алгоритмов поточного и блочного шифрования. Проблема их построения в общем случае является открытой. В работе получены достаточные условия ортоморфности класса нелинейных преобразований регистров сдвига. Приведены примеры таких преобразований. Получен критерий ортоморфности композиции линейных регистровых преобразований. Показано, что критерию удовлетворяет MDS-матрица алгоритма «Кузнечик».

Преобразования регистров сдвига над конечными полями традиционно используются при синтезе блочных и поточных шифрсистем. В данной работе рассматривается класс биективных регистровых преобразований $\rho_v^{(n)}$ на n-мерном векторном пространстве $V_n(2^m)$ над полем $GF(2^m)$ с функцией обратной связи $v: V_n(2^m) \to GF(2^m)$, заданных условиями

$$\rho_v^{(n)} : (x_1, ..., x_n) \mapsto (x_2, ..., x_n, v(x_1, ..., x_n)) \quad (1)$$

и являющихся ортоморфизмами, т.е. отображение

$$\tilde{\rho}_v^{(n)} : (x_1, ..., x_n) \mapsto (x_2 - x_1, ..., x_n - x_{n-1}, v(x_1, ..., x_n) - x_n)$$

есть подстановка на $V_n(2^m)$. Несложно убедиться, что если отображение v линейно,

$$v(x_1, ..., x_n) = \sum_{i=1}^{n} c_i x_i, \quad c_1, ..., c_n \in GF(2^m),$$

то для ортоморфности достаточно проверить условие $c_1 \neq 0$, $\sum_{i=1}^{n} c_i \neq 1$. Однако, для нелинейных преобразований проблема построения ортоморфизмов остается открытой (например, [1, 2]). В данной работе получено достаточное условие ортоморфности преобразования $\rho_v^{(n)}$.

Утверждение 1. *Пусть* $m, n \in \mathbb{N}$, $m \geq 1$, $n \geq 3$, *преобразования* $v: V_n(2^m) \to GF(2^m)$ *задано условием:*

$$v(x_1, ..., x_n) = c_1 x_1^{d_1} + c_2 x_2^{d_2} + ... + c_n x_n^{d_n},$$

где набор $(c_1,...,c_n) \in V_n(2^m)$ *и числа* $d_1,...,d_n \in \{1,...,2^m-2\}$, $p \in \{1,...,n\}$ *таковы, что:*

$$c_j \neq 0,\ \text{НОД}(d_j, 2^m-1) = 1 \text{ для каждого } j \in \{1,p\},$$

$$\{d_i \mid i \in \{1,...,n\} \setminus \{p\}, c_i \neq 0\} \subseteq \{2^t \mid t \in \{0,...,m-1\}\},$$

а преобразование $\tilde{v} : GF(2^m) \to GF(2^m)$,

$$\tilde{v} : y \mapsto v(y,...,y,y) + y \text{ для каждого } y \in GF(2^m),$$

есть подстановка на $GF(2^m)$. *Тогда* $\rho_v^{(n)}$ *есть ортоморфизм.*

Отметим, что при $m=1$ утверждению 1 удовлетворяют только линейные функции обратной связи, у которых число существенных переменных четно, а x_1 существенна. При $m>1$ приведены примеры функций обратной связи v, при которых $\rho_v^{(n)}$ – ортоморфизм. Выясним, для каких линейных функций обратной связи v и степеней $r \in \mathbb{N}$ преобразование $(\rho_v^{(n)})^r$ есть ортоморфизм.

Утверждение 2. *Пусть* $m, r \in \mathbb{N}$, $n \geq 3$, $v : V_n(2^m) \to GF(2^m)$, $\rho_v^{(n)} : V_n(2^m) \to V_n(2^m)$ *заданы условиями:*

$$v(x_1,...,x_n) = c_1x_1 + c_2x_2 + ... + c_nx_n,$$

где $(c_1,c_2,...,c_n) \in V_n(2^m)$, $c_1 \neq 0$. *Пусть также орграф* $\Gamma(\rho_v^{(n)}) = \left(V_n(2^m), \Lambda_v^{(n)}\right)$ *линейного преобразования* $\rho_v^{(n)}$ *на множестве* $V_n(2^m) \setminus \{0_n\}$ *имеет* s *циклов длин* $l_1,...,l_s$. *Тогда и только тогда* $(\rho_v^{(n)})^r$ *есть ортоморфизм, когда* $r \not\equiv 0 \pmod{l_d}$ *для каждого* $d \in \{1,...,s\}$.

Показано, что утверждению 2 удовлетворяет MDS-матрица линейного слоя алгоритма блочного шифрования «Кузнечик» [3].

Список литературы

1. Johnson D.M., Dulmage A.L., Mendelsohn N.S. Orthomorphisms of groups and orthogonal Latin squares, I. Canad. J. Math. 1961, v.13, p. 356–372.

2. Denes J., Keedwell A.D. Latin squares and their applications. London: English Univ. Press, 1975.

3. Погорелов Б. А., Пудовкина М. А. Обобщенные квази-адамаровы преобразования на конечных группах. Математические вопросы криптографии. т. 13, № 4, с. 97–124, 2022.

4. Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2016.

УДК 004.912

А.А. ВАРФОЛОМЕЕВ

Московский государственный технический университет им. Н.Э. Баумана
Национальный исследовательский ядерный университет «МИФИ», Москва

НЕКОТОРЫЕ ЗАМЕЧАНИЯ К НОВОЙ МАТРИЧНОЙ РЕАЛИЗАЦИИ ТРЕХЭТАПНОГО ПРОТОКОЛА ШАМИРА

Рассматривается новая (2023 год) матричная реализация классического трехэтапного протокола Шамира в части предлагаемой в ней схемы обеспечения аутентификации участников и в части защиты от администратора сети связи конфиденциальности передаваемых сообщений.

Введение

Протокол Шамира [1–4] является классическим протоколом, поэтому представляет интерес еще одна новая его реализация [5] на основе случайных секретных квадратных матриц над конечным полем.

Обсуждение протокола

Известно несколько реализаций: реализация Шамира [1-3], Месси – Омуры [6], Рубина [7] и других. В новой реализации [5], открытый текст представляется квадратной матрицей M размера 24 на 24 над целыми числами в интервале [-20, …, 0, …20].

Подлинность участников в [5] предлагается обеспечить с помощью перестановочных матриц UI (“unequivocal identifier”), которые каждый член сети вырабатывает самостоятельно, но с помощью сетевого администратора (Разделы 3.2, 4.2, 5.3.3, 7.1.4 из [5]). Из описанного в [5] протокола следует, что они должны быть известны всем участникам сети.

С использованием указанных перестановочных матриц и ключевых матриц протокол имеет следующий вид:

1 раунд. Участник A отправляет B: C1 = UIBl*A1*M*A2*UIBr;

2 раунд. Шаг 1. Участник B восстанавливает A1*M*A2 из C1;

Шаг 2. Вычисляет и отправляет C2 = UIAl*B1* A1*M*A2*B2*UIAr;

3 раунд. Шаг 1. Участник A восстанавливает B1*A1*M*A2*B2;

Шаг 2. Вычисляет и отправляет C3 = A1^(-1)* B1*A1*M*A2*B2*A2^(-1) = A1^(-1) * A1*B1*M*B2*A2 *A2^(-1) = B1*M*B2.

Предлагается в качестве шифрующих матриц генерировать матрицы вида: A1 = Cl*FAl*Cl^(-1); B1 = Cl*FBl*Cl^(-1);

A2 = Cr*FAr*Cr^(-1); B2 = Cr*FBr*Cr^(-1).

Здесь матрицы FAl, FAr, FBl, FBr вырабатываются встроенным псевдослучайным алгоритмом для каждого сеанса связи и имеют блочно-диагональный вид с восемью циркулянтными 3x3 матрицами на диагонали. Обратимые матрицы Cl и Cr являются общими для всех участников сети (рекомендуется менять раз в неделю), которые вырабатываются псевдослучайным алгоритмом на основе некоторых начальных условий.

Атака администратора сети на конфиденциальность сообщений

Администратор сети, при известных ему матрицах Cl и Cr, может получить соотношения для нахождения ключевых матриц FAl, FAr, FBl, FBr:

G1 = Cl^(-1)*C1*Cr = FAl*N*FAr; G2 = Cl^(-1)*C2*Cr = FBl*FAl*N*FAr*FBr; G3 = Cl^(-1)*C3*Cr = FBl*N*FBr;

где матрица N = Cl^(-1)*M*Cr.

Откуда получаются соотношения:

G2 = FBl*G1*FBr;

G2 = FBl*FAl*N*FAr*FBr = FA1*FB1*N*FBr*FAr = FAl*G3*FAr.

Вывод

Предложенный в работе [5] метод аутентификации сообщений не обеспечивает подлинности отправителей и получателей этих сообщений.

Предложенный в работе метод построения ключевых матриц не обеспечивает секретность передаваемых сообщений от администратора сети. Атака на протокол в этом случае сводится к решению 576 уравнений от 48 переменных [8].

Список литературы

1. Konheim A. Cryptography. A Primer. John Willey&Sons, Inc., 1981 – 432 с.
2. Schneier B. Applied cryptography Second Edition: protocols, algorithms? And source code in C, John Willey&Sons, Inc., 1996 – 758 с.
3. Шнайер Б. прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002 – 816 с.
4. MasseyJ. An introduction to Cotemporary Cryptology, Proceedings of the IEEE, v. 76, n.5, 1988.
5. Dupont F. A new Shamir's three pass random matrix ciphering mechanism, Journal of Computer Virology and Hacking Techniques, Springer-Verlag France SAS, part of Springer Nature 2023, https://doi.org/10.1007/s11416-023-00467-0.
6. Massey J., Omura J., Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission, Patent: US4567600A, 1982.
7. Рубин Ф. Криптография с секретным ключом. – М.: ДМК Пресс, 2022. – 386 с. (16 глава. Трехпроходный протокол).
8. Johnson C., Stimoc Y., Yang Dian. Solution Theory for Systems of Bilinear Equations. 2013.

УДК 519.7

М.А. ПУДОВКИНА, А.М. СМИРНОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПРИМЕНЕНИЕ ПОДХОДА «ЙО-ЙО» ДЛЯ АТАКИ НА АЛГОРИТМ LILLIPUT-TBC-II-256

В работе обобщается подход «йо-йо» для атаки на произвольное число раундов алгоритма LILLIPUT-TBC-II-256 с ключом длины 256 бит. Для атаки требуется $2^{128} + 2^{16}$ текстов, $30 \cdot 2^{16}$ бит памяти. Трудоемкость атаки равна $31 \cdot (2^{128} + 2^{80})$ операций зашифрования. Вероятность успеха атаки равна 1.

В [1] предложена атака на 5-раундовый алгоритм блочного шифрования AES и описан для него 6-раундовый различитель, основанные на подходе из игры «йо-йо». Идея атаки состоит в использовании свойства XSL-алгоритмов блочного шифрования, включая обобщения SAS и SASAS [2], которое сохраняет нулевую разность между байтами векторов состояния. В данной работе, используя предложенную модификацию подхода «йо-йо», анализируется 32-раундовый алгоритм LILLIPUT-TBC-II-256 с длиной ключа 256 бит, участвующий в конкурсе американского института стандартизации (NIST) на стандарт низкоресурсного алгоритма шифрования США [2].

Пусть $V_{16}(2^8)$ – 16-мерное векторное пространство над полем $\mathbb{F}_{2^{32}}$; $\oplus -$ операция сложения в $V_{16}(2^8)$; $I(A)$ – индикатор выполнения условия A; $g: V_{16}(2^8) \times V_{16}(2^8) \longrightarrow V_{16}(2^8) -$ раундовая функция алгоритма LILLIPUT-TBC-II-256; $k \in V_{16}(2^8)$ – раундовый ключ; h – (0,1)-матрица порядка 16 над полем $\mathbb{F}_{2^8}$ линейного слоя раундовой функции g; s – фиксированная подстановка S-бокса; $\varepsilon_j -$ базисный вектор пространства $V_{16}(2^8)$, $j \in \{0, \dots, 15\}$, у которого j-я координата равна единице, а все остальные координаты нулевые.

Для каждых $\alpha = (\alpha_0, \dots, \alpha_{15}) \in V_{16}(2^8)$ и $k \in V_{16}(2^8)$ раундовая функция g задается условием

$$g(\alpha, k) = hs(\alpha \oplus k).$$

Для отображения $\chi^{(i)}: V_{16}(2^8) \longrightarrow \mathbb{F}_2$,

$$\chi^{(i)}(\alpha) = I(\alpha_i \neq 0), \qquad i = 0, \dots, 15,$$

положим $\chi(\alpha) = \left(\chi^{(0)}(\alpha), \dots, \chi^{(15)}(\alpha)\right)$.

Матрицу h представим в блочно-диагональном виде с (4×4)-подматрицами $h_{i,j}$, $i,j = 0,\dots,3$.

На основании следующих теорем 1, 2 разработана атака на полнораундовый алгоритм LILLIPUT-TBC-II-256, использующая модификацию подхода «йо-йо».

Теорема 1. *Пусть* $\alpha_0, \alpha_1, k_0, \dots, k_{30}$ – *произвольные элементы векторного пространства* $V_{16}(2^8)$, $\beta_i = g_{k_{30}} \dots g_{k_1} g_{k_0}(\alpha_i), i = 0,1$. *Тогда справедливо равенство*

$$\chi((sh)^{-2}(\beta_0) \oplus (sh)^{-2}(\beta_1)) = \chi(g_{k_{28}} \dots g_{k_0}(\alpha_0) \oplus g_{k_{28}} \dots g_{k_0}(\alpha_1)).$$

Теорема 2. *Пусть* $\alpha, k \in V_{16}(2^8)$ *и существуют такие* $i, j_1, j_2 \in \{0, \dots, 15\}$, *что элементы матрицы линейного отображения* h^{-1} *удовлетворяют условиям*

$$(h^{-1})_{i,j_1} = (h^{-1})_{i,j_2}, (h^{-1})_{i,j_1} \neq 0.$$

Тогда для каждого $\omega \in \mathbb{F}_{2^8}$ *существует такое* $\delta \in \mathbb{F}_{2^8}$, *что уравнение*

$$((sh)^{-1}(\alpha \oplus \omega \cdot \varepsilon_{j_2} \oplus k) \oplus (sh)^{-1}(\alpha \oplus \delta \cdot \varepsilon_{j_1} \oplus (\delta \oplus \omega) \cdot \varepsilon_{j_2} \oplus k))_i = 0$$

имеет 2^8 *решений.*

Доказано, что для атаки требуется $2^{128} + 2^{16}$ текстов, $30 \cdot 2^{16}$ бит памяти, а трудоемкость атаки составляет $31 \cdot (2^{128} + 2^{80})$ операций зашифрования. Вероятность успеха атаки равна 1

Список литературы

1. Ronjom S., Bardeh N. G., Helleseth T. Yoyo tricks with AES // ASIACRYPT 2017. Lect. Notes Comput. Sci. 2017. V. 10624. No. 1. P. 217 – 243.

2. Biryukov A., Shamir A. Structural cryptanalysis of SASAS // EUROCRYPT'01, Lect. Notes Comput. Sci. 2001. V. 2045. P. 394–405.

3. Adomnicai A., Berger T. P., Clavier C., Francq J., Huynh P., Lallemand V., GouguecK.Le, MinierM., ReynaudL. and ThomasG. Lilliput-AE: a New Lightweight Tweakable Block Cipher for Authenticated Encryption with Associated Data // NIST Lightweight Cryptography Standardization Process, 2019. https://csrc.nist.gov/Projects/Lightweight-Cryptography.

УДК 519.7

Н.А. КОНОВАЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

MD45: СОВМЕЩЕННЫЙ ПАРАМЕТРИЗОВАННЫЙ АЛГОРИТМ ДЛЯ ВЫЧИСЛЕНИЯ ХЕШ-ЗНАЧЕНИЙ MD4 И MD5

В работе приводится описание и реализация алгоритма MD45 – параметризованного алгоритма для вычисления хеш-значений MD4 или MD5, в зависимости от входных данных. Использование предлагаемого алгоритма в качестве альтернативы стандартным программно-аппаратным реализациям данных хеш-функций позволяет существенно сократить аппаратные ресурсы, требуемые для осуществления вычислений.

При проектировании программных или аппаратных средств ускорения вычислений распространен подход параллелизма вычислений с разбиением по данным. Счетные алгоритмы при этом являются физическими или виртуальными копиями, производящими вычисления над разными массивами данных. В том случае, когда такие копии реализуются аппаратно без возможности реконфигурирования, особенное значение имеет их количество, размер и универсальность.

В работах [1, 2] приведены стандартные реализации алгоритмов хеш-функций MD4 и MD5. Оба алгоритма имеют почти идентичную структуру: информационный блок M, который расширяется и разбивается на p блоков по k бит, вычисление образа h, которое происходит путем применения рекуррентной функции C (функция сжатия) над очередным промежуточным значением образа h_i и блоком открытого текста M_i:

$$C: \{0,1\}^{(128)} \times \{0,1\}^{(k)} \rightarrow \{0,1\}^{(128)}, k = 512; \#$$
$$h_{i+1} = C(h_i, M_i); \#(1)$$
$$F(M_0, \dots, M_{p-1}) = h_p, i = \{0, \dots, p-1\}. \#$$

Результатом вычисления хеш-функций (образом) является конкатенация 32-х битных векторов:

$$h = h_p = h_{p-1}^0 \,||\, h_{p-1}^1 \,||\, h_{p-1}^2 \,||\, h_{p-1}^3. \#(2)$$

Основными различиями между хеш-функциями MD4 и MD5 являются количество раундов, используемые константные значения, а также

изменённая функция G и новая функция I. Данные различия учитывались при разработке модифицированного алгоритма, позволяющего считать одну из хеш-функций (MD4 или MD5) в зависимости от входных параметров. Приведенный в работе параметризованный алгоритм MD45 совмещает структуру построения хеш-функций MD4 и MD5, и принимает на вход следующие параметры:

- информационный блок размером 512 бит;
- 32-х битный флаг;
- таблицу значений циклических сдвигов;
- таблицу значений констант;
- таблицу значений индексов.

В MD45 были переработаны и параметризованы функции F, G, H, I. Параметризована функция обновления состояний, добавлен ранний выход по условию. Сгенерированы таблицы значений циклических сдвигов, констант, индексов.

При подсчете количества базовых логических операций, необходимых для осуществления вычислений, было получено, что требуемое количество операций для алгоритма MD45 существенно меньше количества операций, необходимых для возможности вычислений хеш-функций MD4 и MD5 при стандартной программной реализации. Такие же результаты были получены при оценке максимального объема занимаемой памяти, необходимой для работы вышеупомянутых алгоритмов.

Таким образом, при проектировании и реализации аппаратных ускорителей вычислений без возможности реконфигурации, использующих параллельный подход с разбиением по данным, размещение копий алгоритма MD45 будет являться более эффективным, чем размещение копий алгоритмов хеш-функций MD4 и MD5 по отдельности.

Техника синтеза алгоритма MD45 в дальнейшем может быть применена для объединения и параметризации других алгоритмов хеширования (SHA-семейство) и шифрования со схожими структурами.

Список литературы

1. Rivest, R.L.: The MD4 Message Digest Algorithm. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 303–311. Springer, Heidelberg (1991).

2. Rivest R.L.: MD5 Algorithm. Network Working Group, Request for Comments: 1321. [Электронный ресурс] // MIT Laboratory for Computers. (1991).

УДК 512.531; 519.7

В.П. ЦВЕТОВ
Самарский национальный исследовательский университет им. академика С.П. Королева

НЕАССОЦИАТИВНЫЕ АЛГЕБРЫ И ОТКРЫТОЕ РАСПРОСТРАНЕНИЕ КЛЮЧЕЙ

В докладе рассматривается обобщение протокола открытого распространения ключей Диффи-Хелмана на произвольный конечный группоид.

В основе современных криптосистем с открытым ключом лежат алгебры с ассоциативными бинарными операциями. Это объясняется тем, что свойство ассоциативности обеспечивает построение алгоритмов формирования односторонних функций. В частности, протокол Диффи-Хелмана использует быстрый алгоритм возведения в степень элементов полугруппы, имеющий сложность $O(log(n))$ полугрупповых операций, в то время как известные алгоритмы дискретного логарифмирования имеют сложность порядка $O(n)$. Тем не менее, неассоциативные операции могут оказаться полезными в асимметричной криптографии, с точки зрения представления их в качестве элементов ассоциативных алгебр. Подобный подход изложен в [1-2] в терминах полугрупп многоместных отношений $R_1, R_2 \subseteq U^n$ на множестве U, в которых полугрупповые операции обобщают операцию композиции/произведения бинарных отношений:

$$R_1 \circ_{ij} R_2 = \{(u_{1,..}u_i,..,u_{j,..}u_n) \mid \exists u_0 (u_{1,..}u_{0,..}u_{j,..}u_n) \in R_1 \wedge (u_{1,..}u_{i,..}u_{0,..}u_n) \in R_2\}. \quad (1)$$

Для бинарных операций $\varphi_1, \varphi_2 : U^2 \to U$ определение (1) для $i = 3$ и $j = 1$, может быть записано в виде:

$$\varphi_1 \odot \varphi_2 (u_1, u_2) = \varphi_1 \circ_{31} \varphi_2 (u_1, u_2) = \varphi_2 (\varphi_1 (u_1, u_2), u_2). \quad (2)$$

В случае определения бинарных операций $\varphi_1, \varphi_2 : U^2 \to U$ при

помощи матриц Кэли $A_1 = \left(a_{ij}^1\right)$ и $A_2 = \left(a_{ij}^2\right)$ на множестве $1..n$ элементы матрицы Кэли их композиции $A_3 = \left(a_{ij}^3\right)$ определяются как $a_{ij}^3 = a^2_{a_{ij}^1 j}$. При вычислении степеней в циклической полугруппе, определенной операцией $\varphi : U^2 \to U$ с матрицей Кэли $A = \left(a_{ij}\right)$, для достаточно больших значений n, обеспечивающих нужную степень криптостойкости, будут требоваться большие объемы памяти. Эти ограничения снимаются для матриц Кэли специального вида, имеющих фрактальную структуру. В [3] определены понятия фрактальных расширений и эффективные алгоритмы их реализаций, перестановочные с операцией возведения в степень матриц Кэли. В частности, диагональное расширение порядка $2n$, которое определяется как:

$$a_{ij}^d = \begin{cases} a_{ij}, i \in 1..n,\ j \in 1..n \\ a_{ij-n} + n, i \in 1..n,\ j \in n+1..2n \\ a_{i-nj} + n, i \in n+1..2n,\ j \in 1..n \\ a_{i-nj-n} + n, i \in n+1..2n,\ j \in n+1..2n \end{cases}$$

Строящиеся на их основе расширения порядка $2^k n$ позволяют экспоненциально относительно k увеличивать мощность носителя группоида, оперируя только элементами матрицы Кэли порядка n.

Список литературы

1. Tsvetov V.P. Algebras of finitary relations. CEUR Workshop Proceedings, 2019, vol. 2416, pp. 119–125. DOI: https://doi.org/10.18287/1613-0073-2019-2416-119-125.

2. Цветов В.П. Полугруппы бинарных операций и криптосистемы на группоидах // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 1. С. 23–51. DOI: http://doi.org/10.18287/2541-7525-2020-26-1-23-51.

3. Цветов В.П. Фрактальные группоиды и криптография с открытым ключом // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 2. С. 23–49. DOI: http://doi.org/10.18287/2541-7525-2020-26-2-23-49.

УДК 519.719.2

А.С. ТИССИН

ООО «Центр сертификационных исследований», Москва

О КРИВИЗНЕ ФУНКЦИИ ВЫДЕЛЕНИЯ РАЗРЯДА В ДВОИЧНОМ ПРЕДСТАВЛЕНИИ ЧИСЛА

Пусть заданы числа $n \in \mathbb{N}$, $k \in \mathbb{N}_0$, удовлетворяющие условиям $2^k \le n < 2^{k+1}$ и $t \in \mathbb{N}$. Любое число $a \in \{0,1,\dots, n-1\}$ однозначно представляется в виде $a = a_0 + a_1 2 + \cdots + a_k 2^k$, где $a_0, a_1, \dots, a_k \in \{0,1\}$. Для функции $\varphi_t(a) = a_t$ получены нетривиальные верхние оценки кривизны $\sigma(\varphi_t)$ в случаях нечетного n при $t = 0$, $t = k$, а также при $n = 2^{k+1} - 1$ или $n = 2^k + 1$ и всех $0 \le t \le k$. Рассмотрены применения результатов к алгоритму поточного шифрования ZUK.

Введение

Пусть $\mathbb{N}$ – множество натуральных чисел, $\mathbb{N}_0$ – множество целых неотрицательных чисел. Пусть заданы числа $n \in \mathbb{N}$, $k \in \mathbb{N}_0$, удовлетворяющие условиям $2^k \le n < 2^{k+1}$ и $t \in \mathbb{N}$. Тогда любое число $a \in \{0,1,\dots, n-1\}$ однозначно представляется в виде

$$a = a_0 + a_1 2 + \cdots + a_k 2^k, \tag{1}$$

где $a_i \in \{0,1\}$, $i \in \{0,1,\dots,k\}$.

Обозначим через $\mathbb{Z}_n$ – кольцо вычетов по модулю n. Рассмотрим отображение $\varphi_t: \mathbb{Z}_n \to \{0,1\}$, действующее по правилу

$$\varphi_t(a) = a_t, \tag{2}$$

где a_t из формулы (1), $t \in \{0,1,\dots,k\}$.

Кривизной функции φ_t, определенной равенством (2) назовём следующую величину (см., например, [1–4]):

$$\sigma(\varphi_t) = \frac{1}{n} \sum_{a \in \mathbb{Z}_n} \left| \sum_{b \in \mathbb{Z}_n} (-1)^{\varphi_t(b)} e^{-2\pi i \frac{ab}{n}} \right|$$

Оценки кривизны φ_t функции применимы для оценки числа появлений элементов в алгоритме поточного шифрования ZUK.

Оценки кривизны функции выделения двоичного разряда

Теорема 1. Пусть n – нечетное число, $t = 0$ или $t = k$. Тогда верна следующая оценка

$$\sigma(\varphi_t) \le \frac{8}{\pi^2} \log n + \frac{13}{5}.$$

Теорема 2. Пусть $\mathrm{n} = 2^{k+1} - 1$ или $\mathrm{n} = 2^k + 1, 0 \le t \le k$. Тогда верна следующая оценка

$$\sigma(\varphi_t) \le \frac{8}{\pi^2}\log \mathrm{n} + \frac{13}{5}.$$

Отдельно отметим, что эти оценки улучшают общую оценку

$$\sigma(\varphi_t) \le \sqrt{n},$$

полученную в [2] при $\mathrm{n} \ge 29$.

В алгоритме поточного шифрования ZUK [6] используется линейная рекуррентная последовательность u над полем $GF(2^{31} - 1)$. При этом любому значению $u(i)$ при реализации сопоставляется двоичный вектор $\left(\varphi_0(u(i)), \dots, \varphi_{31}(u(i))\right), i \ge 0$. Обозначим через $\varphi_t(u)$ последовательность с элементами $\varphi_t(u(i)), i \ge 0$. Для каждого $z \in \{0,1\}$ $l \ge 1$ обозначим через $N_l(\varphi_t(u), z)$ – число появлений z среди $\varphi_t(u(0)), \dots, \varphi_t(u(l-1))$ при фиксированном t.

Теорема 3. [1, 5] Пусть $F(x)$ – реверсивный многочлен степени m над полем $P = GF(q)$ с периодом $\mathrm{T(F)}$, u–линейная рекуррентная последовательность с характеристическим многочленом $F(x)$, $v = \varphi_t(u)$. Тогда для любого $z \in \{0,1\}$ при $l \le \mathrm{T(F)}$ верно

$$\left|N_l(v, z) - \frac{l}{2}\right| \le \frac{1}{2}\sigma(\varphi_t) \cdot \left(\frac{4}{\pi^2}\ln \mathrm{T(F)} + \frac{13}{5}\right).$$

В алгоритме поточного шифрования ZUK для $z \in \{0,1\}$ верно

$$\left|N_l(\varphi_t(u), z) - \frac{l}{2}\right| \le 1.1 \cdot 2^{23}.$$

Список литературы

1. Камловский О.В. Спектральный метод оценки числа решений систем нелинейных уравнений с линейными рекуррентными аргументами. Дискретная математика. 2016, т. 28, № 2, с. 27–43.

2. Логачев О.А., Федоров С.Н., Ященко В.В. Булевы функции как точки на гиперсфере в евклидовом пространстве. Дискретная математика. 2018, т. 30, № 1, с. 39–55

3. Камловский О.В. Суммы модулей коэффициентов Уолша-Адамара некоторых сбалансированных функций. Математические вопросы криптографии. 2017, т. 19, № 2, с. 129–145.

4. Де Ла Крус Хименес Р.А., Камловский О.В. Суммы модулей коэффициентов Уолша-Адамара булевых функций. Дискретная математика. 2015, т. 27, № 4, с. 49–66.

5. Тиссин А.С. Число появлений элементов из заданного подмножества на отрезках усложнений линейных рекуррентных последовательностей, ПДМ, 2023, т. 60, № 2, с. 30–39.

6. Wu, H., Huang, T., Nguyen, P.H., Wang, H., Ling, S. (2012). Differential Attacks against Stream Cipher ZUC. In: Wang, X., Sako, K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg.

УДК 519.7

А.А. КОЗЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ОБ АППАРАТНОЙ РЕАЛИЗАЦИИ НИЗКОРЕСУРСНЫХ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

В связи с активным развитием Интернета вещей особо остро стоит проблема обеспечения безопасности информации в устройствах с ограниченными вычислительными ресурсами. В работе представлены результаты по аппаратной реализации ARX-алгоритмов блочного шифрования. Представлены выходные характеристики алгоритма по числу необходимых для построения логических вентилей, и скорости генерации выходной последовательности. Качество алгоритма подтверждается проведенными статистическими тестами.

Существующие классические алгоритмы стохастического преобразования данных, например AES, не подходят для использования в устройствах с ограниченными вычислительными ресурсами. Основным средством обеспечения конфиденциальности и целостности в таких устройствах является использование низкоресурсных алгоритмов [1, 2]. В связи с этим существует открытая проблема построения эффективного низкоресурсного алгоритма блочного шифрования. При этом эффективность оценивается по двум параметрам: числу логических вентилей, необходимых для аппаратной реализации и скорости генерации выходной последовательности алгоритма.

Для решения этой задачи был разработан и запатентован [3] ARX-алгоритм блочного шифрования. Статистические свойства разработанного алгоритма были проанализированы в соответствии со стандартами NIST. В режиме гаммирования алгоритм был протестирован на популяции из 100000 выборок. Для каждой из них было получено, что не менее 94% выходных последовательностей алгоритма удовлетворяют требованиям на случайность.

Эффективность алгоритма оценивалась по его производительности и числу требуемых для его аппаратной реализации логических вентилей. Выходные данные для практической реализации алгоритма представлены в табл. 1. Сравнительные данные с другими известными низкоресурсными алгоритмами представлены в табл. 2.

Таблица 1. Требования к элементной базе и полученная производительность

Входной блок, бит/ключ, бит	Логические элементы, шт	Производительность, Кбит/сек (100 КГц)
32/32	781	44.4
64/64	1184	122.7
128/128	1501	180.3

Таблица 2. Требования к элементной базе и полученная производительность

Название алгоритма	Входной блок, бит/ ключ, бит	Логические элементы, шт	Производительность, Кб/сек (100 КГц)
SIMON [4]	64/128	1524	133.3
SIMECK [4]	64|128	1484	133.3
PRESENT [5]	64/128	1884	200

Данные в табл. 2 убедительно показывают, что реализация разработанного алгоритма превосходит имеющиеся аналоги по одному из двух или сразу по обоим показателям эффективности. Полученные результаты сравнения позволяют утверждать, что реализация разработанного алгоритма может эффективно применяться в низкоресурсных технических решениях, позволяя поддерживать при этом высокую скорость обработки данных.

Список литературы

1. Рындина С.В., Куликова С.В., Михайлова К.Д. // Модели, системы, сети в экономике, технике, природе и обществе. – 2020. – No 2 (34). – С. 145–153. – DOI 10.21685/ 2227-8486-2020-2-11.

2. Курчеева Г.И., Денисов В.В. Угрозы для информационной безопасности в высокоорганизованных системах типа «Умный город»//Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, No3(2016).

3. Козлов А.А., Иванов М.А. НИЯУ МИФИ. Устройство для генерации псевдослучайных чисел. Патент №RU2774812C1. МПК G06F 7/58. Заявл. 2021120046, 2021.07.08. Опубл. 2022.06.23.

4. R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith and L. Wingers, "The SIMON and SPECK lightweight block ciphers," *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, CA, USA, 2015, pp. 1-6, doi: 10.1145/2744769.2747946.

5. Poschmann, A. (2009). Lightweight Cryptography - Cryptographic Engineering for a Pervasive World. Cryptology ePrint Archive, Paper 2009/516. https://eprint.iacr.org/2009/516

УДК 519.7

Б.Н. ЗАГАРТДИНОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ РЕАЛИЗАЦИИ АППАРАТНОЙ ПЛАТФОРМЫ КОНФИДЕНЦИАЛЬНЫХ ВЫЧИСЛЕНИЙ НА БАЗЕ ПРОЦЕССОРА AMD EPYC 7313

Исследование направлено на анализ аппаратной платформы конфиденциальных вычислений на базе процессора AMD Epyc 7313. В результате исследования восстановлен и проанализирован алгоритм доверенной загрузки, обнаружены недостатки в его реализации. Системный и всесторонний анализ реализаций позволит сформулировать требования к будущим вычислительным системам.

Конфиденциальные вычисления – новое направления теории построения архитектур современных вычислительных систем. Предметом исследований этого направления являются методы имплементации на аппаратном уровне защиты данных во время использования в различных сценариях [1].

Всестороннее исследование реализаций платформ конфиденциальных вычислений позволит более детально подойти к формированию функциональных требований к будущим аппаратным платформам, реализующим концепцию конфиденциальных вычислений. В частности, исследования в этой области позволят повысить общую безопасность облачных вычислений, а также в будущем реализовать открытую платформу конфиденциальных вычислений на базе открытых архитектур, таких как RISC-V, с учетом опыта ведущих производителей.

Процессор AMD Epyc 7313 с технологией SEV-SNP является одной из систем реализующей концепцию конфиденциальных вычислений. Выбор AMD Epyc 7313 в качестве предмета исследования обусловлен относительной новизной и доступность на рынке. Данная система на кристалле представляет 3 поколение внутренней архитектуры Zen. Уже существует 4 поколение, но приобрести серверные системы на кристалле с такой архитектурой на свободном рынке в настоящее время затруднительно.

Ранее в исследованиях [2–4] рассматривались недостатки реализации технологии SEV-SNP, однако раскрытые в данном исследовании недостатки программной реализации алгоритма загрузки платформы освещены не были.

Центральным элементом безопасности платформы на базе этого процессора является сопроцессор AMD PSP, обеспечивающий шифрование памяти, изоляцию защищаемых виртуальных машин от гипервизора и функции удаленной аттестации платформы. Для его изучения на основе исследования [2] была проведена атака внедрения контролируемого аппаратного сбоя, в результате чего из внутреннего ПЗУ получен загрузочный код сопроцессора безопасности, выступающий начальным элементом цепочки загрузки платформы. Суть атаки внедрения контролируемого аппаратного сбоя заключается в контролируемом выведении одного или нескольких внешних параметров среды (температура, питающее напряжение и т.п.) за допустимые для работы устройства границы. Изменение внешних параметров вносит непредсказуемость в поведение устройства, однако за счет контролируемости данных изменений возможно в зависимости от выбранной модели атаки достижение благоприятных для атакующего событий, например пропуска одной или нескольких инструкций на центральном процессоре, передача управления в произвольное место и т.д.

В результате анализа полученного загрузочного кода выявлено, что реализация платформы содержит ряд недостатков: несмотря на наличие аппаратной возможности производителем не предприняты шаги для защиты от отката версии программного обеспечения сопроцессора безопасности, в реализации механизма аттестации платформы используется криптографически не стойкая функция выработки ключей.

Дальнейшее направление исследований безопасности платформы включает в себя изучение возможностей недокументированного аппаратного отладочного интерфейса AMD Hardware Debug Tool (HDT).

Список литературы

1. Mulligan D. P. et al. Confidential Computing—a brave new world //2021 international symposium on secure and private execution environment design (SEED). – IEEE, 2021. – С. 132–138.

2. Buhren R. et al. One glitch to rule them all: Fault injection attacks against amd's secure encrypted virtualization //Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. – 2021. – С. 2875–2889.

3. Li M. et al. A systematic look at ciphertext side channels on AMD SEV-SNP //2022 IEEE Symposium on Security and Privacy (SP). – IEEE, 2022. – С. 337-351.

4. Wang W. et al. PwrLeak: Exploiting Power Reporting Interface for Side-Channel Attacks on AMD SEV //International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. – Cham: Springer Nature Switzerland, 2023. – С. 46–66.

УДК 519.7

Ю.Р. КИНДЕЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

РАЗРАБОТКА СПОСОБОВ ПОИСКА ЭКВИВАЛЕНТНЫХ КЛЮЧЕЙ В ПОТОЧНЫХ ШИФРСИСТЕМАХ, ОСНОВАННЫХ НА АЛГОРИТМЕ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ПОДСТАНОВОК ФИШЕРА-ЙЕТСА

Выполнен сравнительный анализ алгоритмов генерации начальной подстановки в поточной шифрсистеме RC4 и её модификаций RC4A, VMPC и RC4D, основанных на алгоритме генерации случайной подстановки Р.А. Фишера и Ф. Йетсом. Проанализированы алгоритмы получения пар эквивалентных ключей малой длины. Найдена закономерность при формировании эквивалентных ключей. На основе нее разработан новый алгоритм генерации пар эквивалентных ключей.

В основе поточной шифрсистемы RC4 [1] лежит алгоритм генерации случайной подстановки, предложенный Р.А. Фишером и Ф. Йетсом [2]. Для улучшения её криптографических свойств предложено множество модификаций: RC4A (2004), VMPC (2004), TPy6-A и TPy6-B (2007), RC4+ (2008), NGG и GGHN (2011), Spritz (2014), mRC4 (2019), eRC4 (2021), RC4D (2021).

В поточной шифрсистеме RC4 существует уязвимость, связанная с эквивалентными ключами [3]. Доказать наличие таких ключей можно следующим образом: число различных ключей длины m равно m^m, а число возможных подстановок длины m равно $m!$, что значительно меньше количества ключей. Однако распределение классов эквивалентных ключей остается неизвестным. Поэтому актуальным является разработка алгоритмов поиска эквивалентных ключей. Одним из наиболее эффективных является алгоритм Джена-Пол [4].

В данной работе показано, что по найденной паре эквивалентных ключей меньшей длины можно получить пару эквивалентных ключей большей длины, фиксируя начальные первые m бит ключей и опираясь на найденную ранее пару. Используя найденную закономерность, разработан и впоследствии модернизирован новый алгоритм.

Сравнительная оценка трудоемкости предложенных ранее и разработанного алгоритма представлена в табл. 1. Трудоемкость разработанного алгоритма оказалась меньше предложенных ранее

алгоритмов на 7 двоичных порядков для длины ключа 32 байта и на 21 двоичный порядок для длины ключа 20 байт.

Таблица 1. Оценка трудоемкости алгоритмов поиска эквивалентных ключей

Длина ключа в байтах	Алгоритм Мацуи	Алгоритм Чэнь-Миядзи	Алгоритм Джена-Пол	Разработанный алгоритма
20	2^{56}	2^{51}	2^{33}	2^{12}
26	2^{42}	2^{36}	2^{26}	$2^{12.5}$
32	2^{36}	2^{32}	2^{20}	2^{13}

В работе была дана оценка успешности работы разработанного алгоритма для модификаций поточной шифрсистемы RC4. Под успешностью алгоритма понимается вероятность получения пары эквивалентных ключей для заданных входных данных. Ранее такую оценку создатели своих алгоритмов в [4] не приводили. Полученная оценка успешности для модификаций RC4A, VMPC, RC4D и исходной шифрсистемы приведена в табл. 2.

Таблица 2. Оценка успешности разработанного алгоритма поиска эквивалентных ключей

Значение параметра m	RC4 $p_{усп}$	RC4A $p_{усп}$	VMPC $p_{усп}$	RC4D $p_{усп}$
4	1	1	1	1
84	0,800	0,684	0,641	0,777
204	0,730	0,613	0,57	0,724
256	0,714	0,596	0,554	0,711

Подводя итог нужно подчеркнуть, что разработанный алгоритм является менее трудоемким, чем представленные ранее в [4–6].

Список литературы

1. R. Rivest RSA security response to weaknesses in key scheduling algorithm of RC4 // Technical note, RSA Data Security Inc. 2001. – С. 3.

2. Fisher R. A., Yates F. Statistical tables for biological, agricultural and medical research // Journal of the Royal Statistical Society: Series A (General). – 1938. – С. 426-449.

3. Sumartono I., Siahaan A. P. U., Mayasari N. An overview of the RC4 algorithm // IOSR J. Comput. Eng. – 2016. – Т. 18. – №. 6. – С. 67–73.

4. Jana A., Paul G. Revisiting RC4 key collision: Faster search algorithm and new 22-byte colliding key pairs // Cryptography and Communications. – 2018. – С. 479–508.

5. Matsui M. Key collisions of the RC4 stream cipher // Fast Software Encryption: 16th International Workshop, FSE 2009 Leuven, Belgium, February 22-25, 2009 Revised Selected Papers. – Springer Berlin Heidelberg, 2009. – С. 38–50.

6. Chen J., Miyaji A. Novel strategies for searching RC4 key collisions // Computers & Mathematics with Applications. – 2013. – С. 81–90.

УДК 519.7

К.В. АНТОНОВ, Д.А. ЗАХАРОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

О ПОИСКЕ НЕВОЗМОЖНЫХ РАЗНОСТЕЙ АЛГОРИТМА GRANULE С ПРИМЕНЕНИЕМ SAT-ПОДХОДА

Работа посвящена разработке метода поиска невозможных разностей для алгоритмов блочных шифрования. Предложен подход, который с помощью транслятора SAW и SAT-решателя CryptoMiniSat позволяет в процессе поиска учитывать не только свойства нелинейных преобразований, но и алгоритма развертывания ключа. Для алгоритма шифрования GRANULE с использованием данного подхода найдено 562 8-раундовых невозможных разности. Данный результат является наилучшим по числу раундов на момент написания работы.

Введение

Метод невозможных разностей, предложенный в 1999 г. в [1], является одним из эффективных методов анализа алгоритмов блочного шифрования [2, 3]. Он позволяет частично восстановить секретный ключ на основе невозможной разностной характеристики с использованием свойств линейных преобразований раундовой функции. Долгое время поиск разностей не был автоматизирован, первой работой в этом направлении является [4].

Для автоматизации в нашей работе применяются алгоритмы SAT [5]. В рамках SAT-подхода анализ алгоритмов симметричного шифрования сводится к задаче булевой выполнимости (SAT). Для решения SAT применяются специальные программные средства – SAT-решатели [6].

Описание алгоритма поиска

На основе функции зашифрования, заданной алгоритмически, строится КНФ специального вида, в ней фиксируются значения входной и выходной разностей. Если при заданных значениях КНФ невыполнима, то найдена невозможная разность [5]. КНФ строится при помощи транслятора SAW [7], для этого алгоритм зашифрования записывается на языке Cryptol [7]. Выполнимость КНФ проверяется решателем CryptoMiniSat [6].

Разработанный метод был применен к алгоритму шифрования GRANULE [8]. Сравнение с другими работами приведено в табл. 1.

Перебор разностей проводился только по векторам веса 2, причем только с 1 ненулевым 4-битным подблоком. Из 2304 опробованных 8-раундовых разностей 562 оказались невозможными. Это лучший результат по числу раундов. Нахождение таких разностей позволяет

построить атаку на 14 раундов GRANULE [8] с использованием методики из работы [9]. Этот факт приведен в табл. 1.

Таблица 1. Сравнение атак на GRANULE [9] методом невозможных разностей

Число раундов различителей	Число различителей	Число раундов атаки	Источник
5	9	11	[9]
7	144	13*	[10]
7	6048	13*	[11]
8	562	14*	Данная работа

В результате исследования удалось разработать метод доказательства невозможности разности с использованием SAT-решателей, который позволил впервые найти 8-раундовую разность для алгоритма шифрования GRANULE [8]. Данные разности могут быть использованы для атаки 14 раундов GRANULE [8], что также получено впервые в данной работе.

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 Proceedings. – Berlin, Heidelberg : Springer, 1999. – P. 12–23.

2. Lu J. et al. New impossible differential attacks on AES // Progress in Cryptology-INDOCRYPT 2008. Proceedings. – Berlin, Heidelberg : Springer, 2008. – P. 279–293.

3. Liu W., Yang Y. The 7-round subspace Trail-based impossible differential distinguisher of Midori-64 // Security and Communication Networks. – 2021. – T. 2021. – P. 1–15.

4. Wu S., Wang M. Automatic search of truncated impossible differentials for word-oriented block ciphers // International Conference on Cryptology in India. – Berlin, Heidelberg : Springer, 2012. – P. 283–302.

5. Sun L., Wang W., Wang M. Accelerating the search of differential and linear characteristics with the SAT method // IACR Transactions on Symmetric Cryptology. – 2021. – P. 269–315.

6. Soos M. The CryptoMiniSat 5 set of solvers at SAT Competition 2016 // Proceedings of SAT Competition. – 2016. – P. 28.

7. Carter K. SAW: the software analysis workbench / K. Carter, A. Foltzer, J Hendrix, B. Huffman, A. Tomb // Proceedings of the 2013 ACM SIGAda annual conference on High integrity language technology. – 2013. – P. 15–18.

8. Bansod G., Patil A., Pisharoty N. GRANULE: An Ultra lightweight cipher design for embedded security // Cryptology ePrint Archive. – 2018. – P. 1–12.

9. Shi S., He J. Impossible Differential Cryptanalysis of GRANULE Algorithm // Computer Engineering, 45(10). – 2019. – P. 134–138.

10. Wu X., Li Y., Wei Y., Sun. Y. Analysis of impossible differential distinguisher for GRANULE and MANTRA ciphers // Journal on Communications, LNCS, 41. – 2020. – P. 94–101.

11. Zakharov D., Pudovkina M. Full round impossible differentials for Feistel ciphers // Journal of Computer Virology and Hacking Techniques. – 2023. – P. 1–6.

УДК 519.7

А.А. МУХОРТОВА, В.Д. АФОНИН

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ СЕМЕЙСТВА АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ MANTIS МНОГОМЕРНЫМ МЕТОДОМ ВСТРЕЧА ПОСЕРЕДИНЕ

В работе исследуется стойкость алгоритма блочного шифрования MANTIS к атаке на основе многомерного метода «встречи посередине» (MD-MITM). Построена и смоделирована атака на MANTIS_2. Временная сложность атаки: $2^{111,1}$, объём памяти: 2^{67} ячеек памяти по 72 бита, необходимый объём материала: две пары открытый текст/шифртекст. Результаты обобщены на семейство MANTIS-подобных алгоритмов шифрования.

Впервые атака методом встречи посередине [1] была предложена Диффи и Хеллманом в 1977 г.. Дальнейшее исследование привело к появлению многомерного метода встречи посередине [2], предложенного Бо Жу и Гуан Гоном в 2011 г. применительно к низкоресурсному алгоритму блочного шифрования KATAN. Позднее этот же метод атаки был применен к алгоритму PRINCE. MANTIS [3] – низкоресурсный алгоритм блочного шифрования, базирующийся на алгоритмах PRINCE [4] и MIDORI [5].

Раундовая функция идентична раундовой функции MIDORI: $R_i(\cdot, tk) = \text{MC} \circ \text{P} \circ \text{AT}_{tk} \circ \text{RC}_i \circ \text{S}$, где S – S-бокс, RC_i м побитовое сложение с i-й раундовой константой, AT_{tk} – побитовое сложение с раундовым ключом tk, P — перестановка, MC – линейное преобразование, задающееся инволютивной матрицей. Функция зашифрования задана условием

$$E(\cdot, k_0, k_1, k_0') = \text{AT}_{k_0' \oplus k_1 \oplus \alpha \oplus T} \circ R_1^{-1}(\cdot, tk) \circ \ldots \circ R_r^{-1}(\cdot, tk) \circ \text{S} \circ \text{MC} \circ \text{S} \circ R_r(\cdot, tk) \circ \ldots \circ R_1(\cdot, tk) \circ \text{AT}_{k_0 \oplus k_1 \oplus T},$$

$$E: V_{256}(2) \to V_{64}(2), k_0, k_1, k_0' \in V_{64}(2),$$

где r – количество раундов. От PRINCE алгоритм унаследовал общую конструкцию, что обеспечило наличие у него свойства α-отражения, т.е. $E^{-1}(p, k) = E(p, k')$, где $k' = f(k, \alpha)$ – сопряжённый ключ. Открытый текст m представим в виде матрицы 4×4 следующим образом:

$$m = m_0 || m_1 || \ldots || m_{15}, m \in M_4\big(V_4(2)\big), m_i \in V_4(2), i \in \{0, \ldots, 15\},$$

где $V_m(2^n)$ – m-мерное векторное пространство над $GF(2^n)$, $M_n(A)$ – множество квадратных матриц размера n, элементы которых принадлежат множеству A.

В данной работе предложено семейство MANTIS-подобных алгоритмов блочного шифрования. Пусть открытый текст представим в виде d $\boldsymbol{r}$-битных ячеек:

$$d = 4\delta^2, \delta \in \{1,2,\dots\}: m = m_0|\,|m_1|\,|\dots|\,|m_{d-1},$$
$$m \in M_n\big(V_r(2)\big), m_i \in V_r(2),\ i\ \in \{0,\dots,d-1\}.$$

MANTIS является частным случаем семейства при значениях параметров $d = 4, r = 4$. На семейство алгоритмов блочного шифрования MANTIS разработана атака, основанная на многомерном методе «встречи посередине» [2] и применяет идея на атаке на PRINCE [13]. Перебирая только определённые биты ключа с учётом строения MANTIS, находим и последовательно уменьшаем множество допустимых ключей. Показано, что необходимый объём материала для атаки равен 2 парам открытых текстов. Временная сложность алгоритма равна

$$2^{r(d^2-2d+1)+r(d-1)+rd^2}(2d^2 + 2 \cdot (d^2 - 2d + 1)) \cdot \frac{1}{d^2} \cdot \frac{1}{6}$$

элементарных операций. Объём памяти равен 2^{rd^2-d+1} ячеек памяти по $2r(d^2 - 2d + 1)$ бит. Для оригинального MANTIS_2 имеем: $2^{111,1}-$ временная сложность, 2^{67} ячеек памяти по 72 бита– объём памяти.

Список литературы

1. Biham, E., Shamir, A. (1991). Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds) Advances in Cryptology-CRYPTO' 90. CRYPTO 1990. Lecture Notes in Computer Science, vol 537. Springer, Berlin, Heidelberg.
2. Boztaş, Ö., Karakoç, F., Çoban, M. (2013). Multidimensional Meet-in-the-Middle Attacks on Reduced-Round TWINE-128. In: Avoine, G., Kara, O. (eds) Lightweight Cryptography for Security and Privacy. LightSec 2013. Lecture Notes in Computer Science, vol 8162. Springer, Berlin, Heidelberg.
3. Beierle, C. et al. (2016). The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS . / Robshaw, M., Katz, J. // Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science(), vol 9815. Springer, Berlin, Heidelberg.
4. Borghoff, J. et al. (2012). PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications. / Wang, X., Sako, K. // Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg.
5. Banik, S. et al. (2015). Midori: A Block Cipher for Low Energy. / Iwata, T., Cheon, J. // Advances in Cryptology – ASIACRYPT 2015. ASIACRYPT 2015. Lecture Notes in Computer Science(), vol 9453. Springer, Berlin, Heidelberg.
6. Shahram Rasoolzadeh and Håvard Raddum. 2016. Cryptanalysis of PRINCE with Minimal Data. In Proceedings of the 8th International Conference on Progress in Cryptology – AFRICACRYPT 2016 – Volume 9646. Springer-Verlag, Berlin, Heidelberg, p. 109–126.

УДК 519.7

А.А. ГОЛЯШОВ[1], В.О. ГУРЬЯНОВ[2], А.А. МУХОРТОВА[2],
О.Ю. НЕМОВА[2], К.Д. ЦАРЕГОРОДЦЕВ[3]

[1]*Балтийский Федеральный Университет им. Иммануила Канта, Калининград*

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

[3]*Московский государственный университет им. М.В. Ломоносова, Москва*

СТАТИСТИЧЕСКИЙ АНАЛИЗ СДВИГОВЫХ ПРЕОБРАЗОВАНИЙ В КВАЗИГРУППАХ

Для сохранения формата при зашифровании текста из некоторого относительно маленького множества могут использоваться подстановки на основе квазигрупповых сдвигов (умножений слева/справа на элементы квазигруппы). В настоящей работе проводится эмпирическое исследование распределения некоторых статистик квазигрупповых сдвигов при разном задании структуры квазигруппы. Проведено сравнение распределений анализируемых статистик с теоретическими значениями. Лучший результат показал способ порождения квазигрупповой операции на основе случайного изотопа абелевой группы.

Введение

Преобразования на основе квазигрупповых сдвигов используются в построении и анализе хеш-функций [1], блочных алгоритмов шифрования [2,3] и др. В данной работе рассматривается применение квазигрупповых сдвигов в задаче построения алгоритма шифрования, сохраняющего формат сообщения [4]. Заметим, что стандартные блочные шифры не могут обеспечить свойство сохранения формата. Для решения указанной задачи могут быть использованы псевдослучайные подстановки на основе квазигрупповых сдвигов. Целью работы являлось эмпирическое исследование статистик для получаемых таким образом преобразований. Ранее свойства подобных подстановок и их композиций изучались, например, в [5].

Статистические тесты для подстановок на малых множествах

Существующие статистические батареи тестов (например, NIST SP800-22, DIEHARD) предназначены для исследования гипотезы о независимости и равновероятности битов двоичной гаммы и не подходят для тестирования псевдослучайности подстановок на малых множествах. По указанной причине в работе были использованы специфические для

подстановок статистики: число фиксированных точек, циклов, рекордов, длина кратчайшего цикла [6], а также порядок подстановок [7].

Описание экспериментов

В рамках работы проведены эксперименты с различным способом задания квазигрупп на множестве $\{0,1\}^{10}$: на основе случайных изотопов абелевых групп и правильных семейств функций. В рамках эксперимента псевдослучайно выбирался элемент a квазигруппы, и по нему строился левый сдвиг $L_a(x) = a \circ x$. Для каждого способа задания квазигруппы генерировалось 12000 подстановок L_a, для них рассчитывались указанные выше статистики. Полученное в результате эмпирическое распределение сравнивалось с теоретическим при помощи критериев Стьюдента и χ-квадрат. Программный код был написан на языке Python.

Выводы и направления дальнейших исследований

Статистические эксперименты выявили значительное расхождение эмпирического и теоретического распределений для статистик, рассчитанных для левого сдвига в квазигруппе, порожденной при помощи правильных семейств. Для случайных изотопов эмпирическое распределение соответствует теоретическому. Среди дальнейших направлений исследований можно выделить изучение сдвигов на переменное число элементов, а также изучение свойств цепи Маркова, получающейся при последовательных сдвигах.

Список литературы

1. Slaminková I., Vojvoda M. Cryptanalysis of a hash function based on isotopy of quasigroups //Tatra Mountains Mathematical Publications. – 2010. – Т. 45. – вып. 1. – С. 137–149.
2. Tiwari S. K. et al. INRU: A Quasigroup Based Lightweight Block Cipher //arXiv preprint arXiv:2112.07411. – 2021.
3. Teşeleanu G. Quasigroups and substitution permutation networks: a failed experiment //Cryptologia. – 2021. – Т. 45. – вып. 3. – С. 266–281.
4. Bellare, M. и др. Format-preserving encryption //Selected Areas in Cryptography: 16th Annual International Workshop. – Springer Berlin Heidelberg, 2009. — С. 295–312.
5. Яшунский, А. Д. О скорости сходимости квазигрупповых сверток вероятностных распределений//Дискрет. матем. – 2022. – Т. 34 – вып. 3. – С. 160–171.
6. Sedgewick R., Flajolet P. An introduction to the analysis of algorithms. – Addison-Wesley Longman Publishing Co., Inc., 1996.
7. Goh W. M. Y., Schmutz E. The expected order of a random permutation // Bulletin of the London Mathematical Society. – 1991. – Т. 23, вып. 1. – С. 34–42.

КИБ-2023
КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Финансовая и экономическая безопасность

Руководитель секции – Норкина А.Н., к.э.н., доцент,
заместитель директора ИФТЭБ НИЯУ МИФИ

УДК 004.056

А.В. ОЛИФИРОВ[1], К.А. МАКОВЕЙЧУК[2]

[1]*Гуманитарно-педагогическая академия (филиал) «Крымский федеральный университет им. В.И. Вернадского», Ялта*

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОЙ ВАЛЮТЫ ЦЕНТРАЛЬНОГО БАНКА: РИСКИ И СРЕДСТВА ЗАЩИТЫ

В статье систематизирован перечень информационных рисков перехода на цифровую валюту центрального банка и показана связь этих рисков с экономическими и финансовыми рисками на макро и микроуровнях. Предложены средства защиты информации по рискам нарушения конфиденциальности, целостности и доступности на платформе цифрового рубля в финансово-кредитных организациях и у конечных потребителей цифровой валюты.

Переход на цифровую валюту Центрального банка (ЦВЦБ) обеспечивает много преимуществ, но, вместе с тем, несет много угроз и рисков. Если преимущества цифровых валют в научной литературе представлены хорошо, то внимание безопасным информационным технологиям и информационным рискам перехода на цифровые валюты центральных банков уделяется недостаточно [1-3]. В данной статье мы комплексно рассмотрели информационные риски платформы цифрового рубля.

Результатом данной работы является схема взаимосвязи информационных рисков и деловых рисков при переходе на цифровой рубль (см. рис. 1). В работе рассмотрены средства защиты информации от рисков нарушения конфиденциальности: несанкционированного доступа к платформе цифрового рубля, хищения профиля пользователя цифрового рубля через взлом личного кабинета, несанкционированного доступа при использовании мобильного приложения кредитной организации. Предложены средства защиты от риска нарушения целостности: при подписании транзакций с цифровым рублем и при эмиссии цифрового рубля, а также от рисков нарушения доступности: рисков неготовности инфраструктуры финансово-кредитных организаций и недостаточной производительности технологии распределенных реестров при хранении десятков терабайт информации о всех движениях денег всех людей. К ним относятся следующие основные категории средств защиты информации: средства защиты инфраструктуры, сетей, приложении, данных, пользователей.

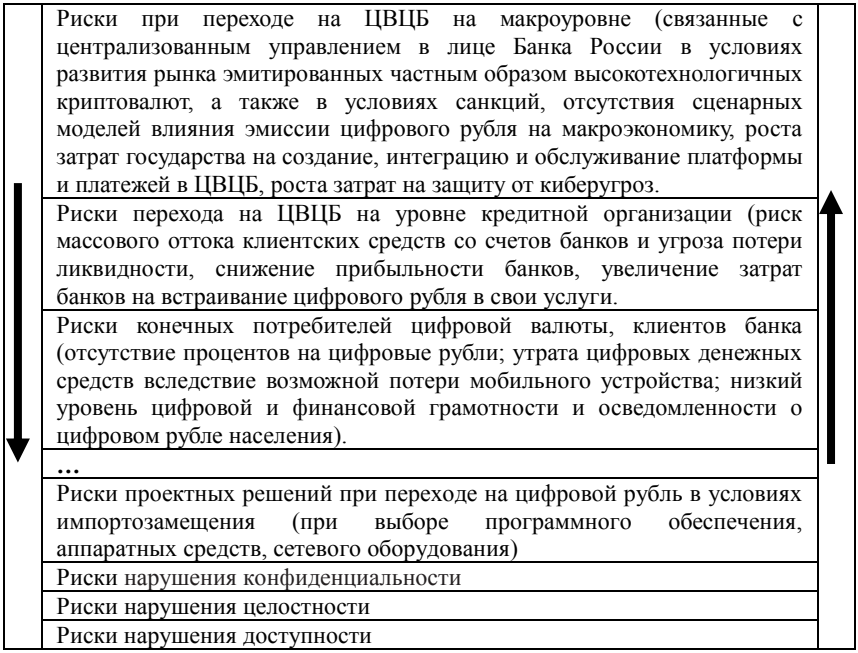

Рис. 1. Схема взаимосвязи информационных рисков и деловых рисков при переходе на ЦВЦБ

Заключение

Информационные риски влияют на деловые риски предметной области. И наоборот, экономические и финансовые риски на макро и микроуровнях влияют на риски конфиденциальности, целостности и доступности. Поэтому важным является дальнейшее исследование сценарных моделей влияния уровня информационной безопасности на эмиссию цифрового рубля.

Список литературы

1. Масленников В.В, Ларионов А.В. Цифровые валюты: концептуализация рисков и возможности регулирования. Мир новой экономики. 2021, 15(4), с. 16–28. DOI: 10.26794/2220-6469-2021-15-4-16-28

2. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С. Маркова. М.: ДМК Пресс, 2017. – 224 с.

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

УДК 336.71

Т.О. ПЛАКАСОВ
Финансовый университет при Правительстве Российской Федерации, Москва

ЦИФРОВИЗАЦИЯ ФИНАНСОВОЙ ОТРАСЛИ: НОВЫЕ ВЫЗОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цифровизация и развитие финансовых технологий стали главными причинами структурных изменений в работе финансовых организаций. Одновременно с этими процессами расширяется спектр рисков информационной безопасности, которым может подвергаться финансовая отрасль. В данной работе систематизированы угрозы в области информационной безопасности, с которыми сталкиваются организации в этой отрасли, приведены инструменты реагирования на них.

Введение

Цифровые технологии привели к смене парадигмы функционирования финансовой отрасли и широко используются как при внутреннем управлении организацией, так и предоставлении услуг клиентам. Пандемия COVID-2019 стала катализатором этих процессов: ИТ-затраты российских банков в 2021 г. выросли более чем на 12% [1].

Эта тенденция неизбежно результирует в сопоставимые изменения в области информационной безопасности (ИБ), приводя к созданию новых и развитию существующих методов атак.

Постановка задачи

В 2022 г. в отношении инфраструктуры российских банков наблюдался рост хакерских атак [2], а доля атак на финансовую отрасль за первые три квартала составила 5% от числа всех хакерских атак на российские организации [3], что также обусловлено геополитическими факторами.

Для обеспечения эффективного управления рисками в области ИБ необходима их систематизация для последующей интеграции в системы управления рисками.

Анализ открытых источников и практических бизнес-кейсов позволяет категорировать угрозы в области ИБ с точки зрения объектов (инфраструктура, в т.ч. КИИ, персональные данные (ПДн) и платежная информация, денежные средства клиентов) и инструментов хакерских атак.

Получение несанкционированного доступа к инфраструктуре организации имеет своей целью нарушение основной деятельности компании, финансовые потери, ущерб интересам стейкхолдеров (банков,

граждан, государства), а также извлечение выгоды от продажи доступа к системам и информации в даркнете [4].

Согласно [5] с 2020 г. также наблюдается глобальная тенденция увеличения финансовых потерь от утечки ПДн, причем финансовая отрасль занимает второе место. Что касается России, то в 2022 г. из финансового сектора утекло более 44 млн записей ПДн и платежной информации, что в 32 раза больше утечек в 2021 г. [6].

Хакерские атаки также направлены на похищение средств клиентов, однако для России эти риски в меньшей степени актуальны, в т.ч. ввиду наблюдающегося сокращения случаев вывода средств через карточный процессинг или систему SWIFT [2].

При этом основными инструментами хакерских атак являются DoS-атаки и ботнеты, фишинг, вредоносное программное обеспечение, трояны, атаки типа «человек посередине», атаки нулевого дня и иные [7].

Заключение

Для эффективного функционирования финансовой отрасли необходимо анализировать ландшафт угроз ИБ. Исходя из результатов анализа следует вырабатывать меры реагирования как превентивного характера (использовать доверенное ПО, проводить пентесты, повышать кибергигиену, проводить киберучения), так и реактивного характера (иметь четкий план по управлению кибер-кризисом, в т.ч. уведомлять необходимые органы, обеспечить непрерывность функционирования бизнеса) в целях ликвидации последствий таких атак.

Список литературы

1. TMT Консалтинг. Отчет: «Информатизация в банковской сфере, 2021». 2022. – 3 с.
2. ЦБ рассказал о потерях банков из-за хакерских атак в 2022 году. URL: https://www.vedomosti.ru/finance/articles/2023/02/22/964073-tsb-rasskazal-o-poteryah-bankov-iz-za-hakerskih-atak (дата обращения: 17.09.2023).
3. Positive Technologies: информация из финорганизаций стала утекать чаще, чем средства. URL: https://www.kommersant.ru/amp/5666246 (дата обращения: 18.09.2023).
4. В 2023 целью хакеров станет не только финансовая, но и политическая выгода.URL: https://rg.ru/amp/2023/02/28/v-2023-celiu-hakerov-stanet-ne-tolko-finansovaia-no-i-politicheskaia-vygoda.html (дата обращения: 17.09.2023).
5. IBM Security. Cost of a Data Breach Report 2023. 2023. – 13 с.
6. Количество утечек данных в финансовом секторе РФ выросло на 71%. URL: https://www.infowatch.ru/company/presscenter/news/kolichestvo-utechek-dannykh-v-finansovom-sektore-rf-vyroslo-na-71-protsent (дата обращения: 17.09.2023).
7. Types of cyberthreats. URL: https://www.ibm.com/blog/types-of-cyberthreats/ (дата обращения: 19.09.2023).

УДК 004.056

М.А. УТЕНКОВА, Е.А. МАКСИМОВА
МИРЭА – Российский технологический университет, Москва

ВЫЯВЛЕНИЕ НАИБОЛЕЕ РЕЗУЛЬТАТИВНОЙ ГРУППЫ ФАКТОРОВ ПРИ ВЕДЕНИИ ГИБРИДНОЙ ВОЙНЫ

Цель исследования: выявление наиболее значимой составляющей гибридной войны, а именно одного из трех типов войн, успешное ведение действий в рамках которого приведет к наибольшей результативности в гибридной войне. Проведен ряд экспериментов с использованием теоретико-множественной и нечеткой модели гибридной войны как крайней формы информационного противоборства. Результаты экспериментов показали, что наибольший вклад в победу при ведении гибридной войны вносят действия в рамках информационной войны.

Развитие цифровых и информационных технологий и их повсеместное внедрение в жизни людей повлияло на появление нового вида конфликта – информационного противоборства. Крайней формой информационного противоборства в разных источниках [1, 2] указывают информационную войну, кибервойну и гибридную войну. При этом гибридная война включает в себя элементы классической войны, информационной войны и кибервойны.

Для достижения цели исследования были разработаны две модели: теоретико-множественной модели отношений между множествами составляющих разных видов войн (рис. 1) и нечеткая модель реализации гибридной войны. Первая модель необходима для разграничения, к какому типу войны какие концепты относятся, а вторая – для оценки влияния одного концепта на другой. Проверка значимости каждой составляющей гибридной войны осуществляется путем проведения экспериментального исследования. В рамках каждого эксперимента значения концептов, в рамках выбранного типа войны и относящиеся к одной из сторон конфликта (атакующей или обороняющейся), на нечеткой модели принимают максимальное положительное значение «1». При этом одновременно это выполняется сразу к двум различным группам концептов: первая для атакующей стороны, вторая для обороняющейся. Результаты представлены в табл. 1. Всего существует 6 комбинаций:

1. Атака: классическая война, оборона: информационная война;
2. Атака: классическая война, оборона: кибервойна;
3. Атака: информационная война, оборона: классическая война;
4. Атака: информационная война, оборона: кибервойна;

5. Атака: кибервойна, оборона: классическая война;
6. Атака: кибервойна, оборона: информационная война.

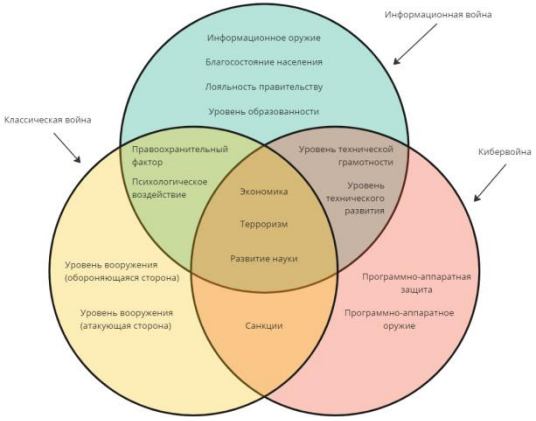

Рис. 1. Визуализация теоретико-множественной модели отношений между множествами элементов разных видов войн ©

Таблица 1. Результаты эксперимента по выявлению эффективности ведения войн в случае различных сильных сторон противников

Номер комбинации	Гибридная война	Информационная война	Классическая война	Кибервойна
1	0	-0,6	0,09	-0,2
2	0,01	0,03	0,11	-0,06
3	0,02	0,15	-0,07	0,13
4	0,02	0,16	0,01	-0,06
5	0	-0,02	-0,09	0,09
6	-0,1	-0,9	-0,3	0,08

При анализе результатов выявлено, что действия в рамках информационной войны имеют наибольшую значимость при ведении гибридной войны. Поэтому при разработке стратегии развития концептов предпочтительнее вкладывать силы в относящиеся к информационной войне, являющейся крайней формой информационного противоборства.

Список литературы

1. Сержантов А.В. Трансформация содержания войны: от прошлого к настоящему - технологии «гибридных» войн / А. В. Сержантов, А. В. Смоловый, А. В. Долгополов // Военная мысль. – 2021. – № 2. – С. 20–27. – EDN YICWQP.

2. Комлева Н.А. Гибридная война: сущность и специфика / Н. А. Комлева // – 2017. – Т. 12, № 3(167). – С. 128–137. – EDN ZRQKVP.

УДК 004.056

Д.А. САЯКОВ, Г.О. КРЫЛОВ, В.А. РЫЧКОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕХАНИЗМОВ ЗАЩИТЫ НАЦИОНАЛЬНОЙ ЦИФРОВОЙ ВАЛЮТЫ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном информационном обществе развитие технологий приводит к возникновению новых форм валюты – цифровых валют. Однако, наряду с ее преимуществами, цифровая валюта сталкивается с угрозами информационной безопасности. В данном докладе рассмотрена необходимость и возможные подходы к защите национальной цифровой валюты в сфере информационной безопасности.

Современная цифровая трансформация приводит к постоянному развитию различных сфер деятельности, включая банковскую систему и денежные операции. В последние годы интерес к криптовалютам и блокчейн-технологии значительно вырос, и все больше стран рассматривают вопрос о создании национальной цифровой валюты, в том числе из-за ее потенциальной экономической эффективности и удобства использования. Но есть определенные проблемы и риски, связанные с информационной безопасностью. В связи с этим, важно исследовать и разработать механизмы по снижению рисков реализации угроз, связанные с цифровыми транзакциями и финансовыми операциями.

Одним из главных вопросов является защита от несанкционированных транзакций или/и несанкционированный доступ к данным пользователей. Но также с развитием области квантовых компьютеров требуется разработать меры по криптографической защите, которые обеспечат безопасность цифровых подписей, шифрования данных и аутентификации пользователей.

Если защитой цифровой валюты и аккаунтов пользователей является задачей криптографических средств защиты, то остается уязвимое место это атаки человек по середине, DoS и DDoS атаки против которых важно установить механизмы контроля и мониторинга для обнаружения и предотвращения финансовых мошенничеств и отмывание денег. Это может включать в себя разработку аналитических инструментов и внедрение искусственного интеллекта для анализа и сравнения финансовых операций, а также выявления подозрительных транзакций.

Необходимо разработать механизмы безопасного хранения и передачи цифровых активов, а также защиту от утери или кражи средств пользователей.

Одной из лучших практик, которые многие страны применяют, является использование технологии блокчейн. Блокчейн представляет собой децентрализованную систему хранения данных, которая обеспечивает непрерывность, безопасность и прозрачность транзакций. Модели блокчейн-технологии могут быть использованы для создания и обслуживания цифровой валюты [1].

Однако существуют и неудачные примеры реализации национальной цифровой валюты, в основном такая проблема связана с недоверием со стороны жителей к новой форме денег, вместе с этим коррупция и экономический кризис.

Успехом зарубежного опыта является Китайский электронный юань или же e-CNY. Она уже успешно внедрена в торговлю и платежи в различных секторах экономики страны, так как Китай уделяет большое внимание безопасности, чтобы предотвратить мошенничество и взломы [2]. Например, голландский банк разработал специальные физические устройства, которые требуют аутентификации для осуществления транзакций. Это значительно повышает безопасность и предотвращает несанкционированный доступ к цифровой валюте.

В результате предлагается использование механизмов защиты национальной цифровой валюты включающие в себя обучение пользователей правильному и безопасному использованию цифровой валюты. Для этого могут проводиться образовательные программы и курсы, которые помогут пользователям избегать финансовых рисков и атак.

Список литературы

1. Саяков, Д.А. Особенности развития цифровой валюты и перспективные применения в Кыргызской республике. Проблемы автоматики и управления, 2023 (1), с. 96–105. http://pau.imash.kg/index.php/pau/article/view/404 (дата обращения: 14.09.2023).

2. Цифровой юань. - URL: https://www.china-briefing.com/news/china-launches-digital-yuan-app-what-you-need-to-know/ (дата обращения: 14.09.2023).

УДК 004.056

К.Д. НАУМОВА, В.Ю. РАДЫГИН, В.А. РЫЧКОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПОСТРОЕНИЕ ТИПОЛОГИИ СОВРЕМЕННЫХ АТАК, ОСНОВАННЫХ НА МЕТОДАХ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ПРИМЕНЯЕМЫХ В ОТНОШЕНИИ ЮРИДИЧЕСКИХ И ФИЗИЧЕСКИХ ЛИЦ В РФ

В работе проведен анализ и выявлены недостатки существующих методик классификации атак с использованием социальной инженерии. Цель работы заключается в классификации последовательностей атак, основанных на методах социальной инженерии, для последующего возможного определения уровня защищенности от данных атак в РФ. В результате предложена новая типология современных атак с использованием социальной инженерии, применяемых в отношении юридических и физических лиц. Типология основана на результатах предыдущих исследований и поэтапно отражает структуру рассматриваемых атак, способных нанести урон финансовому сектору РФ.

В информационной безопасности социальная инженерия подразумевает собой психологическое манипулирование людьми с целью получения конфиденциальной информации, совершения незаконных операций или получения доступа к ресурсу с ограниченным доступом. На сегодняшний день атаки с использованием социальной инженерии затрагивают как физических, так и юридических лиц, включая финансово-экономический сектор страны.

Существует множество различных классификаций методов социальной инженерии. Наиболее частым считается подход к рассмотрению атак социальной инженерии, происходящих либо со стороны непосредственно атакующего, либо атакующего, использующего некоторую среду передачи и получения данных, например посредством телефонного разговора или взаимодействия с жертвой в интернете. Каждый из подходов в свою очередь подразделяется на методы, которыми оперирует атакующий для получения той или иной информации. При проведении анализа построения классификаций атак в предыдущих исследованиях [1-4], выявлена их недостаточная структурированность, размытость представления конкретики различных методов атак и отсутствие последовательностей этапов воздействия на атакуемого. Подтверждено, что для выявления уровня защищенности от рассматриваемых атак социальной инженерии в РФ необходимо составить типологию последовательностей этапов – от выбора атакуемого, которым

может быть как физическое, так и юридическое лицо, до конечного варианта воздействия на жертву.

В результате предложена новая типология атак, основанных на методах социальной инженерии и объединенных в единую структуру с общими особенностями. В типологии отражен спектр последовательностей возможных атак с использованием социальной инженерии. Среди этапов выделяются: распространение атаки, взаимодействие (коммуникация) с атакуемым, вид психологического манипулирования атакуемым и конечное воздействие на атакуемого. В зависимости от поставленной цели и реализованных этапов злоумышленник получает от атакуемого информацию ограниченного доступа, денежный платеж, возможность нарушить конфиденциальность, целостность или доступность полученной информации через электронный ресурс, физическим путем или через вредоносное ПО. Выявлены различия в этапах проведения атак с использованием социальной инженерии при воздействии на юридических и физических лиц. Таким образом, представленная типология не только поможет в определении уровня защищенности для разных сфер РФ, но и будет полезна в выявлении новых актуальных мошеннических схем и в способах реагирования и защиты от них.

Список литературы

1. Salahdine F., Kaabouch N. Social engineering attacks: A survey //Future internet. – 2019. – Т. 11. – №. 4. – С. 89.
2. Heartfield R., Loukas G. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks //ACM Computing Surveys (CSUR). – 2015. – Т. 48. – №. 3. – С. 1–39.
3. Krombholz K. et al. Advanced social engineering attacks //Journal of Information Security and applications. – 2015. – Т. 22. – С. 113–122.
4. Ivaturi K., Janczewski L. A taxonomy for social engineering attacks. – 2011.

УДК 004.056

А.А. КОРЧАГИН, П.Ю. ЗЮКИН, Е.Е. ЛЕВТЕРОВ,
В.А. РЫЧКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

БЕЗОПАСНОСТЬ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

В работе проведен анализ роста мирового рынка видеоконференцсвязи в связи с началом пандемии COVID-19, выявлены преимущества использования систем видеоконференцсвязи в органах государственной власти Российской Федерации (далее – ОГВ РФ) и основные проблемы при их проектировании, внедрении и эксплуатации. Целью работы является анализ типовых уязвимостей, построение модели угроз и рассмотрение типовой модели потенциальных нарушителей для дальнейшего определения требований к системам защиты проектируемых систем видеоконференцсвязи и модернизируемых в процессе импортозамещения.

Значительный рост числа видеоконференций в мире за последние годы связан прежде всего с началом пандемии COVID-19 в 2020 г., введением карантина и появлением связанных с ним различного рода ограничений на личные встречи.

Так, в первые три месяца 2020 г. акции американской компании Zoom выросли на 30% [1].

В 2021 г. рост международного рынка видеоконференцсвязи составил 20% [2]. Опробовав использование в своей работе систем видеоконференцсвязи, компании не собираются от них отказываться. Так, в 2022 г. мировой рост рынка составил 13% [3]. Снижение темпов роста связаны, прежде всего, со снятием карантинных ограничений. Схожая картина характерна и для российского рынка.

В этот же период произошел рост числа пользователей видеоконференций в органах государственной власти. Руководители всех звеньев, даже наиболее скептически настроенные, во время пандемии стали проводить служебные совещания, используя видеоформат.

Использование систем видеоконференцсвязи в органах государственной власти позволяет:

– оперативно реагировать на чрезвычайные происшествия,

– сократить расходы на командировки,

– более эффективно использовать человеческие ресурсы за счет сокращения времени в дороге на совещания и назад;

– улучшить межведомственное взаимодействие.

При всех положительных сторонах использования систем видеоконференцсвязи еще на стадии проектирования и внедрения в органы государственной власти сталкиваются с рядом проблем:

1. Основная часть существующих систем видеоконференцсвязи построена на базе иностранного оборудования, в частности продукции компаний Cisco и Polycom, которые заявили о своем уходе с российского рынка в 2022 г.

2. Наличие в сетях ОГВ РФ сведений ограниченного доступа. При этом различные министерства и ведомства не могут сопрягать свои сети видеоконференцсвязи между собой из-за невозможности выполнения требований нормативной документации.

3. Установлен запрет на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд [4, 5].

В результате работы были рассмотрены основные проблемы систем видеоконференцсвязи ОГВ РФ при разработке, внедрении и модернизации в рамках проектов по импортозамещению. Рассмотрены типовые уязвимости систем видеоконференцсвязи, построена модель потенциального нарушителя информационных систем с учетом опыта субъектов критической информационной инфраструктуры и разработана типовая модель угроз информационной безопасности систем видеоконференцсвязи ОГВ РФ, которые могут содержать персональные данные участников видеоконференции и иную охраняемую государством информацию.

Список литературы

1. Статистика роста популярности видеочатов и сервисов видеосвязи за 2020 год. https://www.cnews.ru/news/line/2021-02-09_statistika_rosta_populyarnosti

2. Коронавирус помог популярности видеоконференций https://www.kommersant.ru/doc/4277265

3. Рынок ВКС в России и мире: итоги 2022 года и перспективы 2023-го https://www.cnews.ru/reviews/videokonferentssvyaz_2023/articles/rossijskie_proizvoditeli_vks_zahvatyvayut

4. Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

5. Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

Направление

Проблемы информационной безопасности в системе Высшей школы

Руководитель секции – Толстой А.И. к.т.н., доцент,

и.о. заведующего кафедрой №44

УДК 004.056

П.В. РЕВЕНКОВ
Финансовый университет при Правительстве Российской Федерации, Москва

НОВЫЕ КОМПЕТЕНЦИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОГО БАНКИНГА

Цифровой банкинг сегодня является одним из самых востребованных способов оказания банковских услуг. Наряду со своими удобствами, он значительно расширил профили типичных банковских рисков и предъявил новые требования к специалистам надзорных подразделений Банка России, участвующих в контроле за обеспечением информационной безопасности.

Очевидной тенденцией нескольких последних лет становится развитие принципиально новых технологий банковского обслуживания клиентов. Наиболее динамично развивающимися являются технологии цифрового банкинга, основу которых составляют системы дистанционного банковского обслуживания (ДБО) [1].

Использование систем ДБО дает ряд преимуществ:

- существенно экономится время за счет исключения необходимости посещать банк лично;
- клиент имеет возможность 24 часа в сутки контролировать собственные счета и оперативно реагировать на изменения ситуации на финансовых рынках;
- клиент может отслеживать операции с банковскими картами, поскольку доступ к работе с системой не зависит от его местонахождения (достаточно иметь устройство с установленным web-приложением и доступ к интернету).

Очевидно, что новая реальность и вопросы безопасности, с которыми вынуждены сталкиваться организации кредитно-финансовой сферы (ОКФС), и их клиенты при использовании цифрового банкинга требует модернизации, а в ряде случаев и значительного пересмотра процедур мониторинга и парирования рисков, соответствующей организации процедур внутреннего контроля и квалификации специалистов службы внутреннего контроля.

Аналогичные требования предъявляются и к сотрудникам надзорных подразделений Банка России, непосредственно участвующих в подготовке нормативных документов (на базе которых разрабатываются методики

проведения инспекционных проверок), а также осуществляющих мероприятия по дистанционному и контактному надзору в условиях распространения цифрового банкинга.

Далее перечислим, что должен знать сотрудник надзорного подразделения Банка России в области обеспечения информационной безопасности (ИБ) в условиях применения цифрового банкинга:

- основы банковского, страхового дела и рынка ценных бумаг, принципы обеспечения ИБ, основные банковские автоматизированные системы (БАС), включая системы ДБО;
- нормативные и методические документы по тематике банковского, страхового дела и рынка ценных бумаг, порядок обеспечения ИБ в ОКФС, включая требования отечественных и зарубежных стандартов по ИБ;
- внутренние регламенты взаимодействия надзорных подразделений Банка России;
- состав и назначение форм отчетности, данные из автоматизированной системы обработки инцидентов Банка России (АСОИ ФинЦЕРТ), основные виды атак на БАС ОКФС и их клиентов.

И, что должен уметь такой сотрудник:

- проводить проверки и киберучения в ОКФС по вопросам обеспечения ИБ;
- выявлять нарушения и недостатки в обеспечении ИБ в ОКФС в соответствии с нормативными и методическими документами по данной тематике (включая требования отечественных и зарубежных стандартов по ИБ);
- составлять схемы информационного контура ОКФС (в том числе в условиях применения систем ДБО) и выявлять точки концентрации рисков;
- составлять в установленные сроки акт по результатам проверки ОКФС и своевременно отвечать на возражения по выявленным нарушениям.

Добавим, что представленные требования непрерывно расширяются по мере развития цифрового банкинга и дистанционных услуг для клиентов ОКФС. Это свою очередь требует постоянного повышения квалификации специалистов надзорных подразделений, участвующих в контроле за обеспечением ИБ в условиях применения цифрового банкинга.

Список литературы

1. Кибербезопасность в условиях электронного банкинга: Практическое пособие / Под ред. П.В. Ревенкова. – М.: Прометей. 2020. – 522 с.

УДК 004.056

Н.Г. МИЛОСЛАВСКАЯ, А.И. ТОЛСТОЙ
Национальный исследовательский ядерный университет «МИФИ», Москва

ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОДГОТОВКИ МАГИСТРОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Рассматриваются вопросы, посвящённые подготовки профессионалов в актуальной в настоящее время области, относящейся к кибербезопасности. 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 «Обеспечение кибербезопасности и киберустойчивости информационных объектов» (направление 10.04.01).

Начиная примерно с конца 90-х годов прошлого века, в англоязычной научной и образовательной среде началось активное использование термина «кибербезопасность» (КБ) [1]. Ведущие зарубежные страны увидели в этом новую содержательную сущность в области национальной и международной безопасности [2]. В РФ только после включения технологии КБ в Перечень приоритетных технологический направлений ОПК РФ, утвержденный Правительством РФ (на основании Указа Президента РФ 20.07.2016 года № 347) стала наблюдаться активность на уровне дискуссионного обсуждения проблематики, связанной с КБ [2]. Имеются подходы, основанные на утверждении уникальности области КБ [3], что должно быть учтено и при подготовке профессионалов.

Определение компетентностных требований к профессионалам в области КБ можно осуществить с использованием положений профессионального стандарта (ПС) ПС 06.053 «Специалист по информационной безопасности в кредитно-финансовой сфере» [4], который сформулировал для профессионалов трудовые функции, трудовые действия и рекомендации к их знаниям и умениям, имеющие отношения к КБ и киберустойчивости (КУ).

Анализ положений ПС 06.053, а также опыт реализации в НИЯУ МИФИ магистерской программы «Обеспечение непрерывности и ИБ бизнеса» позволил определить набор профессиональных компетенций

(ПК), предполагающих, что выпускник магистерской программы должен быть способен:

- проводить оценку рисков КБ с целью обеспечения формирования и функционирования эффективной системы обеспечения КБ и системы обеспечения КУ объектов информатизации – ПК2;
- участвовать в проектировании, эксплуатации и совершенствовании систем управления инцидентами КБ и КУ, оценки КБ и КУ, управления КБ и КУ, обеспечения КБ и КУ информационных объектов.

ПК были положены в основу разработки Основной образовательной программы (ООП) магистратуры по направлению 10.04.01 ИБ «Обеспечение КБ и КУ информационных объектов», 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.

Магистерская программа предполагает реализацию по двум траекториям, связанными с обеспечение КБ и КУ информационных объектов, относящихся к организациям финансового сектора и организации атомной отрасли.

ООП прошла экспертизу в организациях, потенциальных потребителей выпускников, а также общественное обсуждение среди представителей образовательных учреждений, ведущих подготовку специалистов по направлению 10.00.00 ИБ.

Список литературы

1. Definition of Cybersecurity – Gaps and overlaps in standardization. - European Union Agency For Network And Information Security, v1.0, December 2015. URL: https:// www.enisa.europa.eu. ISBN 978-92-9204-155-7. DOI 10.2824/4069.

2. Добродеев А.Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века// Вопросы кибербезопасности, 2021, № 4(44). С. 61–72.

3. Зегжда Д.П. Теоретические основы киберустойчивости и практика прогностической защиты от кибератак. – СПб.: ПОЛИТЕХ-ПРЕСС, 2022. – 490 с.

4. 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).

УДК 004.056

Г.П. ГАВДАН, В.Г. ИВАНЕНКО
Национальный исследовательский ядерный университет «МИФИ», Москва

ПОДГОТОВКА ДЛЯ ВЫСШЕЙ ШКОЛЫ КАДРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализируются вопросы совершенствования Высшей школы в аспекте информационной безопасности (ИБ), которые не теряют своей актуальности и сегодня. Так, одним из приоритетных направлений продолжает оставаться дальнейшее развитие высшего образования (ВО) и совершенствование подготовки кадров. Предметом исследования является Высшая школа (ВШ) в условиях существования различных угроз безопасности информационной. Проведённый анализ научных публикаций и других источников по теме исследования показал, что в данной области существует проблема. По результатам работы установлено, что ВШ ещё имеются незащищенные в данной области объекты, что требует дополнительного внимания со стороны представителей Министерства науки и высшего образования и контроля государственных служб, таких как ФСТЭК России, ФСБ России и др. органов власти.

Введение

Приоритетным направлением Высшей школы в аспекте информационной безопасности (ИБ) остаётся совершенствование подготовки кадров, где вузам отведена особая роль в решении некоторых задач. Проблема обеспечения ИБ может рассматриваться в трёх аспектах: *техническом*, связанном с созданием защищённых средств хранения и обработки информации и их программного обеспечения; *кадровом*, предусматривающем подготовку и расстановку кадров по ИБ; *организационно-правовом*, устанавливающем систему законов, правил, норм, организацию функционирования информационной среды [1]. Подготовка кадров в России остаётся достаточно сложной и важной задачей, которая тем не менее решается. Так, 11 августа 2023 г. Президентом Российской Федерации было проведено оперативное совещание с Советом безопасности по ИБ, где поднимались и кадровые вопросы [2]. На совещании В. Путиным было предложено обсудить актуальные вопросы ИБ.

Поиск и обучение талантов для подготовки кадров в области ИБ

Пентагоном опубликован «План реализации стратегии кибертрудовых ресурсов на 2023–2027 гг.» [3]. Направленность данного Плана реализации стратегии Cyber Workforce Focus (CWF) представлена в [3] (Fig. 1: CWF Strategy Implementation Plan Focus, page 8). В стратегии обозначены такие проблемные области, как отсутствие общих критериев требований к кибернетическим кадрам; потребность в отборе кандидатов на основе

навыков для заполнения пробелов в возможностях; нехватка программ развития навыков; выгорание [3], что привело к четырём «столпам» стратегии и Плана реализации, обозначенных как выявление, набор, развитие и удержание. Поиск и обучение талантов, должен охватывать детские сады и школы. Детей и подростков следует увлечь технологиям, инженерией, математикой и кибернетикой [4].

Программа предлагает частное и государственное партнерство. Устранение дефицита рабочей силы в киберпространстве потребует меры по ускорению удержания и найма. По словам Горака, это будет применяться как к военным, так и к гражданским кибербезопасникам, а также работникам по контракту, причем каждая из сфер включает около 75 000 должностей [4].

В настоящее время большинство специализированных кафедр вузов реализует основные образовательные программы (ООП) высшего образования, в меньшей степени уделяя внимание программам повышения квалификации (ПК) и профессиональной переподготовки (ПП) персонала по ИБ. На наш взгляд, сочетание разных ООП для специалистов различного уровня позволит в целом повысить качество обучения по основным ООП, так как опирается на опыт привлекаемых специалистов-практиков и конкретную практическую их деятельность.

Заключение

Необходимо обеспечить поиск и обучение талантов. Программа должна обеспечить частное и государственное партнерство. Устранение дефицита рабочей силы в киберпространстве потребует мер по ускорению найма и его удержания (как к военным, так и к гражданским кибербезопасникам, а также работникам по контракту). Данное развитие кадрового потенциала в области обеспечения ИБ и применения (четвертое направление) информационных технологий может решаться как самостоятельно, так и путем реализации программ в образовательных учреждениях.

Список литературы

1. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. Курс лекц. Учеб. пособ. для вузов. – М.: Горячая линия – Телеком, 2019. – 314 с.

2. РИА НОВОСТИ «В. Путин провел оперативное совещание с членами Совбеза» (15:26 11.08.2023) URL: https://ria.ru/20230811/sovbez-1889553959.html?utm_source =yxnews&utm _medium=desktop (дата обращения: 19.08.2023).

3. «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://media.defense.gov/2023/Aug/03/2003274088/-1/-1/1/2023-2027-DOD-CYBER-WORKFORCE-STRATEGY-IMPLEMENTATION-PLAN.PDF (дата обращения: 19.08.2023).

4. «США не хватает сотен тысяч специалистов в области кибербеза». Эшелон в телеграм канале. URL: https://t.me/EchelonEyes/1834 (дата обращения: 19.08.2023).

УДК 004.056

Г.П. ГАВДАН, Д.А. ДЯТЛОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

МАГИСТЕРСКАЯ ПРОГРАММА «ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ» И ЕЁ РЕАЛИЗАЦИЯ В НИЯУ МИФИ

Анализируется опыт кафедры «Стратегические информационные исследования» НИЯУ МИФИ по реализации магистерской программы «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» направления 10.04.01 «Информационная безопасность», а именно особенности её реализации (проблемы). Рассмотрены проблемы приёмной компании при наборе групп и описаны особенности подготовки магистрантов по данной программе.

Введение

Федеральный закон (ФЗ) от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» регулирующий отношения в области обеспечения безопасности критической информационной инфраструктуры (КИИ) послужил основой для разработки и реализации в (НИЯУ МИФИ) магистерской программы (программы) «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» (ОБЗОКИИ) по направлению 10.04.01 «Информационная безопасность» (ИБ). Взаимосвязь образовательных и профессиональных стандартов (ОС) может быть использована в качестве основы совершенствования и развития системы ОС для перехода к новой системе оценки квалификации, представляя профстандарты как отражение взглядов и потребностей работодателей [1]. Обучение по программе направлено на удовлетворение потребности в кадрах для обеспечения ИБ субъектов КИИ в соответствии с Указом Президента РФ от 1.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Выпускники программы «ОБЗОКИИ» должны овладеть за 2 года необходимыми профессиональными компетенциями, для чего наиболее подготовленными являются специалисты и бакалавры по ИБ [2]. Проблемой является то, что ФЗ № 273-ФЗ «Об образовании в РФ» даёт право на поступление на программу [3] бакалаврам и специалистам с любым высшим образованием (ВО), не относящимся к ИБ [4].

Особенности реализации магистерской программы «ОБЗОКИИ»

Основной целью магистерской программы ОБЗОКИИ (по удовлетворению потребности в кадрах для обеспечения ИБ субъектов

КИИ в соответствии с Указом Президента РФ от 01.05.2022 №250) является получение выпускниками компетенций (универсальных, общепрофессиональных, профессиональных и специальных), необходимых для выполнения должностных обязанностей, связанных с обеспечением безопасности ЗОКИИ в РФ [4].

Многие профильные дисциплины программы ОБЗОКИИ, содержащие к тому же сведения ограниченного доступа, не содержащие сведения, составляющие государственную тайну, требуют от студентов наличия полученных ранее компетенций (знать, уметь, владеть) по высшей математике, общей физике и по теоретической и практической ИБ.

Например, сложно осваивать с «нуля» такие профильные дисциплины, как:

– Основы кибербезопасности атомной энергетики;

– Основы информационной безопасности критически важных объектов;

– Основы категорирования значимых объектов КИИ;

– Методы и средства контроля эффективности ЗИ от НСД;

– Методы выявления недекларированных возможностей в радиоэлектронной аппаратуре;

– Системы безопасности значимых объектов критической инфраструктуры.

Это требует использование дополнительного людского ресурса и времени.

Заключение

Проблему с отсутствием у поступающих абитуриентов необходимых компетенций по общей физике, высшей математике и по теоретической и практической ИБ можно решить, например, включив в рабочую учебную программу или *дополнительный семестр* (для студентов, которые ими не обладают), или *факультативные занятия* для получения необходимых знаний, что в последствии даст им возможность обучаться наравне со студентами с профильным образованием.

Список литературы

1. Мельников, Дмитрий А. и др. К вопросу о цели и задачах национальной образовательной инициативы США в области кибербезопасности. Безопасность информационных технологий, [S.l.], v. 25, n. 2, p. 23-37, май 2018. ISSN 2074-7136, (дата обращения: 09.09.2023). Режим доступа: URL: https://bit.spels.ru/index.php/bit/article/view/1107/1096, doi: http://dx.doi.org/10.26583/bit.2018.2.02.

2. Образовательный стандарт (3++, высшее образование) НИЯУ МИФИ по направлению подготовки 10.04.01 «Информационная безопасность» (уровень магистратуры). Режим доступа: URL: https://mephi.ru/sveden/eduStandarts (дата обращения: 08.09.2023).

3. Марченко, Анатолий В. и др. Анализ состояния системы подготовки специалистов в области информационной безопасности. Безопасность информационных технологий, [S.l.], v. 25, n. 2, p. 6-22, май 2018. ISSN 2074-7136. Режим доступа: URL: https://bit.spels.ru/index.php/bit/article/view/1106/1095. doi: http://dx.doi.org/10.26583/bit.2018.2.01 (дата обращения: 08.09.2023).

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. Режим доступа: URL: https://bit.spels.ru/index.php/bit/article/view/1231/1164, doi: http://dx.doi.org/10.26583/bit.2019.4.04 (дата обращения: 08.09.2023).

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

ВЫЯВЛЕНИЕ ДЕВИАНТНОГО ПОВЕДЕНИЯ ПОДРОСТКОВ МЕТОДОМ КЛАСТЕРНОГО АНАЛИЗА

Работа посвящена проблеме скулшутинга в учебных заведениях. Обосновывается актуальность данной проблемы и необходимость применения превентивных мер. Выделены отличительные черты девиантных групп подростков. Рассмотрены текущие способы измерения тревожности и агрессивности. Отмечена неэффективность текущих подходов к их измерению. Для автоматизации процесса выявления девиантного поведения подростков и исключения субъективного фактора предложено использовать онлайн-профайлинг в комбинации с методами машинного обучения.

Введение

В современном мире человечество сталкивается с проблемами разного характера. Одной из них является проблема девиантного поведения подростков, которое проявляется агрессивностью, садизмом, воровством, лживостью, тревожностью, депрессией, целенаправленной изолированностью, попытками суицида, гиперобщительностью, виктимностью, фобиями, зависимостями, навязчивостями, которые могут приводить к шутингу в учебных заведениях. Лидером по количеству подобных преступлений является США – в среднем за год там происходит порядка150 преступлений подобного рода. За последние годы в Российской Федерации возросло число трагедий, связанных с шутингом в школах и университетах. Первый случай скулшутинга произошел в Москве в 2014 г. [1]. Для минимизации таких трагедий необходимы превентивные меры. Причины данного явления требуется определять с целью последующего устранения. Необходим способ для объективного определения подростков с отклонениями. Речь идет не только о подростках – потенциальных шутерах, но и тех, кто может иметь суицидальные мысли, а также тех, кто склонен к буллингу сверстников.

Текущий подход к решению проблемы.

Для определения потенциальной принадлежности обучающихся к группе с девиантным поведением используется метод оценки тревожности

и агрессивности. Существует множество методик их оценки, например, с помощью тестирования обучающихся [2].

Основной недостаток данного метода состоит в том, что полученные данные нельзя считать объективными, так как испытуемый может выбирать наиболее подходящие под нормы социума ответы. Наиболее точным является метод оценки тревожности и агрессивности психологом. По реакции обучающегося на вопросы, психолог оценивает тревожность и агрессивность подростка, начисляя условные баллы [3].

Однако, проблема в том, что определение психологом тревожности и агрессивности у каждого подростка образовательного учреждения попросту не представляется возможным из-за большого количества обучающихся и динамично меняющихся обстоятельств в жизни подростков.

Предлагаемое решение

В качестве мер для противодействия скулшутингу предлагается ведение индивидуальных карт обучающихся с девиантным поведением для определения потенциальных скулшутеров, а также проведение мониторинга социальных сетей с целью блокировки сообществ, пропагандирующих скулшутинг [4]. Но более действенным является объединение этих мер и составление профиля обучающихся. Таким образом, целесообразно проводить онлайн-профайлинг, который позволит обнаружить информацию, свидетельствующую о тревожности и агрессивности у обучающихся. Проведя анализ полученных данных с помощью методов машинного обучения, представляется возможным выделить обучающихся с девиациями. И далее с ними предметно начинают работать психологи.

Список литературы

1. Пиркина В.Г. Социально опасное поведение обучающихся как психолого-педагогическое явление //Мир науки. Педагогика и психология. – 2020. – Т. 8. – №. 6. – С. 82.

2. Барканова О.В. Методики диагностики эмоциональной сферы //Психологический практикум. Красноярск: Литера-Принт. – 2009. – С. 205–210.

3. Щербатых Ю.В. Методики диагностики тревоги и тревожности–сравнительная оценка //Вестник по педагогике и психологии Южной Сибири. – 2021. – №. 2. – С. 85–104. DOI: https://doi.org/10.24412/2303-9744-2021-2-85-104.

4. Бубнов С.В. Актуальные проблемы деятельности участкового уполномоченного полиции в противодействии скулшутингу //Вестник Московского университета МВД России. – 2022. – №. 4. – С. 41–45. https://doi.org/10.24412/2073-0454-2022-4-41-45.

УДК 004.056

В.Ю. СЕМИЛЕТКИН, К.Ф. ТОКАРЕВ, М.В. ВАНИН
Н.Г. МИЛОСЛАВСКАЯ
Национальный исследовательский ядерный университет «МИФИ», Москва

КАДРОВОЕ ОБЕСПЕЧЕНИЕ ТИПОВОГО ЦЕНТРА УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

Рассматриваются вопросы, посвящённые компетенциям персонала, входящего в Центр управления сетевой безопасностью (ЦУСБ). Целью работы является уточнение известных из профессиональных стандартов компетенций, а также трудовых умений, действий и знаний персонала. В результате актуализирован перечень умений специалистов по информационной безопасности в структурных подразделениях ЦУСБ.

В современных условиях, при учете быстро развивающихся технологий и постоянных угроз кибербезопасности, особое внимание уделяется организации работы ЦУСБ. Одной из ключевых проблем, которая поднимается в данной работе, является вопрос квалификации и количества необходимого персонала ЦУСБ. При этом стандарты в сфере информационной безопасности (ИБ) рассматривают специфику работы специалистов и их квалификацию не в полном объеме, так как не учитывают специфику работы в ЦУСБ.

Основная задача ЦУСБ – защита информации и информационных систем от различного рода угроз в информационно-телекоммуникационных сетях (ИТКС). В структуру ЦУСБ входит множество подсистем, включая подсистемы мониторинга событий ИБ, управления уязвимостями, управления инцидентами, а также защиты веб-приложений. Для обеспечения эффективного функционирования всех этих подсистем необходимо четкое разделение ответственности между сотрудниками.

В работе предлагается создание специализированных подразделений внутри ЦУСБ, таких как подразделение мониторинга событий ИБ, подразделение анализа инцидентов ИБ, подразделение администрирования и подразделение контроля защищенности. В каждом из этих подразделений предусмотрены различные роли: от руководителя до инженера. Такое разделение позволяет обеспечить высокую эффективность работы и быстрое реагирование на возникающие инциденты.

Работа акцентирует внимание на важности правильной организации режимов работы ЦУСБ. Выделяются три основных режима: штатный, технологическое обслуживание и аварийный. Каждый из режимов имеет свои особенности, и переход между ними требует особого внимания.

Что касается квалификации персонала, в работе подчеркивают необходимость наличия у специалистов высшего профессионального образования по направлению «Информационная безопасность». Кроме того, важным является их постоянное профессиональное обучение и переподготовка.

В заключении работы подчеркивается стратегическая важность создания и внедрения типового ЦУСБ для обеспечения ИБ организаций. Такие системы обеспечивают централизованное управление инцидентами, комплексное отслеживание и визуализацию текущей ситуации, что позволяет принимать обоснованные решения в области ИБ. При этом квалифицированный состав сотрудников с определенными функциональными обязанностями позволяет выполнять рабочие задачи, а также работу, связанную с мониторингом и обработкой событий и/или инцидентов ИБ более продуктивно и качественно. Ниже приведен фрагмент таблицы с функциональными обязанностями сотрудников ЦУСБ.

Роль	Выполняемые функции	Квалификация
Подразделение мониторинга событий		
Инженер по мониторингу событий	Мониторинг и анализ событий ИБ	- высшее образование в области ИБ или ИТ; - опыт работы с решениями класса SIEM

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. Профессиональный стандарт. Специалист по защите информации в автоматизированных системах Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

УДК 004.056

Д.В. МАЛЕНКОВ, Н.Г. МИЛОСЛАВСКАЯ
Национальный исследовательский ядерный университет «МИФИ», Москва

ИСПОЛЬЗОВАНИЕ ПЛАТФОРМЫ SECURITY VISION В УЧЕБНОМ ПРОЦЕССЕ НИЯУ МИФИ

Оценивается применимость платформы компании Security Vision для обучения магистрантов в области информационной безопасности, разрабатывая лабораторный практикум для практического опыта. Анализируются функции платформы и её интеграция в обучении, а также способности студентов анализировать и документировать инциденты, улучшая понимание мер защиты.

Исследуется применимость платформы с интегрированным модулем «Управление инцидентами» от компании Security Vision для обучения магистрантов НИЯУ МИФИ по направлению 10.04.01 «Информационная безопасность», принимая во внимание профессиональные стандарты 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях» для группы занятий «Инженеры по телекоммуникациям» и 06.033 «Специалист по защите информации в автоматизированных системах» для группы занятий «Специалисты по компьютерным сетям».

Цель работы заключается в определении применимости использования платформы от Security Vision с интегрированным модулем «Управление инцидентами» для создания лабораторного практикума, предназначенного для выработки практических навыков работы с подобными средствами обеспечения сетевой безопасности. В результате обучения по дисциплине «Центры управления сетевой безопасностью» магистранты приобретут опыт управления функционированием систем обеспечения защиты средств связи сетей электросвязи (СССЭ) и защиты от несанкционированного доступа (НСД), включая реагирование на нарушения и компьютерные атаки [1].

Актуальность работы подтверждается профессиональными стандартами 06.030 и 06.033, в которых учитываются современные требования к специалистам в области защиты информации в телекоммуникационных системах и сетях и к специалистам по защите информации в автоматизированных системах [2].

Исследование эффективности способов, средств и систем защиты СССЭ от НСД и поиска признаков компьютерных атак в сетях электросвязи достигается выполнением рабочего задания с

использованием платформы и её модулей для обнаружения и анализа признаков компьютерных атак, что способствует развитию аналитических навыков обучающихся. Они настраивают платформу, подключая коннекторы, создавая правила для сработки инцидентов информационной безопасности (ИБ) и настраивая так называемый модуль инцидентов ИБ.

Важной частью работы является анализ функциональных возможностей платформы Security Vision, интегрированной с модулем «Управление инцидентами» в контексте обучения магистрантов, специализирующихся в области защиты информации в телекоммуникационных системах и сетях. Платформа позволяет получить соответствующие теоретические знания в неразрывной связи с практическими навыками, что лучше всего достигается при разборе сценариев реальных инцидентов [3].

При использовании модуля «Управление инцидентами» обучающиеся учатся анализировать реальные типы инцидентов ИБ, а также выявлять уязвимости, которые способствовали их возникновению. Этот анализ помогает понять причины инцидентов ИБ и обоснованно выбрать меры по их предотвращению в будущем. Кроме этого магистранты учатся должны образом документировать инциденты ИБ, создавая отчеты с описанием произошедших событий, предпринятых действий и результатами их анализа.

Список литературы

1. Профстандарт: 06.030. Специалист по защите информации в телекоммуникационных системах и сетях. Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 536н [Электронный ресурс] // Classinform.ru [сайт]. [2022]. URL: https://classinform.ru/profstandarty/06.030-spetcialist-po-zashchite-informatcii-v-telekommunikatcionnykh-sistemakh-i-setiakh.html

2. Профстандарт: 06.033. Специалист по защите информации в автоматизированных системах. Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н [Электронный ресурс] // Classinform.ru [сайт]. [2022]. URL: https://classinform.ru/profstandarty/06.033-spetcialist-po-zashchite-informatcii-v-avtomatizirovannykh-sistemakh.html

3. Управление инцидентами ИБ (конспект лекции) [Электронный ресурс] // Securityvision.ru: [сайт]. [2022]. URL: https://www.securityvision.ru/blog/upravlenie-intsidentami-ib-konspekt-lektsii/?sphrase_id=5070

ИМЕННОЙ УКАЗАТЕЛЬ АВТОРОВ СТАТЕЙ

Всероссийская научно-техническая конференция
«Кибернетика и информационная безопасность»

«КИБ-2023»

Сборник научных трудов

Ответственный редактор И.М. Ядыкин

Подписано в печать 10.10.2023. Формат 60x84 1/16.
Печ. л. 10, 5. Уч.-изд. 10, 5. Тираж 150 экз.
Изд. №007-2. Заказ № 89

Национальный исследовательский ядерный университет «МИФИ»
Типография МИФИ
115409, Москва, Каширское ш. 31