ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Сборник материалов XV межрегиональной научно-практической конференции

Брянск
БГТУ
2023

Министерство науки и высшего образования Российской Федерации
Брянский государственный технический университет»

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ»

XV межрегиональная научно-практическая конференция
(Брянск, 28 апреля 2023 г.)

Сборник материалов и докладов

Под общей редакцией О. М. Голембиовской

Текстовое электронное издание

Брянск
БГТУ
2023

ISBN 978-5-907570-60-3

УДК 4.056
ББК 32.97
П74

Утверждено редакционно-издательским советом БГТУ

П74 **Информационная безопасность и защита персональных данных. Проблемы и пути их решения** : сборник материалов и докладов [Электронный ресурс] / под общей редакцией О. М. Голембиовской. – Брянск : БГТУ, 2023. – Режим доступа: https://www.tu-bryansk.ru/mainpage/nauka/konferentsii/sborniki-trudov-konferentsiy-provodimykh-bgtu, свободный . – Загл. с экрана.

Сборник подготовлен по материалам XV межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных. Проблемы и пути их решения», прошедшей 28 апреля 2023 года на базе ФГБОУ ВО «БГТУ» в г. Брянске.

Для студентов, аспирантов, занимающихся научно-исследовательской работой.

Текстовое электронное издание

Минимальные системные требования

- Браузеры: Google Chrome, Microsoft Edge, Mozilla Firefox, Opera
- Скорость подключения к информационно-телекоммуникационным сетям 1 мбит/с

Дополнительные настройки для чтения PDF в браузере: Google Chrome (требуется), Microsoft Edge (требуется), Mozilla Firefox (требуется), Opera (требуется)

Материалы публикуются в авторской редакции. Пунктуация и орфография авторов сохранены.

ISBN 978-5-907570-60-3

Научное издание

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ»

Сборник материалов и докладов
XV межрегиональной научно-практическойконференции

Брянск, 28 апреля 2023 г.

Под общей редакцией О. М. Голембиовской

Электронное текстовое издание

Сборник разработан с помощью программного обеспечения Microsoft Office Word, Adobe Acrobat Pro

Подписано к использованию 15.06.2023.
Объем издания – 2,68 Мб.
Гарнитура Times

Брянский государственный технический университет. 241035, Брянск, бульвар 50 лет Октября, 7.
Тел.: 58-82-49

Организационный комитет

- Сканцев В.М. – первый проректор, председатель оргкомитета;
- Рытов М.Ю. – заведующий кафедрой «Системы информационной безопасности», заместитель председателя оргкомитета;
- Еременко В.Т. – профессор кафедры «Информационная безопасность» Орловского государственного университета им. И.С.Тургенева (по согласованию);
- Громов Ю.Ю. - директор института автоматики и информационных технологий Тамбовского государственного технического университета;
- Голембиовская О.М. – доцент кафедры «Системы информационной безопасности»;
- Горлов А.П. – доцент кафедры «Системы информационной безопасности»;
- Шпичак С.А. – доцент кафедры «Системы информационной безопасности»;
- Шинаков К.Е. - доцент кафедры «Системы информационной безопасности»;
- Лексиков Е.В. – старший преподаватель кафедры «Системы информационной безопасности»;
- Захарова Л.И. – доцент кафедры «Гуманитарные и социальные дисциплины», ответственный секретарь конференции.

Содержание

Научная статья
УДК 001.891.57

Моделирование и его применение в лесной отрасли

Андрей Владимирович Акименко [1], Роман Юрьевич Медведев [2], Евгений Александрович Аникеев [3]✉
[1, 2, 3]Воронежский государственный лесотехнический университет имени Г.Ф. Морозова, Воронеж, Россия
[1]akime77@mail.ru, https://orcid.org/0009-0001-7516-593X
[2]medrom23@inbox.ru, https://orcid.org/
[3]eanikeev@gmail.com ✉, http://orcid.org/0000-0001-6114-9755

Аннотация. В статье оценивается важность моделирования, как метода исследования. Представлена обобщенная классификация моделей. Описаны их разновидности. Рассмотрены перспективы применения моделирования в различных областях лесного хозяйства.

Ключевые слова: модель, моделирование, лесное хозяйство.

Моделирование успешно практикуется во многих сферах человеческой деятельности: промышленность, сельское хозяйство, транспорт, образование, медицина и др. [3].

Под моделированием понимается изучение реальных объектов с помощью моделей.

Моделью (в широком смысле этого термина) является абстрактное представление какого-либо объекта или явления, предназначенное для его исследования.

К одной из наиболее важных характеристик модели следует отнести ее адекватность (степень соответствия реальной системе).

Модели, применяемые в практической деятельности, весьма многообразны. Различные авторы предлагают множество вариантов систематизации моделей, однако, создать их единую, исчерпывающую классификацию – задача непростая.

На рис. 1 приведена обобщенная классификация моделей по нескольким, наиболее существенным, на наш взгляд, признакам.

По области применения можно выделить множество видов моделей. В качестве примера приведем лишь некоторые из них.

Технические модели имитируют устройство и принцип действия различных технических систем. Они незаменимы в техническом конструировании.

Биологические модели являются искусственными аналогами объектов живой природы. Эти модели находят применение в научных исследованиях.

Социальные модели служат для изучения явлений, происходящих в обществе. Они используются в гуманитарных науках.

Экономические модели описывают различные экономические процессы. Примером экономической модели является бизнес-модель.

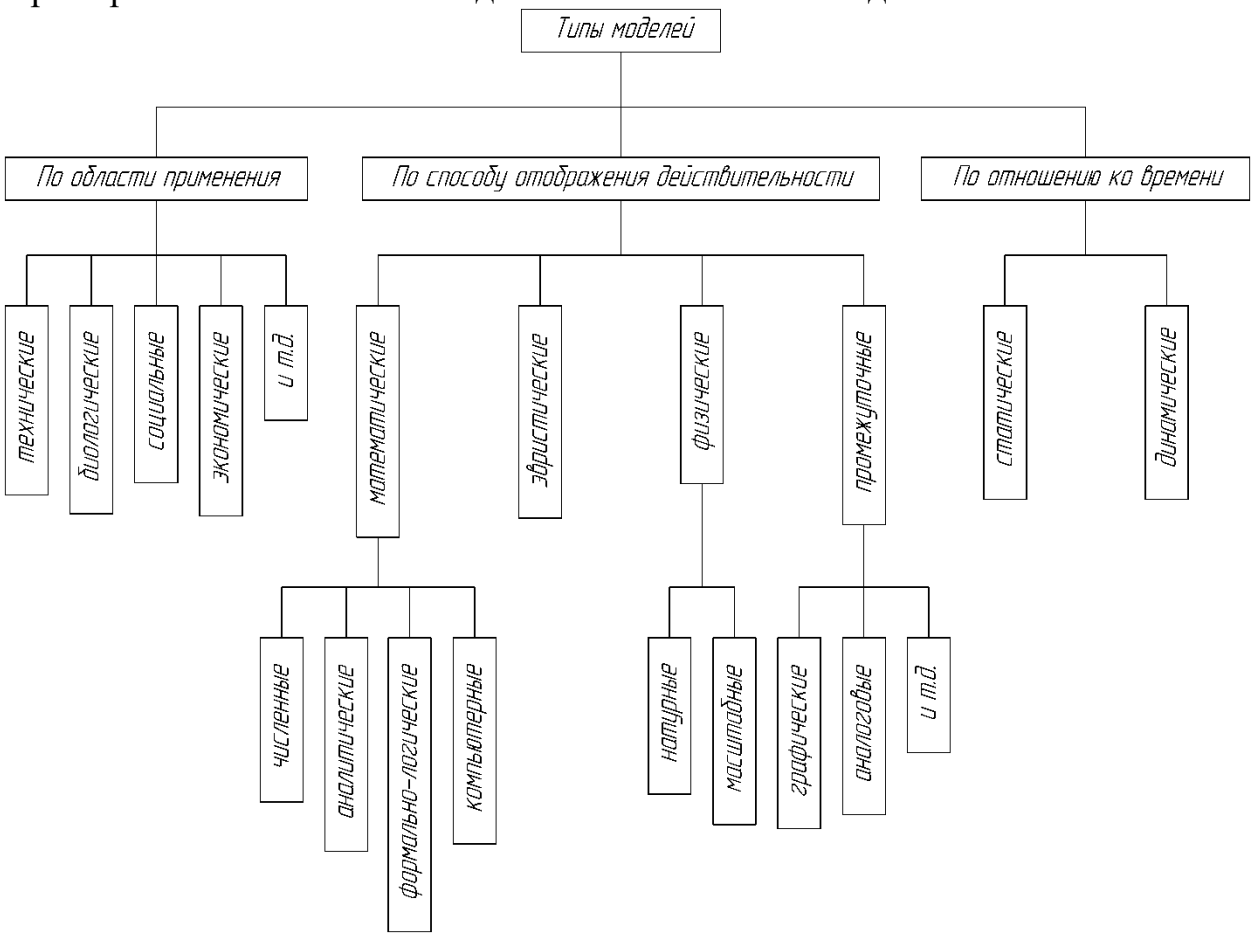

Рис. 1. Классификация моделей

По способу отображения действительности различают эвристические, физические, математические и промежуточные модели.

Эвристические модели – это образы, создаваемые, как правило, в человеческом воображении, и описываемые средствами естественного языка.

Недостатками эвристических моделей являются их субъективность и неоднозначность. Тем не менее, эвристическое моделирование играет не последнюю роль на начальных этапах проектирования или другой созидательной деятельности.

В различных областях знаний нашли широкое применение физические модели, имеющие одинаковую качественную природу с изучаемыми объектами.

Физическое моделирование играет важную роль в естественных и технических науках.

Предметом физического моделирования может быть как материальный объект (техническое устройство, живой организм), так и процесс (производственная технология, природное явление).

Основное достоинство физических моделей – их наглядность.

Разновидностью физической модели является макет – точная или приблизительная копия реального объекта, как правило, не обладающая полной

функциональностью оригинала. Обычно, макеты служат демонстрационным целям.

Физическая модель может быть выполнена в натуральную величину по отношению к оригиналу (натурная модель), или в масштабе (масштабная модель).

Математическая модель является абстрактным описанием рассматриваемой системы с использованием математических методов [1].

С помощью математических моделей можно описывать объекты или процессы, натурное моделирование которых невозможно или сопряжено с трудностями.

Математические модели имеют несколько разновидностей. Среди них следует выделить аналитические, численные, формально-логические, компьютерные модели.

Аналитические модели строятся на основе функциональных зависимостей. Они достаточно наглядны, но для их реализации часто требуются сложные зависимости.

Численные модели представляются в виде дискретных рядов чисел (таблиц). Они универсальны, эффективны при решении сложных задач, но менее наглядны, по сравнению с аналитическими моделями.

Формально-логические информационные модели создаются на формальном языке. В качестве примера может быть приведена модель формальной системы, состоящей из множества объектов, отношения между которыми подчиняются определенным аксиомам и правилам.

Компьютерная модель – тип математической модели, реализуемой с помощью ЭВМ.

Компьютерное моделирование возникло благодаря стремительному развитию информационных технологий и открыло новые возможности для научных исследований [2].

Промежуточная модель сочетает в себе свойства нескольких из вышеперечисленных типов моделей. К промежуточным моделям относятся графические, аналоговые и др.

Графическая модель имеет признаки эвристической и математической моделей, и представляет собой графическое изображение (рисунок, схему, чертеж и т.д.).

Аналоговая модель позволяет исследовать одно физическое явление на основе его сходства с другим явлением.

По отношению ко времени выделяют два типа моделей: статические и динамические.

Статическая модель служит для исследования объекта, состояние которого не изменяется с течением времени или рассматривается применительно к определенному моменту времени.

Динамическая модель отражает изменение исследуемого объекта во времени под действием внутренних и внешних факторов.

Лесной комплекс, как и другие отрасли народного хозяйства, является одной из перспективных сфер применения моделирования.

Моделирование в лесной отрасли можно подразделить на несколько направлений, каждое из которых охватывает определенную часть лесного комплекса. Рассмотрим наиболее актуальные из них (рис. 2).

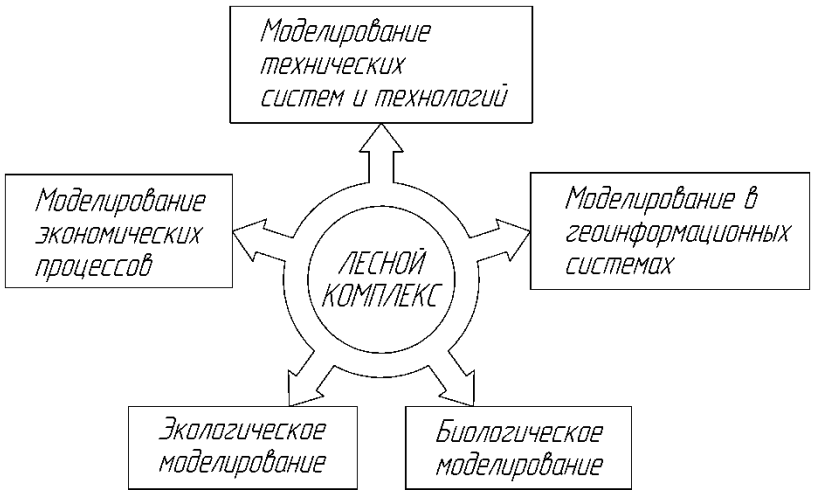

Рис. 2. Моделирование в лесном комплексе

1. Моделирование технических систем и технологий.

В лесном комплексе задействован широкий спектр машин, участвующих в различных технологических процессах. Оборудование для лесной отрасли динамично развивается и совершенствуется. Активно практикуется автоматизация производственных процессов и внедрение информационных технологий.

Как было отмечено выше, создание новых технических средств и технологий не представляется возможным без моделирования.

2. Моделирование экономических процессов.

Методы экономического моделирования, неоднократно упомянутого ранее, могут быть применены к различным задачам экономики и управления в лесной сфере.

3. Биологическое моделирование.

Лес является, прежде всего, биологической системой, поэтому, биологические модели применяются в различных областях лесного хозяйства (лесная генетика и селекция, ландшафтное проектирование и т.д.).

4. Экологическое моделирование.

Лес представляет собой сложный экологический объект, для которого характерны тесные взаимосвязи между составляющими его компонентами, а также активное взаимодействие с внешней средой. Благодаря использованию экологических моделей, становится возможным прогнозировать изменения в лесных экосистемах под влиянием природных факторов (погодные явления, процессы в биосфере, колебания климата за счет неантропогенного воздействия) и в результате хозяйственной деятельности человека (потребление лесных ресурсов, преобразование ландшафтов, парниковый эффект).

5. Моделирование в геоинформационных системах.

Моделирование играет особую роль в геодезии и картографии, которые имеют непосредственное отношение к лесному хозяйству (составление карт лесных угодий). В настоящее время, когда лесной комплекс не обходится без современных геоинформационных систем (ГИС), значимость моделирования становится еще выше.

Как мы видим, моделирование охватило практически все виды человеческой деятельности в лесной сфере, и его роль в развитии отрасли будет только возрастать.

Список источников

1. Звонарев С. В. Основы математического моделирования // Екатеринбург: Издательство Уральского федерального университета, 2019. – 116 с.

2. Королев А. Л. Компьютерное моделирование // Челябинск, 2019. – 189 с.

3. Худякова Е. В., Липатов А. А. Имитационное моделирование процессов и систем в АПК // Москва, 2021. – 256 с.

Статья поступила в редакцию 28.07.2023; принята к публикации 10.05.2023.

Информация об авторах

Акименко А.В. – к.т.н., доцент кафедры Компьютерных технологий и микроэлектронной инженерии ФГБОУ ВО «ВГЛТУ».

Медведев Р.Ю. – ст. преподаватель кафедры Компьютерных технологий и микроэлектронной инженерии ФГБОУ ВО «ВГЛТУ».

Аникеев Е.А. – к.т.н., доцент, зав. кафедрой Компьютерных технологий и микроэлектронной инженерии ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Акименко А.В. – сбор материала, обработка материала, частичное написание статьи (33%).

Медведев Р.Ю. – идея, частичное написание статьи (33%).

Аникеев Е.А. – частичное написание статьи, редактирование текста (33%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.051

Угрозы и методы защиты от нежелательных рассылок в социальных сетях

Александр Алексеевич Алексеев [1]✉, Павел Игоревич Карасев [2], Хайдар Абдулваххаб Х. Шамсулдин [3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]alekseevaaleksandr002@gmail.com✉, https://orcid.org/0009-0008-1745-4697
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3] fit_tstu@mail.ru, https://orcid.org/ 0009-0006-4255-5874

Аннотация. В статье представлены различные методы и технологии защиты от нежелательных рассылок в социальных сетях, такие как фильтрация контента, идентификация и блокировка ложных аккаунтов, анализ поведения пользователей, машинное обучение и искусственный интеллект. Рассмотрены преимущества и недостатки каждого метода, а также их эффективность.

Ключевые слова: информационная безопасность, спам, социальные сети.

С ростом популярности социальных сетей возрастает и угроза, связанная со спамом, который может быть не только раздражающим, но также представлять угрозу для безопасности пользователей и их персональных данных. Поэтому разработка эффективных методов борьбы со спамом в социальных сетях становится все более актуальной задачей.

Одним из основных способов борьбы со спамом в социальных сетях является фильтрацией контента. Этот метод основан на использовании определенных ключевых слов, фраз и других признаков, чтобы выявлять и блокировать спам-сообщения или нежелательный контент [1].

Как пример использования фильтрации контента рассмотрим YouTube. На данной платформе используется система автоматической фильтрации контента, которая проверяет видео на наличие нежелательных элементов. Также, YouTube предоставляет возможность пользователям отмечать видео, которые содержат нежелательный контент, и сообщать об этом администрации платформы.

Преимуществом фильтрации контента является относительная простота ее реализации без необходимости использования сложных технологий и высокотехнологичного оборудования. Она также может быть быстро настроена и может быть эффективной для борьбы со спамом, содержащим определенные ключевые слова или фразы.

Недостатком фильтрации контента является то, что она может быть неэффективна в борьбе со спамом, не содержащим ключевых слов или фраз, которые могут быть легко обнаружены фильтрами. Кроме того, иногда фильтры

могут считать легитимный контент спамом, что может привести к потере ценных сообщений и отношений с клиентами.

Идентификация и блокировка ложных аккаунтов является комплексным методом борьбы со спамом в социальных сетях, включающим анализ поведения пользователей, социальных связей и содержания постов.

Анализ поведения пользователей основан на исследовании ответов пользователя на других пользователей в комментариях и других активностей в социальной сети. Необычное поведение или поведение, не соответствующее типичному для данной социальной сети, может указывать на ложный аккаунт.

Анализ социальных связей основан на исследовании связей между пользователями в социальной сети. Ложные аккаунты могут иметь необычные связи с другими пользователями, которые не соответствуют типичным связям в этой социальной сети.

Анализ содержания постов основан на исследовании содержания постов пользователя. Частая публикация постов с нежелательным содержанием, таким как реклама, спам или фейковые новости, может указывать на ложный аккаунт [2].

В пример использования данного метода можно привести платформу VK. В 2020 году она объявила о блокировке более 2 миллионов ложных аккаунтов за месяц. Среди методов, используемых для выявления ложных аккаунтов, были анализ поведения пользователей, машинное обучение, анализ фотографий и текстовых сообщений. Эти методы позволили ВКонтакте бороться со спамом и мошенничеством в социальной сети, повысив качество пользовательского опыта.

Однако, необходимо учитывать, что этот метод также имеет свои ограничения и недостатки. Например, для данного метода необходима постоянная адаптация системы для выявления новых случаев. Кроме того, при использовании некоторых методов идентификации может возникнуть риск нарушения конфиденциальность данных пользователей.

Использование искусственного интеллекта для борьбы со спамом в социальных сетях может осуществляться с помощью анализа текстовых сообщений, идентификации поведенческих шаблонов и выявления необычных активностей на аккаунте пользователя [3].

Искусственный интеллект может быть использован для проверки на наличие признаков спама, таких как использование определенных ключевых слов и фраз, повторение одинаковых или похожих сообщений, наличие ссылок на вредоносные сайты и т.д. Для этого могут использоваться алгоритмы машинного обучения, которые позволяют обнаруживать и классифицировать спам-сообщения автоматически.

Также, можно использовать нейронные сети для определения ботов. Они могут проанализировать большой объем данных и выделить определенные шаблоны поведения, которые характерны для ботов. Это может быть использовано для автоматической идентификации и блокировки нежелательных аккаунтов.

Помимо прочего, можно применять алгоритмы кластеризации для группировки подозрительных аккаунтов и сообщений. Это позволяет выявлять связи между аккаунтами и обнаруживать более сложные схемы спам-активности, такие как сети ботов или организованные группы спамеров.

Существует множество примеров использования искусственного интеллекта для борьбы с нежелательными рассылками. Например, Facebook (соцсеть запрещена на территории РФ) использует алгоритмы глубокого обучения для анализа текстовых сообщений и выявления спама. В 2018 во французском сегменте социальной сети удалось развеять популярный миф о том, что можно спасти человека от инсульта, проколов палец пострадавшего иглой и пустив кровь. Благодаря этому методу было определено более 20 доменов и 1400 ссылок, распространяющих эту информацию.

Использование искусственного интеллекта для борьбы со спамом обладает преимуществами, такими как высокая точность и скорость анализа данных, а также возможность обучения на основе новых данных. Но также существуют недостатки, включая высокие затраты на разработку и внедрение системы, а также возможность ложноположительных решений и блокировки нормальных сообщений или аккаунтов.

Исследование способов борьбы со спамом в социальных сетях является сложной и постоянно обновляемой задачей. В работе были рассмотрены методы фильтрации контента, идентификации и блокировки ложных аккаунтов, анализа поведения пользователей, машинного обучения и искусственного интеллекта. Несмотря на преимущества каждого из этих методов, их комплексное использование может дать наилучший результат. Важно отметить, что технологии защиты от спама и спамеры постоянно совершенствуются, поэтому системы защиты должны постоянно обновляться и адаптироваться к изменяющейся обстановке.

Список источников

1. Prasanth V. N., Mahendra G. and Jabbar M. A. Analysis of Twitter Spam Detection Using Machine Learning Approach // International Journal of Computer Applications. - С. 1-5.

2. Yao M., Zhou, A., Jia, M. Applied Artificial Intelligence: A Handbook For Business Leaders. - 1-е изд. - San-Francisco: O'Reilly Media, Inc., 2018. - 182 с.

3. Хайкин С. Нейронные сети: полный курс - Neural Networks: A Comprehensive Foundation. 2-е изд. - М.: Вильямс, 2006. - 1104 с.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Алексеев А.А.- студент кафедры КБ-1 «Защита информации», направления подготовки «10.03.01 – Информационная безопасность» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Шамсулдин Хайдар Абдулваххаб Х. - аспирант Института автоматики и информационных технологий «ТГТУ».

Вклад авторов

Алексеев А.А.- идея, сбор материала, обработка материала (40%).
Карасев П.И. - написание статьи, научное редактирование текста (30%).
Шамсулдин Хайдар Абдулваххаб Х. - частичное написание статьи (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.9

Оценка потенциально неработоспособных микросхем в серийном производстве

Евгений Александрович Аникеев[1]✉, Оксана Викторовна Загоруйко[2], Максим Витальевич Солодилов [3], Максим Иванович Колесников[4]
[1,2,3,4] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия
[1] eanikeev@gmail.com✉,https://orcid.org/0000-0002-2509-0338
[2] tvoy.07@mail.ru, https://orcid.org/0000-0003-5411-0385
[3] monne.j@yandex.ru, https://orcid.org/0000-0003-7478-0322
[4] KM17@mail.ru, https://orcid.org/0000-0003-3414-4835

Аннотация. Рассмотрены процессы возникновения скрытых дефектов в ИС и методы их выявления с помощью радиационно-стимулированного метода. Приводятся результаты эксперимента.

Ключевые слова: микросхема, стойкость, отбраковка.

В настоящей работе представлены результаты исследований по отбраковке потенциально-ненадежных биполярных ИС радиационно-стимулирующим методом с применением программно-математического комплекса. Статистика параметрических отказов ИС показывает, что основная их доля вызвана дефектами в тонких (подзатворных) и толстых (пассивирующих) пленках оксидов кремния [1]. Эксперименты по облучению ИС [2] показывают, что в оксиде доминируют два типа дефектов с энергиями активации 0,9 и 1,6 эВ. Анализ методов активации скрытых дефектов показал, что наиболее приемлемым является метод облучения изделий гамма-излучением с последующим их отжигом и ускоренными испытаниями на наработку.

Используя результаты статистической обработки данных по отказам с применением программно-математического метода потенциальных функций, позволяющего сформировать поля «образов» надежных (Н) и ненадежных (НН) изделий данного типа и осуществлять отбраковку ненадежных схем.

Исследовались ИС 530ИР18 на выборке 50 шт. Предварительно был проведен конструктивно-технологический и схемотехнический анализ ИС с целью выбора информативных параметров, которые наиболее полно отражают физические явления, происходящие при активизации скрытых дефектов в активной структуре. Как правило, это могут быть не только предусмотренные в ТУ параметры, но и дополнительно выбранные. Так, для исследуемой ИС, кроме стандартных параметров, измерялся выходной ток низкого уровня.

Уровень облучения определялся по началу разделения массива значений параметров на 2-3 группы на гистограммах после облучения и отжига.

Для ИС режимы радиационно-термической обработки (РТО) составили: доза 105 рад; Тотж=125°С в течение 120 ч. После РТО происходит полный отжиг введенных радиационных зарядов в ТД и стабилизация параметров на уровне значений, близких к первоначальным.

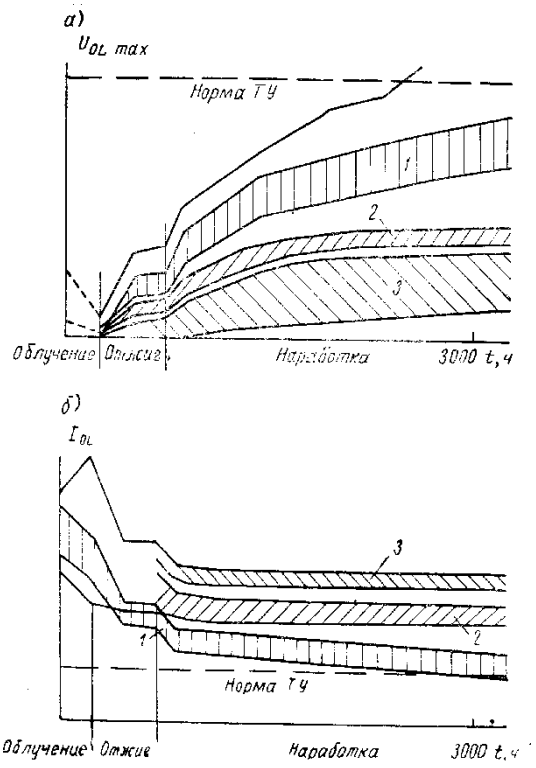

Рис.1. Изменение параметров UOL и IOL в ходе испытаний

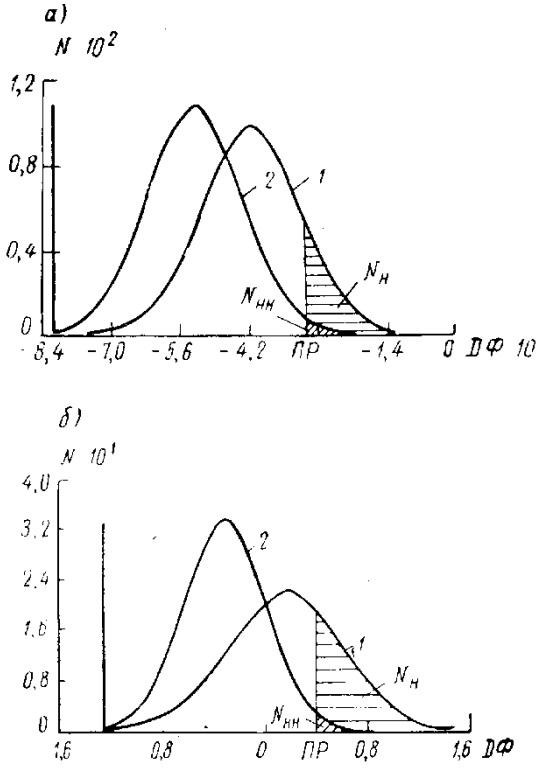

Рис.2 Дискриминационная функция для годных(1) и негодных (2) ИС.

С целью определения степени влияния дефектов второго типа (после их радиационной стимуляции) на надежностные характеристики, после отжига проводились ускоренные испытания ИС на наработку в течение 4000 часов при температуре +125°С и напряжении питания 5,5 В.

На рис. 1 представлен ход изменения параметров ИС на каждой стадии процесса исследования. По окончании ускоренных испытаний осуществлялась разбраковка изделий по более жестким, чем в ТУ (цеховым) нормам и фиксировались отказавшие изделия. По результатам начальных замеров с учетом данных по отказам после РТО и ускоренных испытаний проводилась выработка правила классификации, которая включала в себя: подготовку статистических данных и оптимизацию числа информативных параметров; расчет полей информативных параметров изделий, выдержавших и отказавших за время ускоренных испытаний; расчет порога распознавания и выработка правила классификации.

В рамках исследований разработана программа обработки результатов испытаний обучающей выборки (IMAGE), которая предусматривает выработку правила классификации и разбраковку изделий на надежные и ненадежные по прогнозу с заданной вероятностью ошибки второго рода. В соответствии с ней строилась дискриминационная функция (ДФ), как разность потенциалов в полях информативных параметров.

Список источников

1. Зольников В.К. Экспериментальные исследования радиационного воздействия на микросхемы FRAM / Зольников В.К., Гамзатов Н.Г., Анциферова В.И., Полуэктов А.В., Фиронов В.А. // Моделирование систем и процессов. 2022. Т. 15. № 3. С. 16-24.

2. Козюков А.Е. Методы обеспечения стойкости электронной компонентной базы к одиночным событиям путем резервирования / Козюков А.Е., Зольников В.К., Евдокимова С.А., Квасов О.Н., Яковлев К.А., Платонов А.Д. // Моделирование систем и процессов. 2021. Т. 14. № 1. С. 10-16.

3. Зольников В.К. Схемотехнические методы обеспечения стойкости ЭКБ к воздействию тяжёлых заряженных частиц / Зольников В.К., Макаренко Ф.В., Журавлева И.В., Попова Е.А., Гриднев Ю.В., Литвинова Ю.А. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 35-42.

4. Зольников В.К. Анализ чувствительности и результаты испытаний электронной компонентной базы к воздействию тяжелых заряженных частиц / Зольников В.К., Ягодкин А.С., Анциферова В.И., Евдокимова С.А., Скворцова Т.В., Грошева Е.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 43-51.

5. Зольников В.К. Проектирование интерфейсов сбоеустойчивых микросхем / Зольников В.К., Мозговой Н.В., Гречаный С.В., Селютин И.Н., Струков И.И. // Моделирование систем и процессов. 2020. Т. 13. № 1. С. 17-24.

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Аникеев Е.А. - к.т.н., доцент, и.о. зав. кафедрой «Кафедра компьютерных технологий и микроэлектронной инженерии» ФГБОУ ВО «ВГЛТУ».

Загоруйко О.В. - преподаватель СПО кафедры «Информационные технологии» ФГБОУ ВО «ВГЛТУ».

Солодилов М.В. - преподаватель СПО кафедры «Информационные технологии» ФГБОУ ВО «ВГЛТУ».

Колесников М.И. - аспирант ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Аникеев Е.А.- идея, сбор материала, обработка материала, частичное написание статьи (25%), редактирование текста.

Загоруйко О.В.- частичное написание статьи (25%).

Солодилов М.А.- частичное написание статьи (25%).

Колесников Д.Э.- частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.9

Расчет времени функционирования элементов аппаратуры при внешних воздействиях

Валентина Ивановна Анциферова [1]✉, Владислав Витальевич Котляров [2], Константин Владимирович Зольников [3], Александр Сергеевич Ватуев [4]
[1,2,3,4] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия
[1]Vianc@rambler.ru ✉,https://orcid.org/0000-0001-2589-2238
[2] embro.contact@icloud.com, https://orcid.org/0000-0002-2811-2374
[3] kvzolnikoff@yandex.ru, https://orcid.org/0000-0001-7478-4552
[4] vatuedA@mail.ru, https://orcid.org/0000-0003-2814-7705

Аннотация. Проведены экспериментальные исследования воздействия на биполярные ИС гамма–излучения малой мощности. Приводятся результаты испытаний. Предложена модель оценки деградации электропараметров ИС.

Ключевые слова: микросхема, проектирование, радиация.

При эксплуатации ИС в космических летательных аппаратах на них воздействует ионизирующее излучение малой мощности, приводящее к тому, что наряду с процессами деградации электропараметров от облучения, присутствуют процессы естественного старения. Совместное воздействие радиации и естественного старения изменяют надежность и радиационную стойкость изделий, и что особенно важно, влияние мощности воздействия, температуры среды и режима работы ИС оказывают существенное влияние на показатели стойкости и надежности [1, 2, 3, 4, 5].

Целью настоящих исследования является определения кинетики изменения электропараметров ИС от совместного воздействия радиации и процессов естественного старения с учетом мощности воздействия, температуры среды и режима работы ИС.

Для исследования этих процессов был поставлен многофакторный эксперимент, в ходе которого оценивалось изменение ПКГ от времени без облучения, в ходе облучения разной мощности, при воздействии температуры и различного электрического режима.

Для исследования этих процессов были проведены испытания на специально выполненных образцах (ИС 530ИР18 с тестовыми структурами), что позволило проанализировать изменение электропараметров как у ИС в целом, так и поведение ее отдельных элементов (транзисторов, резисторов, диодных цепочек и др.). Экспериментальные исследования заключались в проведении испытаний гамма–излучением малой мощности на ИС, находящихся в различных термотоковых режимах (при различной температуре окружающей среды, в различных режимах эксплуатации). Проводились также испытания на

долговечность в течение 12000 часов (как при нормальной, так и при повышенной температуре). Кроме того, для разработки полной математической модели были использованы результаты испытаний ИС на НПО "Электроника" в течение более 20 лет работы.

Экспериментальные результаты показали следующее: 1. Доминирующее влияние имеют процессы старения при мощности дозы ниже 0,1Р/с гамма–излучения, при мощности дозы свыше 1Р/с доминирующем процессом является деградация электропараметров вследствие облучения; 2. При увеличении температуры окружающей среды процессы деградации электропараметров ускоряются при мощностях ниже 0,1Р/с и замедляются при мощностях выше 1Р/с; 3. При испытании в активном режиме процессы деградации увеличиваются при мощностях ниже 0,1Р/с и замедляются при мощностях выше 1Р/с.

Результаты экспериментальных исследований позволили разработать модель прогнозирования показателей стойкости и надежности биполярных ИС.

Основу данной модели составляет уравнение, описывающее изменение электропараметра ИС от времени, с учетом накопленной дозы, мощности воздействия, температуры окружающей среды и режима работы ИС.

Изменение электропараметра определяется по формуле:

$$Y = Y_{об} + Y_{ст} + r\, Y_{об}\, Y_{ст},$$

где Y – общее изменение электропараметра; $Y_{ст}$ – изменение электропараметра вследствие старения; $Y_{об}$ – изменение электропараметра вследствие облучения; r – коэффициент влияния процессов старения и облучения друг на друга.

Таким образом, сущность данной модели заключается в том, что общее изменение электропараметров от комплекса факторов (старение и облучение) рассчитывается с помощью составляющих. Изменение электропараметров от облучения (первый член уравнения), изменение электропараметров от старения (второй член уравнения) и учет неаддитивности этих процессов (третий член уравнения). Критерием отказа ИС является достижение толерантного предела границы ТУ, поэтому решение этого уравнения осуществляется при U равном норме ТУ. В качестве неизвестных параметров в эти уравнения входят доза (D) и время (t). Для определения дозы отказа уравнения (1) и (2) решаются относительно дозы, при этом время определяется по формуле:

$$t = \frac{D}{M}$$

Для определения минимальной наработке на отказ уравнения (1) и (2) решаются относительно времени при этом доза определяется по формуле:

$$D = M\, t$$

Для реализации прогноза по этой модели составлена программа расчета.

Список источников

1. Полуэктов А.В. Моделирование колебательных процессов в пакете MVSTUDIUM / Полуэктов А.В., Зольников К.В., Анциферова В.И. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 139-148.

2. Зольников В.К. Схемотехнические методы обеспечения стойкости экб

к воздействию тяжёлых заряженных частиц /Зольников В.К., Макаренко Ф.В., Журавлева И.В., Попова Е.А., Гриднев Ю.В., Литвинова Ю.А. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 35-42.

3. Зольников В.К. Анализ чувствительности и результаты испытаний электронной компонентной базы к воздействию тяжелых заряженных частиц / Зольников В.К., Ягодкин А.С., Анциферова В.И., Евдокимова С.А., Скворцова Т.В., Грошева Е.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 43-51.

4. Зольникова А.Н. Методы обнаружения и исправления ошибок в нерегулярных структурах при воздействии тяжелых заряженных частиц / Зольникова А.Н., Евдокимова С.А., Оксюта О.В., Панина Н.В., Солодилов М.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 51-58.

5. Козюков А.Е. Общие подходы оценки стойкости к воздействию ионизирующего излучения космического пространства для зарубежной электронной компонентной базы предприятий –разработчиков / Козюков А.Е., Гамзатов Н.Г., Гречаный С.В., Зольников К.В., Струков И.И., Ачкасов А.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 58-66.

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Анциферова В.И. - к.т.н., доцент, кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Котляров В.В. - преподаватель СПО, кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Зольников К.В. - к.т.н., доцент, и.о. зав. кафедрой «Базовая кафедра технического и программного обеспечения вычислительных и информационных систем» ФГБОУ ВО «ВГЛТУ».

Ватуев А.С. - аспирант ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Анциферова В.И.- идея, сбор материала, обработка материала, частичное написание статьи (25%).

Котляров В.В.- частичное написание статьи (25%).

Зольников К.В.- частичное написание статьи (25%). научное редактирование текста

Ватуев А.С.- частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Обзор государственных стандартов, регулирующих использование электронных подписей в России

Владлен Дмитриевич Афонин ✉
Национальный исследовательский ядерный университет «МИФИ», Москва, Россия
inzanely@yandex.ru ✉, https://orcid.org/0009-0003-0255-6571

Аннотация. Рассматриваются особенности сохранения юридической значимости документа, подписанного электронной подписью в процессе хранения на основе анализа государственных стандартов, регулирующих использование электронных подписей в Российской Федерации.

Ключевые слова: электронная подпись, электронный документ, информационная безопасность.

В настоящее время электронный документооборот широко распространен в организациях как внутри компании, так и между компаниями. В целях обеспечения подлинности документов и защиты их от несанкционированных изменений в процессе жизненного цикла применяется технология электронной подписи. Долговременное хранение электронных подписей представляет собой важную задачу, решение которой повлечёт за собой решение проблемы сохранения юридической значимости подписанных документов. В связи с этим возникает необходимость обеспечить сохранность электронных документов и их подписей и подтвердить их подлинность и целостность на протяжении всего периода хранения.

Несмотря на то, что текущее законодательство не описывает способов архивного хранения электронных подписей документов на протяжении полного цикла их жизни, в России довольно широко используются форматы усовершенствованной электронной подписи CAdES. CMS Advanced Electronic Signatures (CAdES) — это стандарт ЭП, представляющий собой расширенную версию стандарта Cryptographic Message Syntax (CMS). Главным документом, описывающим данный стандарт, является ETSI TS 101 733 «Electronic Signature and Infrastructure (ESI); CMS Advanced Electronic Signature (CAdES)». CAdES стал развитием CMS, в котором были исправлены такие основные недостатки предшественника, как отсутствие штампа доверенного времени создания ЭП, отсутствие типа содержимого ЭП и отсутствие возможности долгосрочного сохранения свойств юридической значимости ЭП. Формат CAdES-A (в последней спецификации, CAdES-LTA) - один из форматов, описанных в стандарте CAdES, содержащий помимо всех остальных атрибутов архивную метку времени, а также обеспечивающий возможность её повторного добавления, что, во-первых, решает задачу обеспечения юридической

значимости подписи при долгосрочном (потенциально - бесконечном) хранении, а во-вторых, в силу своего устройства позволяет при ослабевании алгоритмов и утрате ими актуальности перейти в новых архивных штампах времени на новые алгоритмы без необходимости как-то изменять исходные данные.

Таким образом, задача архивного хранения на текущий момент сводится к реализации простого в использовании и в интеграции с существующими системами ЭДО [1] программного комплекса.

В данной работе проведён обзор государственных стандартов, регулирующих использование электронных подписей в России, проведён анализ предлагаемых в законодательстве подходов к долгосрочному хранению электронных подписей. Как мы увидим далее, текущее законодательство не даёт возможности получения положительного результата проверки ЭП в течение всего срока её хранения. В качестве решения этой проблемы предложено использование формата ЭП CAdES-A.

Отношения в области применения электронной подписи регулируются Федеральным законом от 06.04.2011 No 63-ФЗ «Об электронной подписи» (Федеральный закон No 63-ФЗ), а также Федеральным законом от 27.12.2019 No 476-ФЗ в котором положения частей 2.3-2.6 статьи 3 действуют до 31.12.2022 года включительно. Федеральным законом No 63-ФЗ определяются понятие электронной подписи и ее виды: простая, усиленные неквалифицированная и квалифицированная электронные подписи. В соответствии с ГОСТ Р 54989-2012/ISO/TR 18492:2005 [2], "аутентичный электронный документ" — это электронный документ, сохраняющий свою точность, надежность и целостность со временем. Это означает, что любой электронный документ, подписанный электронной подписью, считается аутентичным. Если для подписания использовалась квалифицированная электронная подпись, то электронный документ равнозначен бумажному документу, подписанному собственноручной подписью. Главной проблемой здесь является проверка действительности сертификата подписанта на момент подписания электронного документа. И для решения задачи обеспечения аутентичности необходимо реализовать возможность проверки электронной подписи документа в течение всего срока хранения. Согласно требованиям, изложенным в Федеральном законе от 10 января 2002 года № 63-ФЗ «Об электронной подписи» [3], подлинность сертификата подписанта на момент подписания электронного документа подтверждается только при наличии "достоверной информации о моменте подписания электронного документа". Для получения такой информации можно использовать метку доверенного времени (TSP), которая является ответом от доверенного центра времени (службы TSP).

Как было отмечено ранее, в соответствии с 63-ФЗ «Об электронной подписи» действительность сертификата на момент подписания электронного документа подтверждается при наличии метки доверенного времени, которая может быть получена от службы TSP. Однако само по себе наличие метки времени в электронной подписи ничего не говорит о действительности сертификата подписанта. Значит, для обеспечения положительного результата проверки подписи в рамках архивного хранения одной лишь метки времени

недостаточно. Другой возможный подход к организации долгосрочного хранения подписей описан в законопроекте № 1173189-7 [4], находящемся в стадии рассмотрения Государственной думой РФ. Для обеспечения сохранности электронных документов в архиве предлагается полагаться на подпись архивариуса, который имеет лицензию на хранение электронных документов, или на другое лицо, которое ответственно за хранение электронных документов. В случае истечения срока действия сертификата исходного подписанта или архивариуса, рекомендуется переподписывать электронные документы. Однако, с увеличением объема электронных документов, переподписание всего архива может оказаться затруднительным [5].

Таким образом, существующие законодательные нормы и проекты не дают возможность получения положительного результата проверки в течение всего срока хранения документа. Тем не менее, в России довольно широко используются форматы усовершенствованной электронной подписи CAdES (CMS Advanced Electronic Signature), представляющей собой расширенную версию стандарта электронной подписи CMS (Cryptographic Message Syntax) [6], и XAdES (XML Advanced Electronic Signature), закреплённые в стандартах организации ETSI [7].

Электронная подпись, технически реализованная на основе CAdES, имеет статус усовершенствованной электронной подписи [7]. Это означает, что

- она однозначно связана с подписавшим лицом; с она способна идентифицировать подписанта;

- только подписант имеет контроль над данными, использованными для создания подписи;

- ее можно идентифицировать, если данные, приложенные к подписи, были изменены после подписания.

Результирующим свойством CAdES является то, что подписанные электронной подписью документы могут оставаться действительными в течение длительного времени, даже если подписавший или проверяющая сторона впоследствии попытаются опровергнуть действительность подписи.

Электронная подпись на основе CAdES принимается в судебном процессе в качестве доказательства, поскольку усовершенствованные электронные подписи имеют юридическую силу, но она приобретает большую доказательную силу, если становится квалифицированной электронной подписью. Чтобы получить такую юридическую силу, она должна быть снабжена цифровым сертификатом, зашифрованным с помощью устройства создания квалифицированной подписи («квалифицированная электронная подпись»). Авторство заявления с квалифицированной электронной подписью не может быть оспорено — заявление не подлежит опровержению.

Подводя итог, формат CAdES-X Long Type 1 позволяет обеспечить временное (оперативное) хранение и положительный результат проверки электронной подписи документов сроком до 10–15 лет с момента подписания. Однако для документов долговременного (больше 15 лет) или постоянного хранения данный формат подписи не подходит из-за ограниченного срока жизни сертификата службы штампов времени (обычно не более 15 лет), который

используется для заверения доказательств подлинности. Формат CAdES-A является развитием формата CAdES-X Long Type 1 и предназначен для защиты подписи электронного документа в процессе его долгосрочного хранения. Он позволяет добавлять дополнительные архивные метки времени для защиты предыдущих меток времени и доказательств подлинности подписи. В отличие от формата CAdES-X Long Type 1, для CAdES-A необходимо добавлять новые архивные метки времени в течение всего срока хранения документа. Однако процедуру добавления метки времени нужно выполнить гораздо реже (раз в 10–15 лет) по сравнению с ежегодным переподписанием документов подписью архивариуса, а сам процесс добавления метки времени выполняется значительно быстрее создания подписи.

Список источников

1. Итоги работы Всероссийского Форума ЭДО’2022. - 2022. - Режим доступа: https://roseu.org/news/itogi-edo-2022 (дата обращения: 12.08.2022).
2. ГОСТ Р 54989-2012/ISO/TR 18492:2005 «Обеспечение долговременной сохранности электронных документов». — М., 2013.
3. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ. — М., 2011.
4. Законопроект No 1173189-7 О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации. — М., 2022.
5. Архивное хранение электронных документов с ЭП. Законодательство и практика. — 2022. — Режим доступа: https://ib-bank.ru/bisjournal/post/1888 (дата обращения: 12.08.2022).
6. RFC 5126. CMS Advanced Electronic Signatures. — 2008.
7. ETSI TS 101 733 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). — 2013.

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Научная статья
УДК 004.9

Графические средства для проектирования микросхем

Александр Владимирович Ачкасов [1]✉, Роман Валерьевич Тен [2], Николай Олегович Майгур [3] , Екатерина Владимировна Грошева [4], Аким Владимирович Толкачев [5]

[1,2,3,4,5] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия

[1] achkasov@list.ru✉, https://orcid.org/0000-0003-3409-0342

[2] roma.ten.00@inbox.ru, https://orcid.org/0000-0003-3410-0302

[3] maygurno@vglta.vrn.ru https://orcid.org/0000-0003-3409-0342

[4] grosheva.e @mail.ru, https://orcid.org/0000-0003-3409-0324

[5] tolkachev.akim@mail.ru, https://orcid.org/0000-0003-3409-0312

Аннотация. В статье рассматриваются модули графической подсистемы для системы автоматизации проектирования микросхем. Показана структура графического редактора. Она позволяют эффективно реализовать процесс описания всей совокупности данных о типовых элементах КМОП БИС двойного назначения и преобразование структуры схем в рамках различных уровней моделирования.

Ключевые слова: САПР, графическая подсистема, модули, процедуры.

В статье рассматривается структура графической подсистемы (ГП) АРМ проектировщика КМОП БИС двойного назначения, созданной на основе ПЭВМ. Графически подсистема реализована на алгоритмическом языке FORTRAN и С. Для ее функционирования требуется объем ОЗУ до 0,5 Мбайт. В ГП входят программные модули: MG, TMOD, TL, LR, SR, GR, SDPR, PSR, PSTG. Программный модуль MG является управляющим. С его помощью организуется взаимодействие с операционной системой АРМ и между всеми программными модулями системы в том числе программами поведенческого, функционально-логического, схемотехнического, топологического проектирования и генерации тестов [1, 2, 3, 4, 5].

Модули TMOD и TL обеспечивают обработку конструкций входного языка описания входных воздействий и задания на проектирование и модульного описания стандартных элементов, проверку синтаксиса и семантики, выявления наиболее вероятных ошибок, формирование и вывод на экран диагностических сообщений. С их помощью осуществляются такие процедуры автоматического формирования данных в графической форме при символьном методе описания, генерации сигналов по эмпирическим законам и другие [6].

Модуль LR предназначен для управления библиотекой пользователя, включает процедуры инициализации библиотеки, вывода ее оглавления, распечатки элементов библиотеки, удаления или добавления элементов из (в)

библиотеки (у), проверку существования модуля в библиотеке, запись его в библиотеку проекта без модификации и с модификацией (без раскрытия внутренней структуры или с раскрытием по заданию пользователя), выполнение необходимых преобразований для вложенных структур и другие, а также общие процедуры управления базой данных [6].

Ядром подсистемы является графический редактор (ГР) SR. Программно реализованные процедуры ГР можно разделить на группы в соответствии с их функциональным назначением.

Процедуры общего назначения предназначены для настройки ГР (задания спецификаций и цвета линий, временного интервала для создания копий редактируемого файла, задания шага координатной сетки, параметров пользователя и другие), для поддержки пользователя (процедуры оказания помощи), для выхода из редактора с сохранением внесенных изменений или без сохранения. Группа процедур рисования и редактирования базовых фигур - линии, многоугольника, дуги, окружности, прямоугольника, трассы, а также процедур, позволяющих изменять, копировать, удалять сформированные изображения. Следующая группа содержит процедуры формирования библиотеки элементов - задания имени библиотечного элемента, рисования его изображения, обозначения типа библиотечного элемента, размещения его в координатном поле, записи в библиотеку, просмотра библиотеки и другие [6].

Процедуры формирования элементов схемы позволяют вызвать элементы из библиотеки и закрепить их в модели координатного поля с присвоением порядковых номеров по типам элементов; редактировать элементы - сдвигать, изменять ориентацию, копировать, удалять, разрешать или запрещать редактирование отдельных элементов или групп. Группа процедур для формирования и редактирования связей предназначена для интерактивной и автоматической трассировки, для редактирования уже разведенных связей; формирования файла описания цепей и элементов. Групповые процедуры позволяют обрабатывать фрагменты схемы, задавать список наблюдаемых слоев, выводить списки цепей, задействованных библиотечных элементов и всей библиотеки в целом, а также формировать области трассировки. И последняя группа содержит процедуры управления изображением, предназначенные для центрирования, масштабирования изображений, идентификации обрабатываемых элементов, управления координатным полем и т.д. [6].

ГР имеет иерархическую структуру команд, которые разделены на два уровня: командных процедур и команд курсора. В свою очередь, команды курсора можно разделить на подуровни: ввода-вывода, редактирования и управления изображением. К уровню командных процедур относятся процедуры, с помощью которых пользователь может вывести справочную информацию, задать режим координатных осей на экране, установить спецификацию линий чертежа, слоев, войти в режим синтеза и редактирования чертежа, формирования рабочей библиотеки файла - описание структуры схемы, интерактивной и автоматической трассировки связей, идентификации точек привязки библиотечных элементов схемы; выделения подмножества деревьев, принадлежащих цепям схемы; формирование графического файла описания цепей и элементов схемы по файлу

описания схемы; прервать процесс проектирования; вывод изображения на экран графического дисплея, и другие.

В группу рисования и редактирования базовых геометрических фигур входят шесть команд построения прямоугольника, многоугольника, круга, линии, дуги и текста и следующие команды редактирования сдвига, удаления, модификации и копирования.

К этой же группе относятся команды формирования изображения библиотечных элементов - ввод имени библиотечного элемента, его размещения в координатном поле, размещение элемента по матрице, рисование корпуса библиотечного элемента; рисование выводов, задание типа элементов.

Таким образом, разработанные средства позволяют эффективно реализовать процесс описания всей совокупности данных о типовых элементах КМОП БИС двойного назначения и преобразование структуры схем в рамках различных уровней моделирования.

Список источников

1. Беспалов В. А. Обзор методов измерения механической прочности тонких плёнок / Беспалов В. А., Товарнов Д. А., Дюжев Н. А., Махиборода М. А., Гусев Е. Э., Зольников К.В. // Моделирование систем и процессов. 2022. Т. 15. № 3. С. 110-128.

2. Чубунов П.А. Компьютерное моделирование радиационного воздействия на энергонезависимую память с высоким быстродействием / Чубунов П.А., Лапшин А.П., Солодилов М.В., Рязанцев Р.Б., Гамзатов Н.Г., Евдокимова С.А., // Моделирование систем и процессов. 2022. Т. 15. № 3. С. 93-102.

3. Шипилова Е.А. Математическое моделирование и программная реализация процесса управления обеспечением безопасности полетов и деятельностью авиационного персонала / Шипилова Е.А., Платонов А.А., Равлык Р.Ф., Господ А.А. // Моделирование систем и процессов. 2022. Т. 15. № 2. С. 100-109.

4. Макаренко Ф.В. Обзор логических базисов и микросхем при построении комбинационного устройства с учётом надёжности / Макаренко Ф.В., Ягодкин А.С., Зольников К.В., Денисова О.А., Полуэктов А.В. // Моделирование систем и процессов. 2022. Т. 15. № 1. С. 115-124.

5. Полуэктов А.В., Использование сторонних библиотек при написании программ для обработки статистических данных / Полуэктов А.В., Макаренко Ф.В., Ягодкин А.С. // Моделирование систем и процессов. 2022. Т. 15. № 2. С. 33-41.

6. Мерочкин А.С., Будников Р.К., Самойлов В.Д., Клонин И.П., Громов Ю.Ю. Математическое моделирование процесса автоматизированного комбинирования цифровых фильтров // Надежность и качество: труды международного симпозиума. – Пенза, 2022, - Т. 1. – С. 82 – 84.

Статья поступила в редакцию 23.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Ачкасов А.В. - д.т.н., профессор «Базовая кафедра технического и программного обеспечения вычислительных и информационных систем» ФГБОУ ВО «ВГЛТУ».

Тен Р.В. – ст. преподаватель кафедры «Информационные технологии» ФГБОУ ВО «ВГЛТУ».

Майгур Н.О. - преподаватель СПО кафедры «Информационные технологии» ФГБОУ ВО «ВГЛТУ».

Грошева Е.В. - преподаватель «Базовая кафедра технического и программного обеспечения вычислительных и информационных систем» ФГБОУ ВО «ВГЛТУ».

Толкачев А.В. – ассистент кафедры «Вычислительной техники и информационных систем» ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Ачкасов А.В.- идея, сбор материала, обработка материала.

Тен Р.В.- написание статьи, научное редактирование текста (25%).

Майгур Н.О.- частичное написание статьи (25%).

Грошева Е.В.- частичное написание статьи (25%).

Толкачев А. В. частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 003:26

Математические модели анализа криптографических хеш-функций

Алексей Григорьевич Белоусов ✉
Брянский государственный технический университет, Брянск, Россия
belousov-ag@yandex.ru ✉, http://orcid.org/0009-0001-2873-4239

Аннотация. Рассматриваются некоторые математические модели, связанные с оценкой качества и криптостойкости хеш-функций. Для удобства восприятия некоторые модели сопровождаются примерами на конкретных значениях.

***Ключевые слова*:** криптографическое хеширование, хеш-функция, коллизия хеш-функции, восстановление прообраза, статистический тест.

Математические модели и методы широко используются для оценки свойств криптографических хеш-функций. Это связано с необходимостью понимания, насколько быстро может быть нарушена безопасность системы, которая пользуется некоторой хеш-функцией, например, системы авторизации с хешированием паролей. Далее рассмотрим некоторые модели, связанные с математическим исследованием хеш-функций.

Определение оптимального распределения хешей. Интуитивно понятно, что у хорошо спроектированной хеш-функции вероятность каждого хеша при случайном входе должна быть одинаковой. Докажем это на практике. Пусть $p_1, p_2, ..., p_h$ – вероятности появления каждого из h возможных хешей. Вероятность коллизии для двух случайных строк составляет $f = p_1^2 + p_2^2 + ... + p_h^2$. Возникает оптимизационная задача

$$\begin{cases} f = p_1^2 + p_2^2 + ... + p_h^2 \to \min \\ p_1 + p_2 + ... + p_h = 1 \\ 0 \le p_1, p_2, ..., p_h \le 1 \end{cases}.$$

Возможно сократить размерность задачи:

$$\begin{cases} f = p_1^2 + p_2^2 + ... + (1 - p_1 - ... - p_{h-1})^2 \to \min \\ p_1 + p_2 + ... + p_{h-1} \le 1 \\ p_1, p_2, ..., p_{h-1} \ge 0 \end{cases}.$$

Обнуляя частные производные f, получим:
$2p_k - 2(1 - p_1 - ... - p_{h-1}) = 0, k = 1, 2, ..., h-1.$

Решением этой системы уравнений будет $p_1 = p_2 = ... = p_{h-1} = 1/h$, из чего также следует $p_h = 1/h$. Показать, что это действительно точка минимума, можно на основе того, что положительны все угловые миноры матрицы Гессе в точке, в данном случае матрица имеет вид

$$G=(g_{ij}),i,j=1,2,...,h-1,g_{ij}=\begin{cases}4,i=j\\2,i\neq j\end{cases}.$$

Математическое ожидание числа проб при восстановлении прообраза перебором. Пусть дана хорошо спроектированная хеш-функция, т.е. вероятность каждого хеша для случайной строки равна 1/*h*. На первый взгляд, оценка будет достаточно трудоемкой, поскольку требуемое число проб теоретически неограниченное, но на самом деле она выполняется легко. Обозначим *X* – число проб. *X*=*k*, если для *k*-ой строки хеш тот, что нужно, а для предыдущих *k*-1 получены другие хеши. Тогда

$$P(X=k)=\left(\frac{h-1}{h}\right)^{k-1}\frac{1}{h};M[X]=\frac{1}{h}\sum_{k=1}^{\infty}k\left(\frac{h-1}{h}\right)^{k-1}.$$

Как и в предыдущем случае, требуется задействовать как теорию вероятностей, так и математический анализ. Используя ряд Маклорена для степени, можно показать, что

$$\sum_{k=1}^{\infty}kx^{k-1}=\frac{1}{(1-x)^2},|x|<1.$$

Тогда

$$x=\frac{h-1}{h},0<\frac{h-1}{h}<1,\frac{1}{(1-x)^2}=h^2,M[X]=\frac{1}{h}h^2=h.$$

Таким образом, при атаке «грубой силой» для восстановления прообраза, в среднем надо проверить *h* строк, что делает ее для современных хеш-функций малополезной без распределенных вычислений.

Тесты ГПСЧ. Хорошая хеш-функция одновременно является хорошим генератором псевдослучайных последовательностей бит. Один из самых строгих наборов статистических тестов ГПСЧ – тесты NIST. В основе каждого из этих тестов лежит задача вычисления статистики, характеризующей некоторое свойство последовательности, после чего эта статистика сравнивается с эталоном, который дает действительно случайная последовательность [4]. Существует следующий способ использовать тесты NIST для хеш-функций [3]: для каждой из достаточного большого числа строк генерируется хеш в виде последовательности бит, и все полученные последовательности сцепляются в единую, после чего для объединенной серии бит и выполняется тестирование.

Самый простой способ выявить откровенно слабые решения при проектировании новых хеш-функций – провести частотный тест бит по критерию «Хи-квадрат». Приведем упрощенный пример. Допустим, суммарно во всех хешах в коллекции строк имеем 84 нулевых бит и 156 единиц. Идеальные частоты – по 120. Тогда

$$\chi^2=\frac{(84-120)^2}{120}+\frac{(156-120)^2}{120}=21,6.$$

На основе принципа использования «Хи-квадрата» для проверки равномерности распределения дискретной случайной величины [1], получаем для уровня значимости 0,01 критическое значение $\chi^2_{табл}\approx 6,6$. В силу $\chi^2_{табл}<\chi^2$, исходя из выбранного уровня значимости, с вероятностью 99% или выше,

можно утверждать, что такая значительная разница частот нулей и единиц – не случайность, а проявление ошибки проектирования хеш-функции.

Парадокс дней рождения. Как и восстановление прообразов методом простого перебора, поиск коллизий на основе парадокса дней рождения почти не применяется в чистом виде, однако последний служит одной из научных основ теории криптоанализа хеш-функций. Даже для хорошо спроектированной хеш-функции, на множестве из примерно $\sqrt{h}$ строк с вероятностью более 50% есть пара строк с одинаковым хешем, т.е. обнаруживается коллизия второго рода, а для вероятности в 99% нужно увеличить множество вчетверо [2]. Из этого следует, что 256-битные хеш-функции ненадежны, а 128-битные можно удачно атаковать даже с техническими средствами уровня начала 2000-х гг. [2]. В [5] приводится два важных вывода, исходя из парадокса дней рождения относительно хеш-функций.

1. Вероятность коллизии хешей между одним из законных и поддельных документов выше, чем интуитивно ожидается за счет огромных значений *h*. Это требуется учитывать при использовании хеш-функций для защиты от подмены и подделки документов.

2. Фактически требуемое число входных строк для поиска коллизий второго рода существенно меньше $\sqrt{h}$, поскольку неравномерность распределения увеличивает вероятность коллизии для пары строк, а реальные – не идеальные – хеш-функции не дают строго равномерного распределения. Заметим, что это согласуется с тем, что мы вывели ранее.

Статистический анализ комбинаций бит и групп бит в хеше. Рассмотрим на конкретном примере. Пусть дана 64-битная хеш-функция, и для 14 входных строк получены хеши (в 16-ричном виде): 6**00**DF19542B5DECB, 138**BB**0C530B0A0**DD**, B63E0753173A4C**55**, 0939**44**EB5E69521D, 8C8**33**8C8A2CA32D8, 0846AEFEDF3CDFC0, 3B95256BDCD28**FF**D, E05**FF99**579CF6952, 6EC6C695614C**55**32, 360D663F3821**CC**16, 494F47B6404BE4A7, DA4658123545909F, C4CABE5979EB5957, A527B15BFF0C**99**CB. Часто встречаются пары соседних одинаковых 16-ричных цифр – всего в 10 хешах. Само по себе это еще не является основанием считать хеш-функцию плохо спроектированной – человеку свойственно предвзято относиться к некоторым комбинациям. Допустим, выпадение шестерок при трех подряд бросках игральной кости кажется неслучайным, а выпадение комбинации 3,5,4 – случайным, хотя при различении порядка чисел, в обоих случаях вероятность 1/216.

Попытаемся на примере хешей определить, случайно ли обилие выделенных жирным совпадений соседних 4-битных групп. Вероятность того, что две соседние 16-ричные цифры разные, составляет 15/16. Вероятность того, что все 15 пар таких цифр в хеше разные, составляет $(15/16)^{15} \approx 0,3798$. Если хеш-функция – идеальный ГПСЧ, то число «неправильных» хешей подчинено биномиальному закону с $n = 14, p \approx 0,3798$.

Вероятность того, что 64-битная хеш-функция выдала бы $X \geq 10$ «неправильных» хешей из 14, составит

$$P(X \geq 10) \approx \sum_{k=10}^{14} C_{14}^{k} (0,3798)^{k} (0,6202)^{14-k} \approx 0,0117.$$

Заметим, что неправильно считать $P(X = 10)$, и вообще любое конкретное значение X при любом достаточно большом числе проверочных хешей: не следует путать вероятности принятия ровно заданного значения и не менее заданного.

Подводя итог, заметим, что основой анализа хеш-функций являются методы теории вероятностей и математической статистики, однако во многих случаях математическая оценка свойств хеш-функций приводит к использованию сразу нескольких математических дисциплин и к комбинированию теорем и формул, кажущихся даже добросовестно изучавшим курс высшей математики на первый взгляд заведомо не связанными между собой.

Список источников

1. Критерий согласия Пирсона (Хи-квадрат). URL: https://statanaliz.info/statistica/proverka-gipotez/kriterij-soglasiya-pirsona-khi-kvadrat/.

2. Лёвин В.Ю. О повышении криптостойкости однонаправленных хеш-функций // Фундаментальная и прикладная математика. 2009. № 5. С. 171-179.

3. Математические аспекты разработки и анализа функций хеширования. URL: https://hmath.spbstu.ru/userfiles/files/publication/Nedelya-nauki-FizMeh-2022/3-hashing_fully_final.pdf.

4. Перов А.А. Применение статистических тестов NIST для анализа выходных последовательностей блочных шифров // Системы анализа и обработки данных. 2019. № 3. С. 87-96.

5. Пчелинцева Н.В., Самохин К.О., Картечина О.С. Парадокс дней рождения в криптографии // Наука и образование. 2022. № 2.

Статья поступила в редакцию 22.03.2023; принята к публикации 10.05.2023.

Научная статья
УДК 004:056

Особенности нейтрализации человеческого фактора при реализации инцидентов информационной безопасности

Татьяна Вячеславовна Васина
Брянский государственный университет им. акад. И.Г. Петровского, Брянск, Россия
tata.vasina.666@gmail.com✉

Аннотация. Вопрос обеспечения кибербезопасности предприятия актуальный, важный и встает перед объектами любого масштаба. Большие финансовые затраты влечет за собой внедрение эффективных средств и мер защиты информации. Однако, даже внедрение дорогостоящего и комплексного перечня мер и средств далеко не всегда является гарантией высокого уровня безопасности. Свыше 90% утечек конфиденциальной информации – не результат мастерства хакеров, а вина сотрудников. Эффективная работа с внутренними сотрудниками снижает их мотивированность к реализации противоправного деяния относительно объекта и актуальность данной категории возможных нарушителей.

Ключевые слова: информационная безопасность, человеческий фактор, инцидент.

Вопрос обеспечения кибербезопасности предприятия актуальный, важный и встает перед объектами любого масштаба. Большие финансовые затраты влечет за собой внедрение эффективных средств и мер защиты информации.

Однако, даже внедрение дорогостоящего и комплексного перечня мер и средств далеко не всегда является гарантией высокого уровня безопасности.

По данным проведенного в конце 2022 года опроса экспертов по кибербезопасности газетой «Известия», свыше 90% утечек конфиденциальной информации – не результат мастерства хакеров, а вина сотрудников [1].

Представленные данные статистики свидетельствуют о том, что важно уделять внимание не только общим регламентам обеспечения информационной безопасности и установке средств защиты, но и работе с кадровым составом. Эффективная работа с внутренними сотрудниками снижает актуальность данной категории возможных нарушителей.

Человеческий фактор реализации инцидентов информационной безопасности исходит от внутренних сотрудников объекта, которых в общем можно обозначить как категорию «Внутренние нарушители».

Данный тип нарушителя особенно опасен, потому что он осведомлен об устройстве внутренней инфраструктуры объекта и имеет доступ к ряду внутренних систем. Даже если имеющегося уровня доступа недостаточно для реализации инцидента ИБ, его наличие значительно упрощает процедуру повышения привилегий.

То, что некоторые из тех, кто пытается атаковать объект из вне действуют наугад и путем перебора множества различных вариантов (например, атаки типа брутфорс) иногда является решающим фактором в обнаружении попытки реализации инцидента ИБ. В то время как внутренний нарушитель может действовать точечно, поэтапно и незаметно для большинства мониторинговых систем.

Ввиду данных причин гораздо более эффективной является превентивная работа с потенциальными внутренними нарушителями

Превентивная работа должна производиться по двум направлениям – повышение осведомленности и снижение мотивации к реализации правонарушения, поскольку основные причины реализации инцидента со стороны внутреннего нарушителя, это неосторожные случайные действия, сопряженные с незнанием четких инструкций или же преднамеренные противоправные действия из мести или личной выгоды.

Повышение осведомлённости внутреннего нарушителя должно исключать реализацию инцидента информационной безопасности по неосторожности.

Данное направление включает в себя следующий перечень мероприятий:

1. Руководителем организации должны быть разработаны комплексные и подробные должностные инструкции для каждого из работников. Данные инструкции должны включать не только общие обязанности, но и регламент действий при возникновении вопросов и внештатных ситуаций.
2. Ежегодно для сотрудников должны устраиваться курсы повышения квалификации в сфере профильной деятельности, а также семинары и конференции для обмена опытом.
3. При разработке новых положений и инструкций, для сотрудников, чью деятельность они затрагивают, должно быть проведено совещание, в рамках которого автор документа подробно объясняет порядок реализации прописанных положений и отвечает на уточняющие вопросы. По результатам данного совещания все сотрудники должны подтвердить свое ознакомление с документом подписью в листе ознакомления, который хранится вместе с утвержденным документом.
4. Ежегодно для от рудников должны устраиваться лекции или иные обучающие мероприятия, в рамках которых специалисты по информационной безопасности будут информировать сотрудников о правилах, которые необходимо соблюдать для обеспечения информационной безопасности, о новых способах реализации инцидента ИБ со стороны злоумышленников (фишинг, методы социальной инженерии и т.д.), а также о мерах противодействия им. По результатам мероприятия для достижения его более высокой эффективности, сотрудникам может раздаваться краткая печатная памятка с основными рассматриваемыми в ходе мероприятия вопросами.

Соблюдение вышеописанных пунктов повысит теоретическую подготовку потенциальных внутренних нарушителей, как с точки зрения профессиональных компетенций, так и с точки зрения поддержания общего уровня информационной безопасности объекта.

Снижение мотивации к реализации правонарушения со стороны внутреннего нарушителя также не менее важный аспект. Довольно часто внутренние сотрудники реализуют противоправные действия из личных мотивов.

Работа по данному направлению состоит из двух основных пунктов:

1. При приеме сотрудников на работу необходимо производить анализ не только профессиональных, но и человеческих качеств претендента. Данный пункт может осуществляться путем проведения психологического тестирования, запроса рекомендаций с предыдущих мест работы, выяснения причин увольнения с последнего места работы. Все эти мероприятия могут помочь составить общий психологический портрет человека и оценить его склонность к реализации инцидента ИБ из мести или же путем подверженности чужому влиянию.
2. Разработка мотивационной политики объекта. Это комплексный документ, который позволяет закрепить систему положительного подкрепления корректной и эффективной реализации своих обязанностей со стороны сотрудников. В рамках данного документа можно закрепить порядок выплаты премий, оплаты образовательных программ, выплат ко дню рождения и иные привилегии. Важно четко и структурно описать требования, которые должны выполняться для получения тех или иных преимуществ.

Реализация данных пунктов повысит осведомлённость руководства о личных качествах сотрудника, а также общую лояльность работника к руководству.

Таким образом, предложенный в рамках статьи перечень действий при его корректной реализации в значительной степени окажет влияние на нейтрализацию человеческого фактора при реализации инцидентов информационной безопасности.

Список использованных источников.

1. Известия: 90% утечек спровоцировано человеческим фактором. – URL: https://iz.ru/1334130 (Дата обращения: 3.05.2023).

Статья поступила в редакцию 05.05.23; принята к публикации 10.05.2023.

Научная статья
УДК 004:056

Порядок разработки эффективного комплекса мер и средств для обеспечения информационной безопасности объекта

Татьяна Вячеславовна Васина
Брянский государственный университет им. акад. И.Г. Петровского, Брянск, Россия
tata.vasina.666@gmail.com✉

Аннотация. Обеспечение информационной безопасности объекта на сегодняшний день одна из приоритетных задач для руководителей предприятий различного масштаба. В первую очередь это связано ухудшением общих показателей статистики в данной сфере, а также с ужесточением некоторых норм законодательства. В рамках статьи предложен порядок разработки эффективного комплекса мер и средств для обеспечения информационной безопасности объекта, описаны основные аспекты, на которые следует обратить внимание операторам.

Ключевые слова: информационная безопасность, объект, комплекс мер и средств.

Обеспечение информационной безопасности объекта на сегодняшний день одна из приоритетных задач для руководителей предприятий различного масштаба. В первую очередь это связано ухудшением общих показателей статистики в данной сфере, а также с ужесточением некоторых норм законодательства.

По данным отчёта Positive Technologies в 2022 году общее количество инцидентов информационной безопасности увеличилось на 20,8%. В исследовании учитывались только успешные кибератаки (инциденты), которые привели к негативным последствиям для компании или частного лица. Значительное влияние оказывает рост рынка киберпреступности: злоумышленники расширяют теневой бизнес. Тем временем в связи с массовыми утечками данных появляется возможность проведения атак с использованием скомпрометированной информации о пользователях. В 2023 году эти же причины послужат еще большему росту числа атак [1].

Представленные данные статистики подтверждают необходимость уделить особое внимание формированию эффективного комплекса мер и средств для обеспечения информационной безопасности объекта. Тренд на ухудшение показателей статистики сохраняется и в 2023 году, а это значит, что построение системы защиты информации на объекте является необходимым и экономически целесообразным решением.

Безусловно, у каждого объекта, обрабатывающего конфиденциальную информацию есть своя специфика при построении системы защиты. Однако в рамках статьи будет представлен общий поэтапный порядок разработки ффективного комплекса мер и средств для обеспечения информационной езопасности объекта, который применим для любого типа объекта.

Порядок разработки эффективного комплекса мер и средств для обеспечения информационной безопасности объекта включает в себя следующие этапы:

1. Проведение оценки соответствия требованиям действующего законодательства.
2. Изучение специфики и особенностей защиты рассматриваемого объекта.
3. Формирование перечня мер и средств для обеспечения информационной безопасности объекта.
4. Оценка экономической целесообразности внедрения разработанного перечня рекомендаций.

Далее более подробно будет описан каждый из представленных этапов.

Этап 1. Проведение оценки соответствия требованиям действующего законодательства.

Данный этап является базисным, поскольку помогает понять какие требования обязательно должны быть выполнены на объекте и какие из них уже выполнены.

Наиболее удобный способ проведения процедуры оценки соответствия – это составление общей таблицы. В рамках таблицы перечисляются требования законодательства, по каждому из которых расписывается перечень мер и средств, которые должны присутствовать на объекте для выполнения требования, перечень мер и средств, которые имеются на объекте, а также ставится отметка о выполнении (выполнено/не выполнено/выполнено частично). Данная таблица также упрощает процедуру прохождения организациями проверок от контролирующих ведомств, поскольку в документе описано каким образом соблюдены предъявляемые требования, что позволяет оперативно проверить факт его соблюдения.

Этап 2. Изучение специфики и особенностей защиты рассматриваемого объекта.

Цель данного этапа – подготовка к формированию перечня мер и средств защиты.

Для того чтобы предлагаемый перечень не был стандартным и формальным, до его формирования необходимо изучить ряд особенностей объекта.

К данным особенностям относятся:

1. Тип обрабатываемой информации (персональные данные, коммерческая тайна, иные ценные для организации сведения).
2. Тип объекта, в рамках которого ведется обработка конфиденциальной информации (ИСПДн, АСУ ТП, КИИ, ГИС).
3. Размер среднегодового чистого дохода организации.

4. Данные о ранее происходивших инцидентах информационной безопасности на объекте.
5. Данные об особенностях осуществления деятельности – порядок ведения документации, порядок соблюдения установленных правил, порядок обслуживания клиентов и т.д.

Изучение данных особенностей позволит более корректно оценить экономическую целесообразность обеспечения информационной безопасности объекта, подобрать наиболее подходящие средства защиты, детализировано и комплексно сформировать положения организационно-распорядительных документов.

Помимо этого, рассмотрение данных особенностей может поспособствовать внедрению средств и мер, которые не обязательны к внедрению с точки зрения соблюдения буквы закона, но эффективны для конкретных исходных данных. Например, в ряде организаций одной из дополнительных мер при обеспечении информационной безопасности может служить мотивационная политика для работников, вводящая гибкую систему поощрений за эффективную деятельность. Внедрение документа не является обязательным, однако если в организации наблюдается тенденция к реализации инцидентов ИБ со стороны внутренних работников, данная мера в комплексе с другими способна значительно улучшить ситуацию.

Этап 3. Формирование перечня мер и средств для обеспечения информационной безопасности объекта.

На данном этапе формируется перечень средств защиты необходимых к закупке и установке, а также перечень необходимых к разработке приказов. Данный этап обобщает два предыдущих. Все что на объекте должно быть согласно законодательству или в соответствии с особенностями объекта, должно быть внесено в перечень. При этом из перечня исключаются или же помечаются знаком выполнения те средств и меры, которые в соответствии с таблицей оценки соответствия (этап 1) были выявлены как имеющиеся.

Также важно при формировании перечня средств защиты учитывать тенденцию импортозамещения и предлагать средства, имеющие сертификат ФСТЭК и включенные в Единый реестр российских программ для ЭВМ и БД [2].

Этап 4. Оценка экономической целесообразности внедрения разработанного перечня рекомендаций.

Реализация данного этапа необходима для того, чтобы оценить целесообразность внедрения всех мер и средств защиты. Производится путем сравнения стоимости внедрения средств и мер защиты информации с суммой возможных издержек при отсутствии внедрения в процентном соотношении от чистого дохода.

В стоимость внедрения входят: стоимость самих средств защиты, стоимость обслуживания средств защиты в течении года (обновление ПО, техническое обслуживание, стоимость электроэнергии), затраты на внедрение (заработная плата специалистов).

В сумму возможных издержек входят: затраты на выплату штрафов согласно действующему законодательству, затраты на выплату исков (если иски

возможны, на основе сумм компенсаций, назначаемых по схожим судебным делам), затраты на восстановление оборудования (того, которое может быть повреждено при реализации кибератаки – АРМ, сервер и т.д.), предположительные финансовые потери от утраты конкурентного преимущества и репутации на рынке.

В случае если первый процентный показатель превышает второй или равен ему – необходимо пересмотреть сформированный перечень мер и средств на предмет снижения общей стоимости внедрения. В противном случае внедрение предложенного списка мер и средств экономически целесообразно.

Таким образом, предложенный в рамках статьи порядок разработки эффективного комплекса мер и средств для обеспечения информационной безопасности объекта учитывает все наиболее важные тонкости данной процедуры, универсален и может использоваться для объекта любой направленности и масштаба.

Список источников

2. Эксперты ИТ-компании «Инфосистемы Джет» о киберугрозах [Электронный ресурс] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id1 (Дата обращения: 3.05.2023).

3. Единый реестр российских программ для ЭВМ и БД [Электронный ресурс] – URL: https://reestr.digital.gov.ru/reestr/ (Дата обращения: 3.05.2023).

Статья поступила в редакцию 05.05.23; принята к публикации 10.05.2023.

Научная статья
УДК 623:74

Развитие и особенности применения беспилотных летательных аппаратов

Сергей Сергеевич Ващенко[1]✉, Алексей Андреевич Гарев[2], Владимир Владимирович Помещиков[3], Сергей Михайлович Каданцев[4]
[1, 2, 3, 4]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0006-5741-007X
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0003-6742-9266
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0004-9973-203X
[4]nauchnajarota@yandex.ru, https://orcid.org/0009-0006-2737-3239

Аннотация. В статье представлен обзор современных вариантов беспилотных летательных аппаратов, а также возможность применения многофункционального комплекса средств имитации радиоэлектронной обстановки (РЭО) на БЛА.

Ключевые слова: БЛА, средства имитации, РЭБ.

На данном этапе развития техники и технологий автоматизация приобретает всеобщий тренд. Огромное значение БЛА имеют для вооруженных сил, так как в силу своих особенностей имеют ряд таких преимуществ, как:

– низкая стоимость при условии равной эффективности выполняемых задач;

– отсутствие пилотов, что снижает риск гибели личного состава;

– экономия топлива;

– малый вес, позволяющий использовать электрические двигатели;

– существенное уменьшение взлетно-посадочного пространства;

– высокая оперативность применения;

– скрытность применения по причине малых размеров и использования синтетических материалов при изготовлении корпуса [4].

Одной из важнейших задач, которую выполняют БЛА является проведение воздушной разведки и определения расположения различных стратегических важных военных сил противника. К ним относятся командные пункты управления, оборонительные укрепленные позиции противника, дислокация средств противовоздушной обороны (ПВО), размещение боевых баз и складов вооружения, аэродромов, живой силы противника, базирование артиллерии, танковых и мотострелковых подразделений, реактивных систем залпового огня и другие различные вооруженные силы морских и сухопутных войск противника. При ведении боевых действий своевременно полученные результаты разведки тех или иных координат расположения сил противника позволяют, использовав имеющиеся ресурсы, уничтожить их. К примеру, при проведении разведки с использованием БЛА были получены координаты

дислокации танковой колонны или огневых позиций артиллерии. Эти данные позволят задействовать системы точного залпового огня, организовать засады для уничтожения, захвата подразделения сил противника при минимальных потерях со своей стороны. Также БЛА применяются для проведения разведывательных операций для определения координат размещения сил ПВО и других подразделений на территории противника. Подробные данные требуются во время разработки тактических операций с использованием воздушных сил для уничтожения стратегических объектов противника и контроля воздушного пространства вражеской территории.

Комплекс с БЛА «Гранат» предназначен:

– для дистанционного мониторинга подстилающей поверхности и различных объектов;

– сбора информации о противнике в труднодоступных участках местности;

– наблюдения за важнейшими коммуникациями (ж/д и автомобильными дорогами);

– обнаружении диверсионных групп и контроля результатов ударов по объектам противника;

– обеспечивает фото и видео съемками в режиме времени близкого реальному с указанием;

– воздушное наблюдение за противником на поле боя;

– для ведения воздушной фоторазведки объектов противника [5].

Данный БЛА имеет диапазон скоростей полета от 65 до 120 км/ч и максимальную высоту полета не выше 3000 м над уровнем моря. Максимальная дальность радиоканала управления и передачи видеоинформации (при условии прямой видимости) составляет 10 км. Имеет электрический двигатель. Запуск осуществляется с руки или катапульты, а посадка с использованием парашюта [4].

Хоть и различные БЛА выполняют различные функции по своему назначению, одним из наиболее применяемых аппаратов на вооружении ВС РФ является «Орлан-10». Он весит всего 14 килограммов, скорость полета 100-150 км/ч и способен осмотреть зону боевых действий на глубину до 120 километров, продолжительность же полета может достигать 16 часов. При этом передача информации осуществляется по высокозащищенному шифрованному каналу связи [1].

БЛА способен осуществлять корректировку огня артиллерии (в частности, модернизированных САУ «Мста-С» и САУ нового поколения «Коалиция»), иметь множество вариантов полезной нагрузки.

Так, например, эти БЛА могут использоваться для ведения радиотехнической разведки и даже осуществлять подавление тактических средств радиосвязи противника. И помимо всего прочего, сами «Орланы-10» способны объединяться в общую сеть, что многократно повышает их и без того высокую эффективность [4].

БЛА также можно использовать для проведения испытаний техники радиоэлектронной борьбы. В современных условиях широкого применения радиолокационных станций для наблюдения за различными объектами (целями)

с задачами обнаружения, распознавания, определения их местоположения, скорости и направления движения, а также управления ими (в транспортных системах) или поражения (в системах вооруженной борьбы с воздушным, морским или наземным противником) возникает высокая необходимость в системах и комплексах, предназначенных для проведения испытаний современного вооружения, военной и специальной техники, а также для подготовки соответствующих специалистов-операторов.

Рассмотрим многофункциональный комплекс средств имитации радиоэлектронной обстановки (РЭО) на БЛА. В состав комплекса будет входить автоматизированное рабочее место оператора, средства связи, БЛА самолетного или вертолетного типа, сменный программируемый модуль имитации БРЛС. Данный комплекс предназначен для имитации сигналов радиотехнических систем и моделирования различной обстановки, возникающей на экране РЛС. К примеру, вариант применения комплекса средств имитации на дистанционно-пилотируемом летательном аппарате заключается в том, что модуль имитации, закрепленный на дистанционно-пилотируемом летательном аппарате, имитирует заранее заданные радиотехнические сигналы. В это время наземный модуль радиоэлектронного подавления бортовой радиолокационной станции воздушного базирования, при проведении испытаний, производит подавление данного сигнала. Оператор средств радиоэлектронной борьбы наблюдает на пульте автоматизированного рабочего места отображение работы воздушной цели и ее перемещение в пространстве.

Главным достоинством многофункционального комплекса средств имитации является возможность создания очень сложной воздушной обстановки без полетов авиации, что снижает материальные и временные затраты, экономия ресурса техники при подготовке специалистов и операторов, возможность проведения комплексных тренировок подразделения (подразделений), создание обстановки при проведении тактических учений.

Беспилотную авиацию также можно использовать в гражданском направлении. Сферы применения гражданских беспилотников обширны, но одним из основных направлений является контроль технического состояния различных объектов, лесов и подконтрольных территорий. С помощью навесной аппаратуры БЛА производится мониторинг местности, что позволяет её при охране, исследовании труднодоступных мест планеты, а также поиске и спасении при ЧС. Также данные летательные аппараты применяются для транспортировки грузов, а в перспективе планируется создание БЛА для перевозки людей [4].

В настоящее время существует большое многообразие БЛА, которые различаются по своему назначению, типу применения, массогабаритным показателям, конструкции и по типу двигателя. Благодаря этому они имеют широкое применение в различных сферах деятельности. В первую очередь в военной сфере, так как имеют большую оперативность и скрытность применения, а также отсутствие пилотов, что снижает риск гибели личного состава в процессе выполнения поставленной задачи. Таким образом, разработка и использования беспилотных летательных аппаратов для военных и

гражданских потребностей является перспективными направлениями развития науки и техники, что способствует развитию этих сфер деятельности в целом, так и выполнению конкретных задач [4].

Список источников

1. Российские и зарубежные беспилотники. // Военный обзор. URL: https://militaryarms.ru/voennaya-texnika/aviaciya/bespilotnye-letatelnye-apparaty.

2. Румянцев П. Беспилотники в российской армии // Авиация, История ВПК и Военная история, Средства и Системы Безопасности. 2016. № 4(41). URL: https://dfnc.ru/aviazcia/bespilotniki-v-rossijskoj-armii.

3. Беспилотники: что ждет новую отрасль в России. URL: http://www.aviaport.ru/digest/2016/05/24/387099.html.

4. Сташкевич С.П., Кабанов В.А., Хуснутдинов Т.Д. Использование беспилотных летательных аппаратов в военных и гражданских целях // Актуальные проблемы авиации и космонавтики: сборник материалов V Международной научно-практической конференции, посвященной Дню космонавтики / под общей редакцией Ю. Ю. Логинова. – Красноярск: Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, 2019. - Том 1. – С. 171-173.

5. http://bastion-opk.ru/granat-1/.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Ващенко С.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Гарев А.А. – старший оператор научной роты войск радиоэлектронной борьбы.

Помещиков В.В. – оператор научной роты войск радиоэлектронной борьбы.

Каданцев С.М. – начальник цикла боевой подготовки (специалистов комплексов радиоэлектронной борьбы на беспилотных летательных аппаратах и средств комплексного технического контроля).

Вклад авторов

Ващенко С.С. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Гарев А.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Помещиков В.В. – сбор материала, обработка материала, частичное написание статьи (25%).

Каданцев С.М. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.53

Исследование механизмов безопасности гипервизора Hyper-V

Лидия Андреевна Виткова [1], Анастасия Леонидовна Зрелова [2]✉
[1,2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия
[1]vitkova@comsec.spb.ru
[2]nastyzr@gmail.com✉

Аннотация. Статья посвящена проблеме безопасности гипервизоров. Особое внимание уделяется механизмам обеспечения безопасности гипервизора. Отдельно проведен разбор механизмов защиты от типовых атак на виртуальную машину. В работе проведен анализ механизмов безопасности различных гипервизоров и сравнение их доли на рынке виртуальных машин.

Ключевые слова: Hyper-V, механизмы безопасности, гипервизор.

До появления виртуализации и создания гипервизоров оборудование было привязано к одной операционной системе и работало только в одном режиме либо как рабочая станция, либо как сервер. Из-за этого для создания IT-инфраструктуры требовалось несколько физических ресурсов. Виртуализация и гипервизоры, предлагающие различные соотношения аппаратного обеспечения к операционным системам позволили сократить расход физических ресурсов. На данный момент существует множество различных гипервизоров. В данной работе рассмотрим методы обеспечения безопасности, которые нам предлагает компания Microsoft в своем гипервизоре Hyper-V. Hyper-V был выпущен 26 июня 2008 как компонент новой серверной операционной системы и представляет собой продукт виртуализации оборудования Microsoft для x64-систем.

Механизмы безопасности, реализуемые в гипервизоре Hyper-V [1]:

1. Защита памяти. Гипервизор разделяет память физического устройства между виртуальными машинами. Совместное использование одной и той же области памяти разными виртуальными машинами невозможно, т.к. область памяти доступна для использования только одной машине. Гипервизор может изменить права доступа к области памяти (переназначить права на чтение области памяти или лишить прав доступа). Также гипервизор поддерживает технологию динамического распределения памяти, т.е. выделение памяти осуществляется во время выполнения программы.

2. Защита системы ввода и вывода. Ни одному из разделов не разрешено записывать данные в область гипервизора. Только основная операционная система может настраивать правила доступа к устройствам ввода/вывода для других виртуальных машин.

3. Разграничение прав на группы виртуальных машин. Администрировать разделы и управлять доступом ко всем ресурсам, которые не подчиняются

гипервизору, может только родительский раздел. Родительский раздел решает задачи централизованного управления питанием и событиями при аппаратных сбоях.

4. Механизм защиты доступа к гипервызовам. Гипервызов – вызов заданной функции в гипервизоре с помощью инструкции vmcall (для процессоров Intel). При создании виртуальных машин задаются привилегии, которые предоставляют возможность выполнения конкретных гипервызовов.

5. Интеграция с Authorization Manager. В Hyper-V создавать и управлять виртуальными машинами может только пользователь с правами администратора. Authorization Manager позволяет обеспечить ролевое управление виртуальными машинами.

6. SID виртуальной машины. SID – уникальный номер, присваиваемый каждой виртуальной машине. Данный номер используется при настройке прав доступа к физическим файлам, в которых хранятся образы машин и данные. SID так же можно использовать для изолирования процесса работы одной виртуальной машины от другой.

7. Защита от несанкционированного копирования образа диска виртуальной машины. Защита от несанкционированного копирования достигается с помощью зашифрованной файловой системы (Encrypting File System Microsoft).

8. Защита от несанкционированного запуска виртуальной машины. Запретить запуск виртуальной машины Windows возможно при помощи задания системного пароля для операционной системы. Операционная система будет ожидать ввода пароля после сбоя или автоматического перезапуска системы.

9. Защита от компрометации образов (шаблонов). Offline Virtual Machine Servicing Tool позволяет обновлять виртуальные машины, находящиеся в выключенном состоянии. Виртуальные машины запускаются, обновляются до нужного уровня безопасности и возвращаются в выключенное состояние.

10. Защита от несанкционированного доступ к VLT (Virtual Tape Library). В Windows Server 2016 появилась поддержка виртуального безопасного режима (VSM). VSM предотвращает доступ процессов, выполняющихся в одном VTL, к памяти другого VTL.

11. Безопасное развертывание приложений. Развертывание политик управления приложениями защитника Windows – модуль, который отвечает за политику доступа к приложениям и библиотекам. Управление приложениями может уменьшить угрозы безопасности, ограничив приложения, которые могут запускать пользователи, и код, который выполняется в ядре System Core.

12. Изоляция Hyper-V. TrustAccess — распределенный межсетевой экран 2-го класса, предоставляемый компанией «Код Безопасности».

В Windows Server 2016 Hyper-V Microsoft представлены экранированные виртуальные машины. Экранированная виртуальная машина – это виртуальная машина 2-го поколения с виртуальным доверенным платформенным модулем, шифруемая с помощью BitLocker, и возможностью выполняться только на работоспособных и утвержденных узлах. В этих машинах появился метод для защиты виртуальных дисков. Данный метод не позволяет неавторизованным хостам подключать виртуальные жесткие диски с экранированных виртуальных машин. Для защиты 2-го поколения машин появилось ограничение для виртуального диспетчера

подключений (VMConnect). Никто не может использовать VMConnect для подключения к экранированной виртуальной машине, даже администраторы [2, 3].

Рассмотренные основные механизмы защиты Hyper-V достаточно эффективны, но они не могут защитить систему он целенаправленных атак. Для предотвращения этих атак гипервизор имеет особые технологии. Рассмотрим типовые атаки на виртуальную машину и способы защиты гипервизора от них [4, 5]:

1.Атака типа «отказ в обслуживании» (DoS). Для предотвращения данной атаки в гипервизоре возможно настроить ограничения использования процессора гостевыми операционными системами.

2.Атака со стороны администратора среды. В гипервизоре Hyper-V от этих атак защищает технология Shielded VMs. Данная технология позволяет создать защищенные виртуальные машины.

3.Атака на учетные данные домена. Защита учетных данных достигается с помощью Credential Guard. Создается виртуальный контейнер, где хранятся все секреты домена, но система не может напрямую обращаться к ним.

4.Атака переполнения буфера. Для предотвращения данных атак для гипервизора Hyper-V требуется применение DEP. DEP – это метод предотвращения переполнения буфера, блокирующий внедрение вредоносного исполнимого кода в буферы данных системной памяти [6].

5.Атака типа «человек посередине». Чтобы предотвратить атаки этого типа используется SMB 3,0 для сквозного шифрования данных SMB и защиты данных и перехвата в ненадежных сетях, также используется частная сеть для доступа к содержимому общего ресурса SMB.

6.Атака, нацеленная на повреждение памяти. Для защиты от данных атак используется метод рандомизации компоновки адресного пространства (ASLR). Чтобы предотвратить переход злоумышленника к определенной используемой функции в памяти, ASLR случайным образом упорядочивает позиции адресного пространства ключевых областей данных процесса, включая базу исполняемого файла и позиции стека, кучи и библиотек.

7.Атака руткитов и буткитов в процессе загрузки. До появления 2-го поколения виртуальных машин Hyper-V не было механизмов, позволяющих защитить систему от руткитов и буткитов в процессе загрузки. В новом поколении виртуальных машин BIOS был заменен на firmware на базе UEFI и добавилась поддержка технологии Secure Boot. Secure Boot – это функция безопасной загрузки.

8.Escape-атака («побег» виртуальной машины). Данные атаки позволяют злоумышленникам запускать код на виртуальной машине, который позволяет операционной системе, работающей в ней, выйти и напрямую взаимодействовать с гипервизором. При обработке входящих FileGroupDescriptorW форматов файлов клиент передает формат новой функции, которая проверяет структуру большого двоичного объекта.

9.Атака с использованием вредоносной гостевой виртуальной машины. Этот класс атак можно устранить, настроив использование планировщика Core и перенастроив гостевые виртуальные машины.

10. Атака на файловую систему. Для защиты от данного типа атак в гипервизоре используется access control lists (ACLs) и инструменты управления и обеспечения

безопасности System Center Virtual Machine Manager или Authorization Manager, которые беспечивают разграничение прав доступа на виртуальные машины.

11. Атака Pass-the-Hash. Для защиты от данного типа атак Windows позволяет отключить кэширование учетных записей, чтобы злоумышленник не смог добраться до хэшей в памяти. Следует придерживаться принципа минимальных привилегий.

Hyper-V - коммерческое ПО от компании Microsoft. Hyper-V отлично работает в инфраструктуре Windows. KVM – продукт с открытым исходным кодом. KVM развивается вместе с дистрибутивами, такими как RHEV от Red Hat [7].

Сравним использование гипервизоров в различных отраслях (табл. 1).

Таблица 1

Использования гипервизоров в различных отраслях, %.

Отрасль использования	Гипервизор	
	Hyper-V	KVM
Финансы	13	21
Транспорт	9	11
Производство	7	7
Госсектор	7	7

Анализ основных механизмов безопасности гипервизоров Hyper-V, ESXi и KVM можно представить в виде таблицы (табл.2).

Таблица 2

Основные механизмы безопасности гипервизоров Hyper-V, ESXi и KVM

Критерий	Гипервизор		
	Hyper-V	ESXi	KVM
Доверенный платформенный модуль (Trusted Platform Module)	Поддерживает (используется в технологии BitLocket)	Поддерживает (используется для защиты модулей VMkernel)	Не поддерживает
Шифрование при миграции	Encrypt State и VM migration traffic	Encrypted vSphere vMotion	data-declassification
Шифрование дисков	BitLocket	VM Encryption	Аппаратное шифрование полного диска (FDE)
Запрет сканирования сетевого трафика	Технология Shielded VMs	Политика сетевой безопасности	Создание правила в брэндмауэр или Null route
Безопасная загрузка	Поддерживает	Поддерживает	Поддерживает
Разграничение доступа	Authorization Manager	Роли настраиваются в vCenter	SELinux

По результатам сравнения было выявлено, что в Hyper-V, как и в остальных рассматриваемых гипервизорах, присутствуют основные механизмы обеспечения безопасности. Для реализации некоторых механизмов Hyper-V потребовалась интеграция с уже готовыми технологиями, в отличие от других гипервизоров. Данное исследование не позволяет дать точного ответа, какой гипервизор предоставляет более защищенную систему виртуализации, поэтому требуется (дополнительное) другое исследование.

С момента выпуска Hyper-V, безопасность гипервизора претерпела большие изменения. Для обеспечения безопасности используются как классические методы обеспечения безопасности, так и специфичные методы, созданные специально для защиты виртуальной среды.

Список источников

1. Защищаем Hyper-V | Windows IT Pro/RE | Издательство «Открытые системы» — URL: https://www.osp.ru/winitpro/2009/03/7274076 (дата обращения: 1.12.2022).

2. Платунова, С. М. Администрирование вычислительных сетей на базе MS Winsows Server ® 2008 R2 : учебное пособие / С. М. Платунова. — Санкт-Петербург : НИУ ИТМО, 2013. — 127 с. — Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/70799 (дата обращения: 09.12.2022). - Режим доступа: для авториз. пользователей.

3. Обзор защищенной структуры и экранированных виртуальных машин - URL: https://learn.microsoft.com/ru-ru/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms (дата обращения: 09.12.2022).

4. Hyper-V Security или безопасность Hyper-V | ITband.ru. - URL: http://itband.ru/2009/09/hyper-v-security/#1 (дата обращения: 10.12.2022).

5. Фомин А.А. Информационная безопасность виртуальной среды. Информационные системы и технологии. 2008. № 1-4. С. 268-271

6. Средства безопаности Hyper-V в системе Windows Server 2008 Жан де Клерк Windows 2000 Magazine/Re. 2010. № 3. С. 20-25.

7. Знакомство с Hyper-V в Windows 10 - URL: https://learn.microsoft.com/ru-ru/virtualization/hyper-v-on-windows/about/ (дата обращения 09.12.2022).

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Виткова Л.А. – к.т.н., доцент кафедры «Защищенные системы связи» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

Зрелова А.Л. – магистрант кафедры «Защищенные системы связи» Института магистратуры, направления подготовки 11.04.02 –Инфокоммуникационные технологии и системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

Научная статья
УДК 004.056

Порядок формирования политики информационной безопасности для объекта

Анна Николаевна Вишнякова [1]✉, Оксана Михайловна Голембиовская[2], Екатерина Владимировна Кондрашова[3], Кирилл Евгеньевич Шинаков[4]
[1, 2, 3,4] Брянский государственный технический университет, Брянск, Россия
[1] vshnv.a@yandex.ru✉,
[2] bryansk-tu@yandex.ru,
[3]kondrashova_katerina@bk.ru,
[4]shinakov@it-craft.net,

Аннотация. В любой организации очень важно уметь исследовать риски и их актуальность, которые могут принести ущерб. Для защиты информации организации прибегают к решению создания политики безопасности. Составляется документ, программа которого должна обеспечить безопасность информации.

Ключевые слова: политика информационной безопасности, персональные данные, защита информации.

Защита информационной безопасности важная часть в функционировании организации любого масштаба. Одним из центральных аспектов при построении защиты, на котором в последствии базируются все остальные, является организационное обеспечение защиты информации. В рамках данной статьи упор сделан на порядок разработки организационных документов, для объектов, обрабатывающих ПДн, поскольку количество таких объектов очень велико и практически любая организация обрабатывает персональные данные. Однако предложенные рекомендации могут быть экстраполированы и на другие типы объектов.

Утвержденная на объекте документация по защите информации должна быть структурной, понятной с точки зрения применения описанных в ней алгоритмов, а также удовлетворять всем требованиям, предъявляемым со стороны законодательства (ФЗ № 152 «О персональных данных», Постановление Правительства №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК № 21). В то же время при разработке документов должна быть поставлена задача максимальной компактности, чтобы прописать все необходимые требования и процедуры и при этом не наплодить большое количество дублирующих друг друга документов.

Политика безопасности должна описывать все аспекты безопасности в организации, включая правила доступа к данным, управление учетными

записями пользователей, управление сетевой инфраструктурой, а также меры по защите от внешних и внутренних угроз [1].

Важно чтобы политика включала в себя ключевые инструкции по соблюдению информационной безопасности организации и была документом первого уровня на основе которого базируется другая документация – приказы о назначении ответственных лиц, локальные инструкции отделов, должностные инструкции работников предприятия, регламенты, положения и т.д.

Перед началом формирования документа следует провести подготовительную работу, в рамках которой необходимо выписать все требования предъявляемые со стороны законодательства к операторам ПДн в единую таблицу и скомпилировать построчно созвучные требования. Данный шаг позволит увидеть целостную картину предъявляемых требований и избежать дублирования информации при составлении текста Политики. Фрагментарный пример составления подобной таблицы представлен в табл.1.

Таблица 1

Пример таблицы структурирования требований законодательства

ФЗ «О персональных данных» от 27.07.2006 N 152-ФЗ	*Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»*	*Приказ № 21 от 18.02.2013 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»*
Ст. 19. 3) следует использовать средства защиты информации, которые прошли процедуру соответствия	13. г) нужно использовать средства защиты информации, соответствующие всем требованиями в области обеспечения информации	
Ст. 19. 5) машинные носители ПДн следует подвергать учету	13. б) для всех носителей ПДн нужно обеспечить	4. Машинные носители ПДн подлежат защите 11. Защита технических средств

После того как таблица составлена, можно переходить непосредственно к формированию текста Политики. В качестве изначального базиса рекомендуется взять требования таблицы из Приказа ФСТЭК №21 и по пунктам для каждого требования расписать порядок его реализации на объекте. Выбрать именно этот документ предлагается потому, что он наиболее подробный и всеобъемлющий с точки зрения требований и дублирует другие документы во многих пунктах по реализации, если взять его за основу, то в последствии останется дописать небольшое количество пунктов, которые учитываются только в иных документах.

Документ Политики следует начинать с общих положений – целей и задач политики, используемых сокращений и ключевых определений, а затем переходить к основному тексту. При этом сам текст наиболее оптимально делать с как можно большим количеством отдельных подразделов и списков, для того чтобы упростить его изучение, и чтобы при необходимости можно было быстро найти порядок реализации того или иного требования.

При формировании документа Политики также рекомендуется рядом с каждым отдельным разделом или подразделом подписывать пункт нормативно-правового документа, соответствие которому обеспечивает этот фрагмент. Это упростит процедуру проверок документации объекта со стороны проверяющих органов, а также ускорит процессы внутреннего аудита и оценки соответствия.

Далее представлен фрагментарный пример сформированного раздела политики информационной безопасности объекта.

---

1. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА

1.1. Идентификация и аутентификация пользователей, являющихся работниками оператора (при работе с ИСПДн {Организации}). (соответствие п. ИАФ.1 приказа ФСТЭК России № 21)

Идентификация и аутентификация пользователей, являющихся работниками оператора производится при работе с ИСПДн {Организации}. При входе в ИСПДн пользователь вводит логин и пароль, выданный администратором безопасности.

Пароль для входа в ИСПДн меняется администратором безопасности один раз в месяц путем генерации в специализированном ПО.

Пароль выдается администратором безопасности пользователю лично (при посещении администратора) в закрытом конверте.

1.2. Порядок идентификации и аутентификация устройств (в том числе стационарных, мобильных и портативных). (соответствие п. ИАФ.2 приказа ФСТЭК России № 21)

Для исключения возможности подключения стационарных, мобильных и портативных устройств все возможные пути подключения к ПК/серверу должны иметь пароль (Wi-fi), а также должны быть настроены групповые политики управления доступом к операционной системе по отключению возможности использования всех или выбранных USB портов.

Администратор безопасности раз в месяц меняет пароль, а также проверяет корректность настройки политик доступа.

Пароль выдается только работникам {Организации}.

1.3. Порядок управления идентификаторами. (соответствие п. ИАФ.3 приказа ФСТЭК России № 21)

Управление идентификаторами учетных записей производится в рамках выполнения процедур создания пользователя и группы, модификации пользователя и группы, а также удаления пользователя и группы.

Управление идентификаторами производится исключительно администратором информационной безопасности.

Возможные операции:

• создание, удаление, блокировка, редактирование свойств учетной записи;

• создание, присвоение, удаление аппаратных идентификаторов.

Таким образом, представленные рекомендации позволяют для любого объекта составить комплексный организационные документ – Политику информационной безопасности, который будет являться базисом при налаживании процессов обеспечения защиты информации на объекте.

Список использованных источников.

1. Голембиовская О.М. Формализация подходов к обеспечению защиты персональных данных : монография / Голембиовская О.М., Рытов М.Ю., Шинаков К.Е.. — Саратов : Ай Пи Эр Медиа, 2019. — 198 с. — ISBN 978-5-4486-0726-4. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/81851.html (дата обращения: 14.03.2023).

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Вишнякова А.Н. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Голембиовская О.М. - доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Кондрашова Е.В. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Шинаков К.Е. - доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Вишнякова А.Н. – идея, сбор материала (25%).

Голембиовская О.М. – обработка материала, частичное написание статьи (25%).

Кондрашова Е.В. – обработка материала, написание статьи (25%).

Шинаков К.Е. – написание статьи, научное редактирование текста (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004:056

Разработка подхода к классификации компьютерных преступлений

Анна Николаевна Вишнякова[1]✉, Максим Михайлович Голембиовский[2]✉, Екатерина Владимировна Кондрашова[3]✉, Кирилл Евгеньевич Шинаков[4]✉

[1,2,3,4]Брянский государственный технический университет, Брянск, Россия
[1]vshnv.a@yandex.ru✉
[2]maksim32region@yandex.ru✉
[3]kondrashova_katerina@bk.ru✉
[4]shinakov@it-craft.net✉

Аннотация. Компьютерные преступления это действия, совершаемые с целью получения, а также применения информации в компьютерной сфере. Компьютерная информация может быть, как предметом, так и средством совершения правонарушения. К таким преступлениям относятся любого рода преступления, связанные с компьютерной техникой, которые при этом противоречат праву. В данной статье рассматривается класс компьютерных преступлений.

Ключевые слова: компьютерные преступления, информационные преступления, информация.

Компьютерные преступления это предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть [1].

К наиболее типичным целям совершения компьютерных преступлений относятся следующие:

- подделка платежных документов:
- хищение денежных средств;
- получение компромата или засекреченного материала;
- кража машинного времени:
- продвижение по карьерной лестнице;
- получение поддельных документов;
- внесение вредоносных изменений в программное обеспечение;
- совершение покупок с фиктивной оплатой и др.

Отличительными особенностями данных преступлений являются низкая гласность, большой материальный ущерб, сложность сбора доказательств, характер производимых действий, а также специфичность самих преступников. Чаще всего подобные преступления совершают высококвалифицированные

программисты.

Низкая гласность компьютерных преступлений обусловлена тем, что многие организации разрешают конфликт своими силами. Потому что убытки от расследования могут оказаться выше суммы причиненного ущерба, например изъятие сервера для проведения экспертизы может привести к остановке работы на срок до двух месяцев, что повлечет за собой значительные потери финансовых средств за счет простоя) [1].

Классификация преступлений необходимо для того, чтобы понять, как наиболее быстро и эффективно провести процедуру его расследования.

Весь пласт наиболее часто встречающихся компьютерных преступлений можно условно разделить на 2 класса.

Класс 1 – преступления, совершенные посредством атаки на конкретные системы со стороны человека.

Класс 2 – преступления, совершенные посредством внедрения вредоносного ПО.

Для того чтобы определить к какому классу относится компьютерное преступление, предлагается методика анкетирования (таблица 1). В анкете представлены утверждения связанные с последствиями реализации компьютерных преступлений, если утверждение соответствует действительности – ответ «Да», в противном случае ответ «Нет».

Таблица 1

Определение класса компьютерного преступления

№ п/п	Вопрос	Ответ	
		Да	Нет
1	При реагировании на инцидент на экране монитора было представлено сообщение о шифровании сервера (данных)	1	0
2	Последствия инцидента носят полностью или частично хаотичный характер – нельзя сделать вывод что уничтожен (скопирован) только конкретный тип данных	1	0
3	На панели инструментов компьютера появились новые значки	1	0
4	Антивирусное ПО отключено	1	0
5	При открытии программ и файлов загрузка происходит очень медленно	1	0
6	При включении устройства появляется сообщение BSoD	1	0
7	Закрыт доступ к Панели управления и к Параметрам	1	0
8	Замечены ошибки в работе непрограммируемых технических средств	1	0

В случае если по результатам анкетирования получен 1 балл и более – преступление относится к классу 2. Если результат анкетирования 0 баллов – преступление относится к классу 1. При этом нельзя со стопроцентной вероятностью определить класс преступления до проведения расследования,

поскольку преступления 1 класса могут быть замаскированы под 2. Но даже приблизительная оценка принадлежности преступления к конкретному классу может упростить процедуру расследования.

Преступления 1 класса как правило сложнее предотвратить на этапе реализации, поскольку совершение подобных преступлений требует подготовки преступника, изучения системы и всех ее особенностей, а соответственно и поиска способов остаться незамеченным.

Преступления 2 класса, напротив, сложнее расследовать после реализации, поскольку вредоносное ПО обычно действует нецеленаправленно и может уничтожить, копировать или изменить не только те файлы, которые изначально являлись целью преступника, но и множество других, что в конечном итоге запутывает следствие и затрудняет процессы определения мотивов. При этом, в случае наличия на объекте антивирусных систем, SIEM-систем, систем обнаружения вторжений, можно полностью предотвратить реализацию преступления 2 класса или минимизировать его последствия.

Таким образом, предложенная классификация может быть полезна при выборе методики расследования преступлений, а также при их регистрации для дальнейшего анализа и внедрения средств предотвращения реализации схожего преступления в дальнейшем.

Список источников

1. Информационная безопасность и защита информации : сборник студенческих работ: студенческая научная работа. - Москва: Студенческая наука, 2012.

2. Костин В.Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей: учебное пособие / В.Н. Костин. — Москва: Издательский Дом МИСиС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — URL: https://www.iprbookshop.ru/98200.html (дата обращения: 13.03.2023).

Статья поступила в редакцию 10.04.23; принята к публикации 10.05.2023.

Информация об авторах

Вишнякова А.Н. – студент кафедры «Системы информационной безопасности», направление подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Голембиовский М.М. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Кондрашова Е.В. – студент кафедры «Системы информационной безопасности», направление подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Шинаков К.Е. – доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Вишнякова А.Н. – сбор материала, частичное написание статьи (30%).

Голембиовский М.М. – идея, научное редактирование текста, частичное написание статьи (27%).

Кондрашова Е.В. – идея, сбор материала, частичное написание статьи (26%).

Шинаков К.Е. – идея, научное редактирование текста (17%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Обзор основных SIEM-систем, представленных на российском рынке

Анна Николаевна Вишнякова[1]✉, Артем Андреевич Рябцев[2], Екатерина Владимировна Кондрашова[3], Кирилл Евгеньевич Шинаков[4]

[1, 2, 3,4] Брянский государственный технический университет, Брянск, Россия

[1] vshnv.a@yandex.ru✉,

[2]ryabcev@yandex.ru

[3]kondrashova_katerina@bk.ru,

[4]shinakov@it-craft.net,

Аннотация. Выбор представленных на рынке SIEM-систем огромен. Все решения имеют схожую систему функционирования, однако у каждой из них есть свои тонкости и особенности. SIEM-системы предназначены для непрерывного отслеживания сетевых событий и информирования пользователя о нетипичных и аномальных случаях.

Ключевые слова: информационная безопасность, мониторинг, сетевые события.

В сборе и анализе различных данных, связанных с информационной безопасностью (журналы аудита, обнаружение вторжений и т.д.) помогают SIM - системы. За обработку событий безопасности, например сигналы от систем мониторинга и детекторов нарушений отвечают SEM-системы.

Анализ и генерация уведомлений о нарушениях или попытках вторжения берут на себя SIEM - системы, которые объединяют данные от SIM и SEM систем. Также системы могут предоставлять отчеты и анализы по состоянию безопасности организаций.

Благодаря быстрому обнаружению и реагированию, SIEM - системы используются для мониторинга и поиска уязвимостей, а также для соответствия требованиям по информационной безопасности. SIEM-системы в качестве самостоятельного решения не предназначены и не способны предотвращать инциденты нарушения информационной безопасности. Они предназначены для непрерывного отслеживания сетевых событий и информирования пользователя о нетипичных и аномальных случаях [1].

В таблице 1 представлен сравнительный обзор ведущих SIEM-систем, представленных на российском рынке [2].

Таблица 2

Сравнительный обзор ведущих SIEM-систем

Критерий сравнения	RuSIEM	MaxPatrol SIEM	Kaspersky Endpoint Detection and Response	Wazuh
Язык поддержки	Русский и английский	Русский	Русский и английский	Английский
Схема продаж	Смешанная	Партнерская	Смешанная	Открытый код
Цена	Есть бесплатная версия, 10 млн. руб.	16 млн. руб.	10 млн. руб.	Бесплатно
Ориентировочный срок внедрения	До 2-3 недель. Зависит от гетерогенности и и специфичных источников	От 1 месяца	От 1 месяца	От 1 месяца
Крупнейшее из известных внедрений в России	Нет данных	ГК Росатом	VimpelCom	Wildberries
Секторы экономики, в которых могут быть выполнены внедрения	Госсектор, промышленность, коммерческий сектор, процессинг, банки, интернет-коммерция, реклама	Финансы, госсектор, энергетика, промышленность, связь, торговля	Финансы, государственный сектор, промышленность, связь, торговля, здравоохранение	Финансы, промышленность, связь, торговля, здравоохранение
Включена в реестр Российского ПО	Приказ Минкомсвязи РФ от 15.08.2017 № 421, Приложение 1, № пп. 25, реестровый № 3808.	Приказ Минкомсвязи РФ от 15.08.2017 № 421, Приложение 1, № пп. 25, реестровый № 1143	Приказ Минкомсвязи РФ от 15.08.2017 № 421, Приложение 1, № пп. 25, реестровый № 5162	Нет
Сертификат ФСТЭК России	Сертификат №4402 от 12.05.2021 до 12.05.2026	Сертификат №3734 от 12.04.2017 до 30.03.2026	Нет	Нет

Пути эскалации инцидента	Эскалация вручную с возможностью изменения критичности, темы и описания	Автоматическая маршрутизация инцидента при наличии условий	Ручная	Ручная
Агрегация по типу событий	Нет	Да	Да	Да
Нормализация событий	Да	Да	Да	Да
Корреляция по историческим данным	Нет	Нет	Нет	Нет
Формирование и рассылка отчетов	Формирование отчетов по активам, событиям, инцидентам, по расписанию	Формирование отчетов по активам, событиям, инцидентам, по расписанию	Формирование отчетов по активам, событиям, инцидентам, по расписанию	Формирование отчетов по активам, событиям, инцидентам, по расписанию
Обновление предустановленных компонентов (отчеты, правила корреляции)	1-2 раза в неделю и чаще	На партнерском портале может выдаваться по запросу	С различной периодичностью	С различной периодичностью

Таким образом, выбор представленных на рынке SIEM-систем многогранен. Все представленные решения имеют схожую систему функционирования, однако у каждой из них есть свои тонкости и особенности. Применяя представленную таблицу, оператор сможет выбрать для своего объекта наиболее подходящее по всем параметрам решение.

Список использованных источников.

1. Абденов А.Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / Абденов А.Ж., Трушин В.А., Сулайман К.. — Новосибирск : Новосибирский государственный технический университет, 2018. — 122 с. — ISBN 978-5-7782-3603-5. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91179.html (дата обращения: 13.03.2023).

2. Королев И.Д., Попов В.И., Ларионов В.А., Литвинов Е.С. Обзор siem -систем: проприетарные arcsight и maxpatrol против open - source решений // Дневник науки. - № 4 (28). – 2019.

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Вишнякова А.Н. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Рябцев А.А. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Кондрашова Е.В. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Шинаков К.Е. - доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Вишнякова А.Н. – идея, сбор материала (25%).

Рябцев А.А. – обработка материала, частичное написание статьи (25%).

Кондрашова Е.В. – обработка материала, написание статьи (25%).

Шинаков К.Е. – написание статьи, научное редактирование текста (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Описание порядка взаимодействия Роскомнадзора с операторами в рамках ведения реестра учета инцидентов в области персональных данных

Анна Николаевна Вишнякова [1]✉, Артем Дмитриевич Ященко[2], Алексей Петрович Горлов[3], Оксана Михайловна Голембиовская[4]
[1, 2, 3,4] Брянский государственный технический университет, Брянск, Россия
[1] vshnv.a@yandex.ru✉
[2] tema_96bryansk@mail.ru
[3] apgorlov@gmail.com
[4] bryansk-tu@yandex.ru

Аннотация. Предотвращение инцидентов информационной безопасности на сегодняшний день является одним из самых важных вопросов в этой сфере. Для более эффективной защиты персональных данных существует система взаимодействия операторов ПДн с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Ключевые слова: ПДн, информационная безопасность, Роскомнадзор.

Важность защиты информации в современном мире нельзя переоценить. Большое значение в этой сфере имеет работа по недопущению и предотвращению инцидентов информационной безопасности. Для того чтобы эта работа была комплексной и эффективной, а также с учетом имеющегося успешного опыта, разработана система взаимодействия операторов ПДн с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор, РКН) [1].

С 2023 года уведомление РКН о произошедшем инциденте и о результатах его расследования является обязательной процедурой.

Новый алгоритм взаимодействия значительно упростит механизм фиксации различных случаев утечки и в последствии сократит их количество. На рис. 1 схематично представлена идеальная схема взаимодействия по новому Порядку.

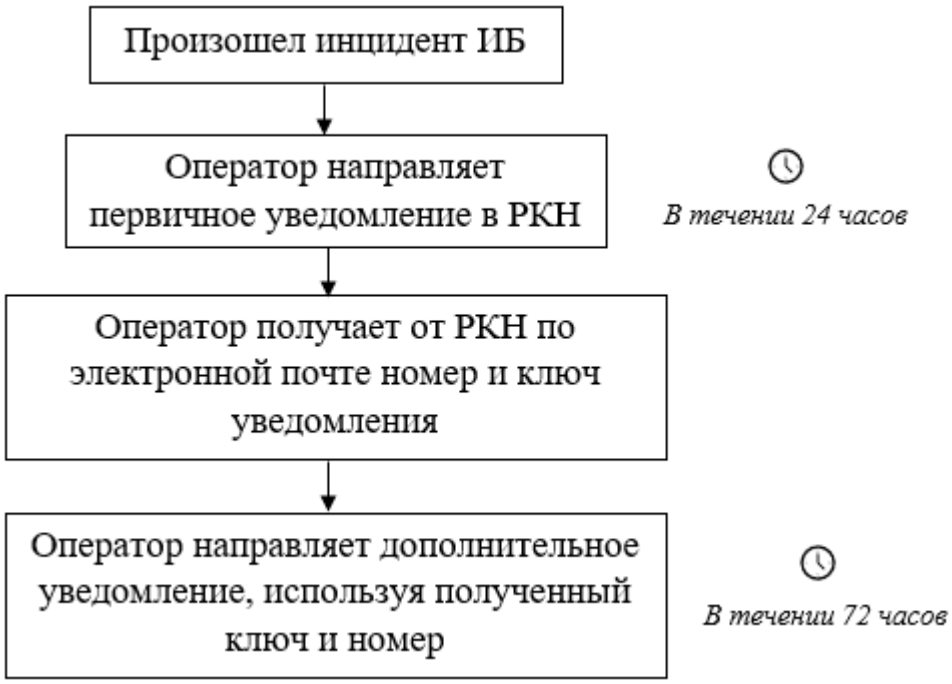

Рис.1 Идеальная схема взаимодействия РКН и оператора по новому Порядку

Первичное уведомление должно содержать информацию о произошедшем инциденте, предполагаемых причинах и вреде, нанесенном правам субъектов персональных данных, принятых мерах по устранению последствий инцидента, а также лице, уполномоченном на взаимодействие с РКН, данные оператора и иные сведения, и материалы, имеющиеся в распоряжении оператора [2].

Дополнительное уведомление должно содержать сведения о результатах внутреннего расследования и лицах, ответственных за инцидент. Если оператор уже провел внутреннее расследование на момент направления первичного уведомления, он может указать соответствующие сведения в нем [2].

В утвержденном порядке также предусмотрен ряд частных случаев, которые могут произойти в рамках взаимодействия РКН и оператора – оператор может направить неполные или некорректные сведения, не прислать дополнительное уведомление, обнаружить повторный инцидент с той же базой данных, отправить некорректную информацию, не касающуюся инцидента ИБ. РКН в свою очередь может раньше оператора обнаружить утечку данных [2].

На рис. 2 и 3 показана схема действий при каждой из упомянутых ситуаций.

Рис. 2 Частные случаи взаимодействия, инициируемые оператором

Рис. 3 Порядок взаимодействия, если инцидент ИБ выявлен РКН

Таким образом, представленный документ является комплексным и структурным и предусматривает все возможные случаи взаимодействия

оператора и Роскомнадзора в рамках ведения реестра учета инцидентов в области персональных данных.

Список использованных источников.

1. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2022 года № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных» Режим доступа: https://www.audar-info.ru/na/editArticle/index/type_id/5/doc_id/37369/release_id/72194/ (дата обращения: 14.03.2023).

2. Рулева А.К. Изменения в законодательстве о персональных данных с 01.03.2023 // Студенческий вестник. - 2023. - № 9 – 2 (248). – С. 19 – 23.

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Вишнякова А.Н. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Яценко А.Д. – аспирант кафедры «Компьютерные технологии и системы» ФГБОУ ВО «БГТУ».

Горлов А.П. - доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Голембиовская О.М. - доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Вишнякова А.Н. – идея, сбор материала (25%).

Яценко А.Д. – обработка материала, частичное написание статьи (25%).

Горлов А.П. – обработка материала, написание статьи (25%).

Голембиовская О.М. – написание статьи, научное редактирование текста (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 623:74

Применение имитатора радиотехнических сигналов на беспилотных летательных аппаратах

Алексей Андреевич Гарев[1]✉, Сергей Сергеевич Ващенко[2], Елисей Александрович Гвоздев[3], Вадим Алексеевич Корягин[4]
[1,2,3,4]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0003-6742-9266
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0006-5741-007X
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0005-3941-1477
[4]nauchnajarota@yandex.ru, https://orcid.org/0009-0007-8209-9495

Аннотация. В статье представлен обзор современных БПЛА и рассмотрена возможность применения имитатора радиотехнических сигналов на БПЛА для создания на его основе многофункционального комплекса средств имитации сложной РЭО.

Ключевые слова: БПЛА, имитатор, РЭБ.

Воздушная разведка считается одной из самых опасных боевых задач. Противник скрывает и защищает свои важные объекты комплексом организационных и технических средств, включая и огневыми средствами. Особенно опасна воздушная разведка в начальный период боевых действий, когда противовоздушная оборона одной стороны еще не подавлена, а у другой стороны отсутствует господство в воздухе. В настоящее время БПЛА признаются одним из важнейших средств повышения боевых возможностей соединений, частей и подразделений различных видов и родов войск. В интересах сухопутных войск, например, БПЛА могут вести воздушную разведку для обнаружения и определения координат стационарных и подвижных объектов поражения, включая танковые и механизированные колонны, огневые позиции артиллерии, реактивных систем залпового огня и оперативно-тактических ракет, командные пункты, склады, средства ПВО, полевые аэродромы [4].

К основным особенностям современных военных действий, которые обусловливают необходимость широкого использование беспилотных систем, относятся:

– адаптивное динамичное планирование применения войск на основе информации от различных источников, получаемой практически в реальном масштабе времени;

– нанесение ударов по критически важным объектам с постоянно возрастающим значением неконтактных действий, особенно на начальных этапах операции до достижения устойчивого превосходства над противником;

– объединение средств разведки, обнаружения целей, управления и связи, а также систем оружия в единые адаптивные разведывательно-ударные системы на принципах сетевых решений;

– широкое применение систем высокоточного оружия большой дальности, что предполагает наличие развитой разведывательно-информационной инфраструктуры, в которой беспилотные средства рассматриваются в качестве эффективного, а в ряде случаев – единственного источника информации о целях вне зависимости от их местонахождения;

– уменьшение количества привлекаемых сил и средств, снижение риска потерь личного состава, вооружения и военной техники в сложных условиях обстановки, в том числе в зонах с эшелонированной и сложной системой огневого поражения.

На БПЛА часто применяются различные целевые нагрузки для выполнения специальных задач. Одним из вариантов такого применения, является имитатор радиотехнических сигналов. Он (модуль имитации) устанавливается на БПЛА, который далее с носимым модулем имитации выводится в район с заданными координатами и производит имитацию радиоэлектронного объекта. При применении комплекса средств имитации радиоэлектронной обстановки оператор выполняет операции по управлению и изменению видов и параметров формируемых сигналов. Таким образом обеспечивается имитация одиночного летательного аппарата или группы летательных аппаратов.

В качестве источников сигналов для многофункционального комплекса средств имитации сложной радиоэлектронной обстановки выбран синтезатор с ФАПЧ со встроенным генератором, управляемым напряжением (ГУН). Данные синтезаторы могут применяться в аэрокосмическом и военном оборудовании. В ассортимент синтезаторов с ФАПЧ со встроенным ГУН входят узкополосные и широкополосные компоненты, работающие с диапазонами частот от 2 МГц до 32 ГГц. Единообразие корпусов различных серий синтезаторов частот позволяет использовать для их установки единую топологию печатной платы устройства имитации сигналов. Для создания имитатора радиоэлектронной обстановки (РЭО) с требуемыми частотными характеристиками необходима лишь установка соответствующего синтезатора частот.

При выборе антенно-фидерной системы имитатора радиотехнических сигналов основными требованиями были малые массогабаритными параметры и обеспечение требуемое изменение характеристик направленности в рабочей полосе частот. Этим требованиям удовлетворяют излучатели на основе симметричных щелевых линий, а также рупорные излучатели. Рассмотрим детальнее рупорные антенны, а именно конический рупор и антенну Вивальди.

Рупорные антенны являются широкополосными антеннами и обеспечивают примерно полуторное перекрытие по диапазону [2]. Возможность изменения рабочей частоты в ещё больших пределах ограничивается возбуждением и распространением высших типов волн в питающих волноводах. Коэффициент полезного действия рупора высокий (около 100%). Рупорные антенны просты в изготовлении. Сравнительно небольшое усложнение

(включение в волноводный тракт фазирующей секции) обеспечивает создание поля с круговой поляризацией [5].

В качестве антенны имитатора радиотехнических сигналов рассмотрим рупорные антенны, а именно конический рупор. Конические рупоры, как и прямоугольные, имеют оптимальные размеры, при которых достигается максимальный коэффициент направленного действия (КНД).

Из зависимости КНД следует, что антенны с большим раскрывом, обладают большим КНД. В следствие чего увеличивается их массогабаритные показатели, что является основным препятствием для их применения в конструкции целевой нагрузки БПЛА.

Наиболее рациональным вариантом антенно-фидерной системы имитатора является антенна Вивальди. Данный тип антенны позволяет достигнуть приемлемой импульсной характеристики при небольших размерах, также данная антенна обеспечивает требуемые характеристики направленности. Антенна Вивальди легко сопрягается с интегральными схемами [3].

В настоящее время не существует точной, хорошо разработанной теории антенн Вивальди, что затрудняет их исследование и проектирование. Для расчёта характеристик антенн Вивальди и подбора их геометрических размеров широко используются программные пакеты компьютерного моделирования [6].

С помощью программных пакетов CST Studio Suite и Antenna Magus, проводились исследования антенны Вивальди в полосе частот от 8,45 до 9,55 ГГц.

Также с помощью CST Studio Suite были рассчитаны значения коэффициента стоячей волны (КСВ) антенны для рабочего диапазона частот, результат представлен на рис. 1.

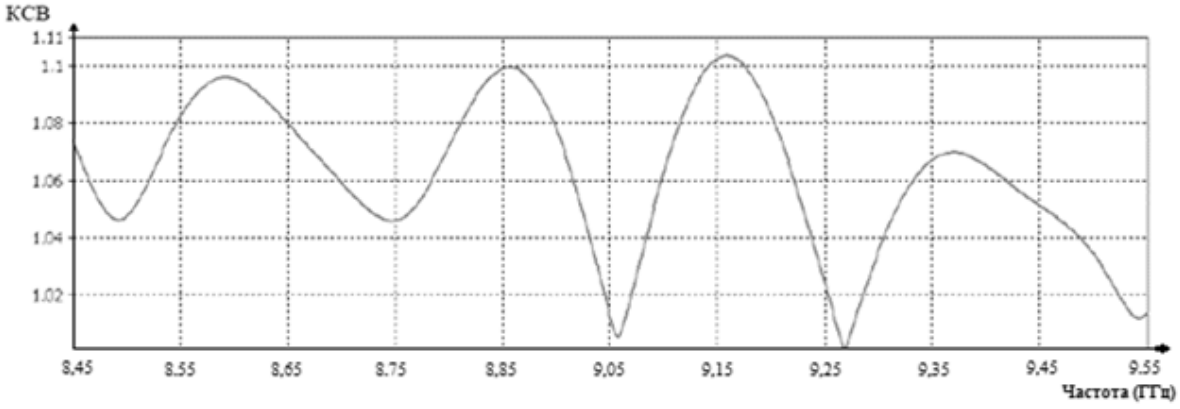

Рис. 1. График зависимости значений КСВ от частоты

Из полученных данных возможно сделать вывод, что во всей полосе частот 8,45-9,55 ГГц уровень КСВ не превышает значение 2, и является приемлемым значением степени согласования фидера и антенны.

Возможность применения имитатора радиотехнических сигналов, на БПЛА, позволит создать на его основе многофункциональный комплекс средств имитации сложной РЭО. Он обеспечит высокую эффективность боевой подготовки специалистов-операторов средств и комплексов РЭБ, а также

снизить материальные и временные затраты при проведении испытаний и обучении личного состава, а также расширит возможности по управлению и изменению видов и параметров формируемых сигналов.

Список источников

1. Кошкин Р.П. Беспилотные авиационные системы. Изд. «Стратегические приоритеты», 2016. 677 с.

2. Воскресенский Д.И., Гостюхин В.Л., Максимов В.М, Понамарев Л.И. Устройства СВЧ и антенны / Под ред. Д.И Воскресенского. Изд. 2-е, доп. и переработка. М.: Радиотехника, 2006. 376 с.

3. Головин О.В., Простов С.П. Системы и устройства коротковолновой радиосвязи. М.: Горячая линия – Телеком, 2006. 598 с.

4. http://www.modernarmy.ru/article/152#1.

5. Шостак, А. С. Антенны и устройства СВЧ : учебно-методическое пособие / А. С. Шостак. — Москва : ТУСУР, 2012. — 61 с. — URL: https://e.lanbook.com/book/10911 (дата обращения: 04.06.2023). — Режим доступа: для авториз. пользователей.

6. http://www.studentlibrary.ru/doc/ISBN9785991202558-SCN0000.html.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Гарев А.А. – старший оператор научной роты войск радиоэлектронной борьбы.

Ващенко С.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Гвоздев Е.А. – оператор научной роты войск радиоэлектронной борьбы.

Корягин В.А. – оператор научной роты войск радиоэлектронной борьбы.

Вклад авторов

Гарев А.А. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Ващенко С.С. – сбор материала, обработка материала, частичное написание статьи (25%).

Гвоздев Е.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Корягин В.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 623:74

Анализ радиоэлектронной обстановки с помощью беспилотных летательных аппаратов посредством применения технологии SDR

Сергей Николаевич Горбунов[1]✉, Иван Сергеевич Гришин[2], Никита Сергеевич Хрущев[3], Альберт Русланович Зайдуллин[4]
[1,2,3,4]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0009-7555-823X
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0000-6355-4551
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0004-5814-2893
[4]nauchnajarota@yandex.ru, https://orcid.org/0009-0005-2857-9290

Аннотация. В данной работе рассматривается возможность применения технологии SDR для решения задач радиомониторинга с помощью беспилотных летательных аппаратов в рамках использования программно-аппаратного комплекса «Рубеж».

Ключевые слова: фильтрация, сигналы, алгоритмы, комплекс.

Одной из задач, решаемых комплексами радиоэлектронной борьбы, является радиоразведка. Для ее выполнения необходим своевременный анализ радиоэлектронной обстановки в зонах боевых действий. С этой целью могут использоваться беспилотные летательные аппараты (БПЛА) с наличием бортовой и стационарной подсистем, которые обеспечивают помехозащищённую радиосвязь между БПЛА и пунктом управления. Стационарная подсистема отображения, в свою очередь, должна обеспечивать интерфейс оператора при управлении, контроле БПЛА и получении информации от бортовых средств. Средства бортовой подсистемы могут быть реализованы с применением концепции SDR.

Программно-определяемая радиосистема (англ. Software Defined Radio – SDR) – это радиосистема, в которой все или большинство функций физического уровня выполняются в программном виде, а функции, выполняемые аппаратно, должны оперативно модифицироваться по требованиям рабочего стандарта связи [4].

Данная технология позволяет устанавливать или изменять рабочие радиочастотные параметры, включая, в частности, диапазон частот, тип модуляции или выходную мощность, при помощи программного обеспечения, а не схемотехнических решений. В классическом виде в составе радиосистемы SDR присутствуют источник питания, антенна, широкополосный преобразователь частоты, АЦП/ЦАП и процессор с интерфейсами связи. При этом функции, которые традиционно выполняют смесители, фильтры и демодуляторы, реализуются программно согласно параметрам модулированных

сигналов и стандартов связи.

Эти функции SDR могут реализовываться с помощью различных устройств: процессор общего назначения, цифровой сигнальный процессор, программируемая логическая интегральная схема (ПЛИС) или интегральная схема общего назначения.

Технология SDR позволяет разрабатывать приемопередающую аппаратуру, обеспечивающую поддержку широкого спектра стандартов связи. Перепрограммирование SDR-трансивера для его адаптации под другой стандарт не несет за собой изменения в аппаратной части. Основными чертами таких устройств являются:

– сверхширокополосная и малошумящая радиочастотная часть, обладающая большим динамическим диапазоном;

– высокоскоростной тракт аналого-цифрового преобразования с большим динамическим диапазоном;

– сигнальный процессор, обладающий большой вычислительной мощностью;

– специализированный цифровой тракт фильтрации [5].

На рис. 1 показана функциональная схема программно-определяемой радиосистемы. Малошумящий усилитель и входной фильтр-преселектор приемника совместно обеспечивают предварительное усиление высокочастотного сигнала, выделение рабочего диапазона частот и подавление зеркальной частоты приема. Смеситель и последующий фильтр основной селекции на промежуточной частоте являются ключевыми элементами приемника. Эти компоненты осуществляют преобразование несущей частоты принятого сигнала на нулевую или ненулевую фиксированную промежуточную частоту и селекцию принятого полезного сигнала. Таким образом, для последующей аппаратной и программной обработки практически остается только полезный модулированный сигнал при отсутствии всех сторонних мешающих сигналов [5].

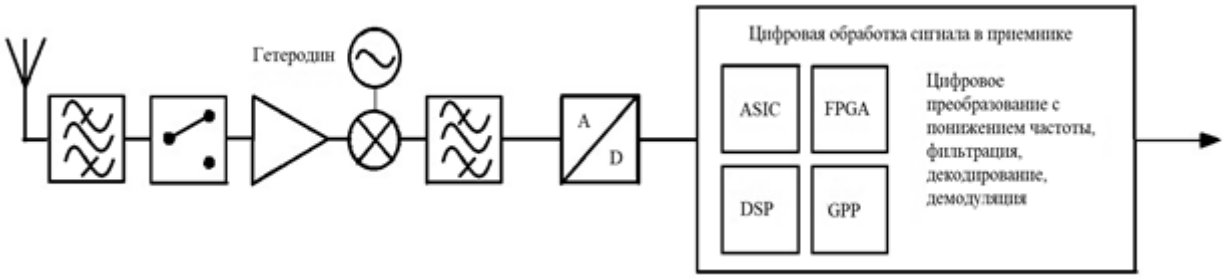

Рис. 1. Функциональная схема программно-определяемого радио

Архитектура программной части SDR состоит из четырех уровней.

Устройства нулевого уровня поддержки, который свидетельствует о полном отсутствии поддержки SDR, представляют собой чисто аппаратные решения, реализующие концепцию SDR [6].

Первый уровень образован программно-управляемым оборудованием

(Software Controlled Radio). Функции программного управления у этих устройств ограничены, тип модуляции или рабочий диапазон остаются постоянными. Использование нескольких программно-управляемых приемопередатчиков в одном устройстве позволяет организовать поддержку большого количества стандартов.

Второй уровень (Software Defined Radio) составляют собственно SDR-устройства. С помощью программного обеспечения в этих устройствах можно управлять основными параметрами сигнала: ширина полосы пропускания, тип модуляции в широком диапазоне частот [6].

Третий уровень (Ideal Software Radio) представляет собой устройства, пока широко не представленные на рынке SDR-технологий. В таких устройствах все процессы являются цифровыми, за исключением (при использовании мобильного телефона) таких аналоговых элементов, как антенна, микрофон и громкоговоритель. Развитие устройств данного уровня обеспечит качественный скачок в развитии концепции SDR [6].

Четвертый уровень (Ultimate Software Radio) включает в себя устройства, которые допускают полный контроль и управление трафиком, поддерживают широкий диапазон частот, радиоинтерфейсов и приложений [6].

Несмотря на то, что уже существует программная поддержка для устройств SDR, существующие программные решения обладают рядом недостатков. К их числу можно отнести большое количество занимаемой памяти, большое количество неиспользуемых или малоиспользуемых функций, замусоренность кода. В связи с этим возникает необходимость в разработке комплекса программных средств, реализующих функции программно-определяемой радиосистемы, обладающей понятным интерфейсом и включающей функции, необходимые оператору пункта управления БПЛА для оперативного решения задач по мониторингу радиоэлектронной обстановки [5].

На базе межвидового центра подготовки и боевого применения войск радиоэлектронной борьбы в рамках программно-аппаратного комплекса «Рубеж» была реализована программная часть системы для поддержки устройств SDR.

Интерфейс программной реализации представляет два модуля: «Эфир» и «Фильтрация».

Модуль «Эфир» выполняет сканирование заданного диапазона частот, позволяет прослушать и записать интересующий сигнал в формате .wav. Основной спектр позволяет наблюдать аномалии в радиоэфире и выбирать целевой сигнал для обработки, а спектр прослушиваемого сигнала предоставляет информацию по его основным параметрам.

Модуль «Фильтрация» предназначен для подавления помех в обрабатываемых сигналах. Он осуществляет их фильтрацию с использованием линейных и адаптивных цифровых фильтров. Результатом работы модуля является визуальное отображение обработанного сигнала, отношение сигнал/шум и его звуковой файл в формате .wav.

Созданная программная реализация на основе технологии SDR позволяет осуществлять ведение радиоразведки. Возможность работы с сигналами

различных стандартов связи и диапазонов частот заложена в самой концепции технологии, что обеспечивает применимость данного сканера частот в большинстве случаев. Высокая скорость обработки сигналов, обеспеченная производительными алгоритмами и языком программирования C++, позволяет быстро выполнить анализ радиоэфира оператором.

Список источников

1. Рембовский А. М., Ашихмин А. В., Козьмин В. А. Радиомониторинг: задачи, методы, средства / Под ред. А. М. Рембовского. 3-е изд., перераб. и доп. М: Горячая линия – Телеком, 2012. 640 с.

2. Воробьев, С.Н. Цифровая обработка сигналов: Учебник для студентов учреждений высшего профессионального образования / С.Н. Воробьев. М.: ИЦ Академия, 2013. 320 с.

3. Шлее, М. Qt 5.3. Профессиональное программирование на C++ / М. Шлее. СПб.: БХВ-Петербург, 2015. 928 с.

4. http://ibooks.ru/reading.php?short=1&productid=333385.

5. Семенюк А.В., Алферов Ю.В. Применение SDR при анализе радиоэлектронной обстановки с использованием беспилотных летательных аппаратов // Состояние и перспективы развития современной науки по направлению «Информатика и вычислительная техника»: сборник статей II Всероссийской научно-технической конференции. – Анапа, 2020. – Т. 4. – Ч. 1. – С. 31 – 40.

6. Рябов И.В., Толмачев С.В. Применение программно-определяемого радио в рамках задачи исследования метеорной радиосвязи // Радиолокация, навигация, связь: XXI Международная научно-техническая конференция. – Воронеж: НПФ «САКВОЕЕ», 2015. – Т. 3. – С. 1076 – 1082.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Горбунов С.Н. – старший оператор научной роты войск радиоэлектронной борьбы.

Гришин И.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Хрущев Н.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Зайдуллин А.Р. – оператор научной роты войск радиоэлектронной борьбы.

Вклад авторов

Горбунов С.Н.– идея, сбор материала, обработка материала, частичное написание статьи (25%).

Гришин И.С. – сбор материала, обработка материала, частичное написание статьи (25%).

Хрущев Н.С. – сбор материала, обработка материала, частичное написание статьи (25%).

Зайдуллин А.Р. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 512.6

Использование модульной арифметики и линейной алгебры при шифровании

Руслан Андреевич Гореленков[1], Андрей Иванович Гореленков[2]✉
[1]Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург
[2]Брянский государственный технический университет, Брянск
[1]rus.gorelenkov03@mail.ru, https://orcid.org/0009-0003-1705-4515
[2]an.gorelenkov@yandex.ru✉, https://orcid.org/0009-0009-7632-1074

Аннотация. Приведен алгоритм системы шифрования Хилла. Рассмотрены шифрование и дешифрование сообщений по системе шифрования Хилла с использованием матриц 2-го и 3-го порядков.

Ключевые слова: система шифрования, матрица, остаток от деления.

В 1929 г. американский математик Лестер Хилл придумал и запатентовал новую систему шифрования, в которой использовались и модульная арифметика, и линейная алгебра. Лежащий в основе такой системы алгоритм заменяет каждые k последовательных символов открытого текста k буквами шифрованного текста [1].

Алгоритм системы шифрования Хилла.

1. Каждой букве алфавита с добавленным символом «пробел» ставится в соответствие число 0, 1, …, n.

2. Последовательность букв открытого текста заменяется на последовательность чисел.

3. Последовательность чисел делится на группы по k чисел в каждой $(1 < k \le n)$. При необходимости добавляется в последнюю группу чисел число, соответствующее символу «пробел».

4. Ключом шифрования является произвольная матрица A размера $k \times k$, определитель которой равен 1. Ограничение на значение определителя установлено для гарантированной расшифровки текста.

5. Умножаем матрицу A на каждую группу из k чисел, записанную в виде матрицы-столбца. Каждое полученное число заменяем остатком от деления его на число $n+1$.

6. Полученная таким образом последовательность чисел заменяется на соответствующую последовательность букв.

7. Ключом дешифрования служит матрица A^{-1}, обратная к матрице A.

8. Для расшифровки текста выполняем пункты 2, 3, 5, 6, применяя матрицу A^{-1}.

Математически систему шифрования Хилла можно записать в виде соотношений

$$Y = AX\ ;\ X = A^{-1}Y\ ,$$

в которых A – матрица размера $k \times k$ (ключ шифрования), A^{-1} – матрица, обратная к матрице A (ключ дешифрования), X – матрица-столбец чисел, соответствующих k последовательным символам открытого текста, Y – матрица-столбец чисел, соответствующих k последовательным символам шифрованного текста.

Преимущество системы шифрования Хилла состоит в том, что она полностью маскирует частоты вхождений отдельных букв в тексте.

Однако у шифра Хилла есть существенный недостаток: имея даже небольшой фрагмент исходного текста, можно расшифровать все сообщение [1].

Рассмотрим систему шифрования Хилла на примерах.

Возьмем алфавит русского языка, в котором отсутствуют буквы Ё, Й и Ъ, что практически не ограничивает возможностей по составлению исходных сообщений на русском языке. В самом деле, замены буквы Ё на букву Е, буквы Й – на букву И, а буквы Ъ – на букву Ь позволяют понять смысл исходного сообщения, написанного с использованием этого алфавита.

Каждой букве этого алфавита и символу «пробел», обозначенного как @, поставим в соответствие число, как показано в следующей таблице [2]:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	@
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Зашифруем слово ИНТЕГРАЛ, используя двухбуквенную группировку текста.

Заменяя буквы слова на числа, получаем числовую последовательность 8 12 17 5 3 15 0 10.

Разделяем последовательность чисел на группы по 2 числа в каждой: (8 12), (17 5), (3 15), (0 10).

Пусть ключом шифрования будет матрица $A = \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix}$. Проверяем равенство 1 определителя матрицы A: $|A| = 2 \cdot 3 - (-5) \cdot (-1) = 6 - 5 = 1$.

Умножаем матрицу A на каждую группу из 2 чисел, записанную в виде матрицы-столбца, и заменяем полученные числа остатками от деления их на число 31:

$$\begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} 8 \\ 12 \end{pmatrix} = \begin{pmatrix} -44 \\ 28 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 28 \end{pmatrix} \pmod{31};\quad \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} 17 \\ 5 \end{pmatrix} = \begin{pmatrix} 9 \\ -2 \end{pmatrix} \equiv \begin{pmatrix} 9 \\ 29 \end{pmatrix} \pmod{31};$$

$$\begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 15 \end{pmatrix} = \begin{pmatrix} -69 \\ 42 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 11 \end{pmatrix} \pmod{31};\quad \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} 0 \\ 10 \end{pmatrix} = \begin{pmatrix} -50 \\ 30 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 30 \end{pmatrix} \pmod{31}.$$

Заменяя в числовой последовательности 18 28 9 29 24 11 12 30 числа на буквы, получаем шифрованное слово ФЮКЯЩМН@.

Операция расшифровки выполняется с помощью матрицы $A^{-1}=\begin{pmatrix}3 & 5\\ 1 & 2\end{pmatrix}$, обратной к матрице *A*.

Заменяем буквы шифрованного слова ФЮКЯЩМН@ на числа и разделяем полученную числовую последовательность 18 28 9 29 24 11 12 30 на группы по 2 числа в каждой: (18 28), (9 29), (24 11), (12 30).

Умножаем матрицу A^{-1} на каждую группу из 2 чисел, записанную в виде матрицы-столбца, и заменяем полученные числа остатками от деления их на число 31:

$$\begin{pmatrix}3 & 5\\ 1 & 2\end{pmatrix}\begin{pmatrix}18\\ 28\end{pmatrix}=\begin{pmatrix}194\\ 74\end{pmatrix}\equiv\begin{pmatrix}8\\ 12\end{pmatrix}\ (\mathrm{mod}\ 31);\quad \begin{pmatrix}3 & 5\\ 1 & 2\end{pmatrix}\begin{pmatrix}9\\ 29\end{pmatrix}=\begin{pmatrix}172\\ 67\end{pmatrix}\equiv\begin{pmatrix}17\\ 5\end{pmatrix}\ (\mathrm{mod}\ 31);$$

$$\begin{pmatrix}3 & 5\\ 1 & 2\end{pmatrix}\begin{pmatrix}24\\ 11\end{pmatrix}=\begin{pmatrix}127\\ 46\end{pmatrix}\equiv\begin{pmatrix}3\\ 15\end{pmatrix}\ (\mathrm{mod}\ 31);\quad \begin{pmatrix}3 & 5\\ 1 & 2\end{pmatrix}\begin{pmatrix}12\\ 30\end{pmatrix}=\begin{pmatrix}186\\ 72\end{pmatrix}\equiv\begin{pmatrix}0\\ 10\end{pmatrix}\ (\mathrm{mod}\ 31).$$

Заменяя в числовой последовательности 8 12 17 5 3 15 0 10 числа на буквы, получаем слово ИНТЕГРАЛ, т.е. расшифровка работает.

Зашифруем слово ПРОИЗВОДНАЯ, используя трехбуквенную группировку текста.

Заменяя буквы слова на числа, получаем числовую последовательность 14 15 13 8 7 2 13 4 12 0 29.

Разделяем последовательность чисел на группы по 3 числа в каждой: (14 15 13), (8 7 2), (13 4 12), (0 29 30). Так как в тексте 11 букв (11 не кратно 3), то в последнюю группу чисел добавили число 30, соответствующее символу «пробел».

Пусть ключом шифрования будет матрица $A=\begin{pmatrix}-2 & 1 & -2\\ 1 & 0 & -3\\ 2 & -1 & 1\end{pmatrix}$, определитель которой равен 1.

Умножая матрицу *A* на каждую группу из 3 чисел, записанную в виде матрицы-столбца, и заменяя полученные числа остатками от деления их на число 31, получаем числовую последовательность: 23 6 26 18 2 11 16 8 3 0 3 1.

Заменяя в числовой последовательности 23 6 26 18 2 11 16 8 3 0 3 1 числа на буквы, получаем шифрованное слово ШЖЫУВМСИГАГБ.

Операция расшифровки выполняется с помощью матрицы $A^{-1}=\begin{pmatrix}-3 & 1 & -3\\ -7 & 2 & -8\\ 1 & 0 & -1\end{pmatrix}$, обратной к матрице *A*.

Заменяем буквы шифрованного слова ШЖЫУВМСИГАГБ на числа и разделяем полученную числовую последовательность 23 6 26 18 2 11 16 8 3 0 3 1 на группы по 3 числа в каждой: (23 6 26), (18 2 11), (16 8 3), (0 3 1).

Умножая матрицу A^{-1} на каждую группу из 3 чисел, записанную в виде матрицы-столбца, и заменяя полученные числа остатками от деления их на число 31, получаем последовательность 14 15 13 8 7 2 13 4 12 0 29 30. Заменяя числа на

буквы, получаем текст ПРОИЗВОДНАЯ@. Убирая символ пробела, получаем исходное слово ПРОИЗВОДНАЯ. Тем самым еще раз убеждаемся, что система шифрования Хилла работает.

Отметим, что чем больше размер матрицы *A* в системе шифрования Хилла, тем больше в шифрованном тексте скрывается информации о различиях в значениях частот появления комбинаций букв.

Список источников

1. Мир математики : в 40 т. Т. 2. Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография / Пер. с англ. – Москва : Де Агостини, 2014. – 144 с. – ISBN 978-5-9774-0639-0 (т. 2).

2. Введение в криптографию / под общ. ред. В. В. Ященко. – Изд. 4-е, доп. – Москва : МЦНМО, 2012. – 348 с. – ISBN 978-5-4439-0026-1.

Статья поступила в редакцию 22.03.2023; принята к публикации 10.05.2023.

Информация об авторах

Гореленков Р.А. – студент направления подготовки 14.03.01 – Ядерная энергетика и теплофизика Высшей школы атомной и тепловой энергетики ФГАОУ ВО «СПбПУ».

Гореленков А.И. – к.т.н., зав. кафедрой «Высшая математика» ФГБОУ ВО «БГТУ».

Вклад авторов

Гореленков Р.А. – идея, сбор материала, обработка материала, написание статьи (50%).

Гореленков А.И. – написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 005.007

Сущность комплексного подхода к разработке системы защиты информации

Алексей Петрович Горлов [1]✉, Максим Леонидович Гулак [2], Евгений Вячеславович Лексиков [3], Дмитрий Андреевич Лысов [4]
[1,2,3,4]Брянский государственный технический университет, Брянск, Россия
[1]apgorlov@gmail.com,https://orcid.org/0009-0003-3100-3466
[2]gml13@yandex.ru,http://orcid.org/0009-0009-3131-4292
[3]jl32@ya.ru,http://orcid.org/0009-0005-3112-0157
[4]lysovdmitriia@gmail.com,http://orcid.org/0009-0003-9666-7191

Аннотация. В статье раскрывается сущность комплексного подхода к разработке систем защиты информации, отражена взаимосвязь между отдельными компонентами комплексной системы защиты информации и важность реализации принципа системности при разработке систем защиты информации.

Ключевые слова: информационная безопасность, комплексные системы защиты информации, технические средства защиты информации, организационная защита информации, программно-аппаратная защита информации.

Основная цель комплексной системы защиты информации заключается в гарантии непрерывности надёжности работы коммерческого предприятия, а так же предотвращении угроз его функционированию. Проблема обеспечения желаемого уровня защиты информации является чрезвычайно сложной, требующей создания целостной организационно-технологической системы и применения специальных средств по обеспечению информационной безопасности [11].

В результате анализа теоретических и практических работ в области информационной безопасности, был сформулирован системно-концептуальный подход к защите информации. Этот способ подразумевает учет всех взаимодействующих и изменяющихся во времени элементов, условий или факторов для понимания проблемы обеспечения безопасности информации. КСЗИ объекта требует взаимодействия для решения задач по проектированию отдельных его компонентов, таких как организационные, инженерно-технические, программно-аппаратные и криптографические меры защиты информации.

К организационным мерам относятся такие действия, как установление правил доступа к информации, организация процедур обмена информацией, обучение персонала вопросам информационной безопасности, а также контроль и проверка защищенности информации. Все эти меры направлены на

обеспечение конфиденциальности, целостности и доступности информации.

Меры по защите информации организации относятся к комплексу нормативных, обязательных и технологических руководств и методов, определяющих основу и содержание системы защиты, а также мотивации работников, отвечающих требованиям по обеспечению защиты информации (рис. 1) [12].

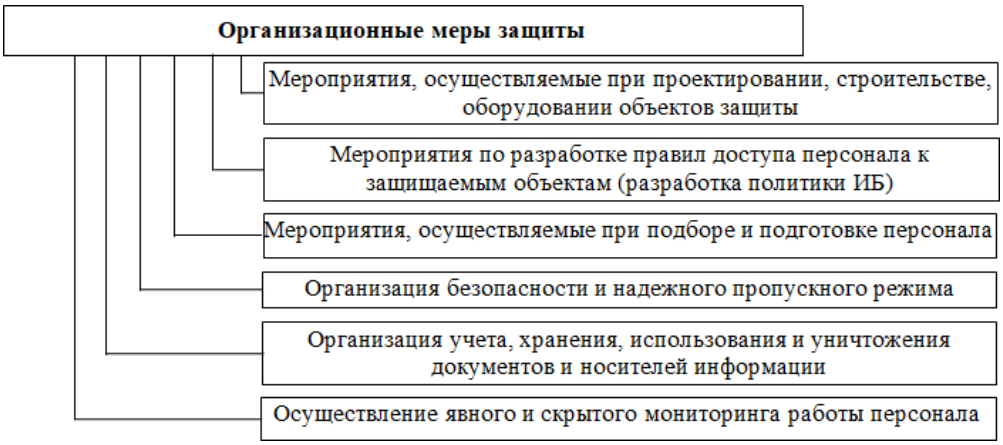

Рис. 1. Компоненты организационных мер защиты информации

Организационную структуру необходимо создавать для обеспечения защиты пользователей, а также регулирования их действий. Кроме того, организация мероприятий должна быть обеспечена более эффективными техническими и физическими средствами для обеспечения безопасности.

Инженерная защита информации – это защита информации от несанкционированного доступа с использованием технических средств и методов. К техническим, инженерным и аппаратным средствам относят техническое, инженерное и аппаратное средства защиты (рис. 2) [13].

Рис. 2. Состав инженерно-технических мер защиты информации

Инженерно-технические меры защиты информации направлены на защиту от проникновения киберпреступников и утечки информации через технические каналы. Инженерные работы могут включать в себя использование защищенного подключения, экранирование потоков данных, шифрование и защиту

информации от нежелательных воздействий.

Аппаратно-программная защита информации – Защита информации, предполагающая использование технических средств и специального программного обеспечения для защиты информации в автоматизированных системах обработки информации (рис. 3).

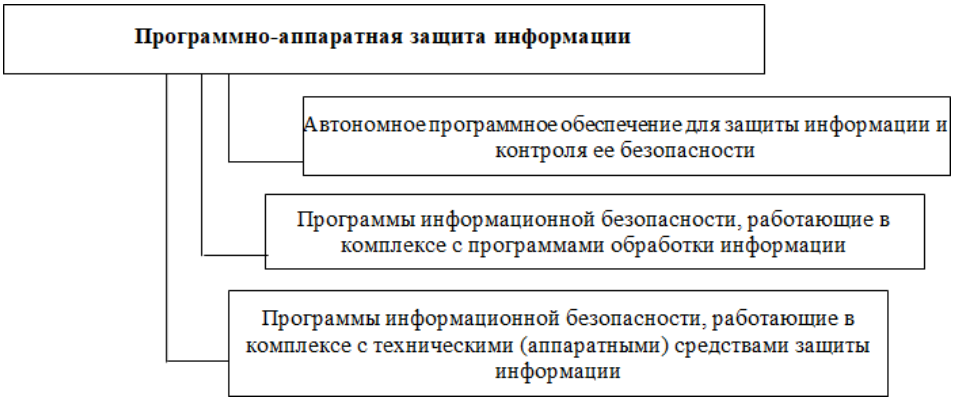

Рис. 3. Состав программно-аппаратных мер защиты информации

Комплексная защита информации для программного и аппаратного обеспечения решает важнейшие задачи, связанные с защитой компьютерных систем и сетей, рабочих станций, системного и прикладного программного обеспечения.

Неотъемлемой частью шифрования комплексных систем защиты информации является регламентация использования различных методов шифрования на ЭВМ и локальных сетях, текста документов, передач по непроверенной почте, телеграфу, телексу. Определяются условия и способ шифрования данных.

Рис. 4. Криптографические меры защиты информации

Аппаратные, программные и инструментальные средства криптографической защиты, а также их методы устраняют слабые места в организационных мерах, создают прочные барьеры для злоумышленников и, по возможности, обеспечивают блокировку и защиту несанкционированного доступа для предотвращения получения несанкционированной информации.

Отдельного внимания заслуживает взаимозависимость в работе этих

компонентов КСЗИ. Наличие технических средств и защитного программного обеспечения не гарантирует их корректного и эффективного использования во всех режимах эксплуатации, особенно при ремонте и техническом обслуживании. Кроме того, хранение документов организацией, устанавливающей правила обращения с конфиденциальной информацией, не исключает угроз, связанных с прямым доступом злоумышленников к источникам информации, утечками по техническим каналам, дистанционным доступом к информационным ресурсам, блокировкой доступа к программным компонентам компьютерной системы.

Взаимосвязь рассматриваемых компонентов КСЗИ приведена на рис. 5.

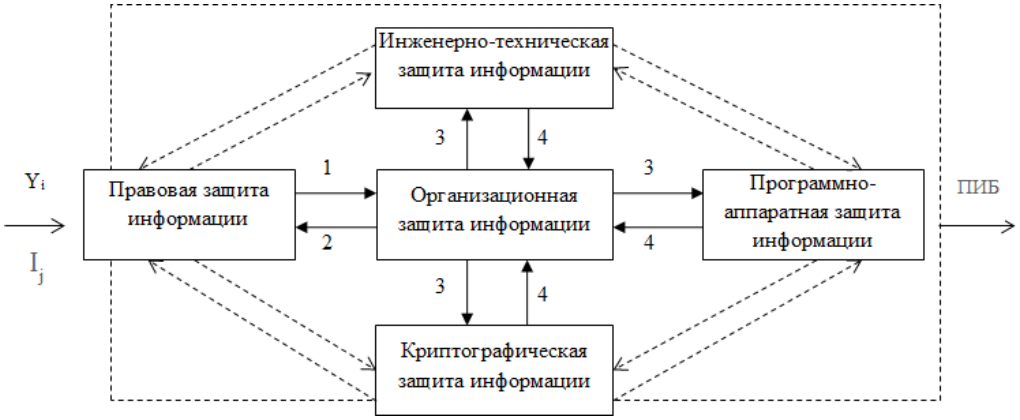

Рис. 5. Взаимосвязь компонентов КСЗИ:
Yi – категории угроз безопасности;
I_j– виды информации, обрабатываемой на объекте защиты;
ПИБ– политика информационной безопасности.
1 – Организационные меры реализуют выполнение действующих правил и разрабатываются с учетом действующих кодексов поведения, принятых в стране или организации.
2 – Реализация организационных мероприятий требует создания нормативных документов.
3 – Чтобы приложение было эффективным, организационные меры должны быть подкреплены техническими, физическими, программными и криптографическими средствами защиты информации.
4 – Применение и использование технических средств защиты требует соответствующего организационного обеспечения

При построении комплексной системы защиты информации могут быть предприняты дополнительные меры по защите персональных данных, защите ИТ-инфраструктуры для безопасного доступа в Интернет и прочее. Каждый компонент комплексной системы защиты информации одновременно обеспечивает эффективную работу других компонентов и при этом полностью зависит от них. По мере осознания важности, сложности и неэффективности защиты с использованием простого набора средств защиты растет осознание необходимости разработки Стратегического подхода к защите.

Список источников

1. Шаньгин, В. Ф. Информационная безопасность и защита информации/В. Ф. Шаньгин. —Саратов : Профобразование, 2017. — 702 с. —

ISBN 978-5-4488-0070-2. — URL: http://www.iprbookshop.ru/63594.html (дата обращения:12.10.2020).— Режим доступа: для авторизир. пользователей.

2. Краковский, Ю. М. Защита информации: учебное пособие / Ю. М.Краковский. — Ростов-на-Дону : Феникс, 2016. — 349 с. — ISBN 978-5-222-26911-4. — URL:https://www.iprbookshop.ru/59350.html (датаобращения:22.02.2023).—Режим доступа: для авторизир. пользователей.

3. Никифоров, С. Н. Защита информации. Защищенные сети: учебноепособие/С.Н.Никифоров.—Санкт-Петербург:Санкт-Петербургскийгосударственныйархитектурно-строительныйуниверситет,ЭБСАСВ,2017.—80 с. — ISBN 978-5-9227-0762-6. — URL: https://www.iprbookshop.ru/74382.html (дата обращения: 20.03.2023). — Режим доступа: для авторизир. пользователей.

Статья поступила в редакцию 22.03.2023; принята к публикации 10.05.2023.

Информация об авторах

Горлов А.П. – доцент кафедры «Системы информационной безопасности», ФГБОУ ВО «БГТУ».

Гулак М.Л. – доцент кафедры «Системы информационной безопасности», ФГБОУ ВО «БГТУ».

Лексиков Е.В. – старший преподаватель кафедры «Системы информационной безопасности», ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности», ФГБОУ ВО «БГТУ».

Вклад авторов

Горлов А.П. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Гулак М.Л. – написание статьи, научное редактирование текста (25%).

Лексиков Е.В. – написание статьи, научное редактирование текста (25%).

Лысов Д.А. – написание статьи, научное редактирование текста (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Особенности атаки «человек посередине» и пути её предотвращения

Дмитрий Андреевич Лысов[1], Алексей Петрович Горлов[2], Вероника Вячеславовна Кузина[3]✉, Вероника Дмитриевна Медведева [4]
[1,2,3,4] Брянский государственный технический университет,Брянск, Россия
[1]lysovdmitriia@gmail.com, https://orcid.org/0009-0003-9666-7191
[2]apgorlov@gmail.com, https://orcid.org/0009-0003-3100-3466
[3]veronika.k02@bk.ru✉, https://orcid.org/0009-0003-9513-5222
[4]nicka.medvedeva2020@yandex.ru, https://orcid.org/0009-0007-4326-8073

Аннотация. В статье раскрывается проблема роста числа кибератак направленная на критически важные объекты государств. Одной из основных причин роста стала приостановка деятельности в России ряда зарубежных поставщиков корпоративных средств информационной безопасности. MITM-атаки основаны на манипулировании сетями или создании вредоносных сетей, контролируемых киберпреступниками. Знание явных признаков атаки и применение методов обнаружения может помочь обнаруживать атаки до того, как будет нанесен ущерб.

Ключевые слова: инструмент, атака, человек посередине, злоумышленник, киберпреступник, HTTP, NLS, сетевой трафик, SSL, MITM.

Рост числа кибератак, направлен на критически важные объекты государств. Одной из основных причин роста кибератак на компании Российской Федерации стала приостановка деятельности в стране ряда иностранных поставщиков корпоративных средств информационной безопасности. Статистика атакованных компьютеров АСУ в России за 2018-2022 годы представлена на рис. 1.

Процент атакованных компьютеров автоматизированной системы управления в России за период 2018-2021 года был примерно одинаков, тогда как статистика первого полугодия 2022 года говорит о том, что рост числа кибератак резко возрастает.

Осуществление атаки «человек посередине»

MITM-атаки опираются на манипулирование сетями или создание вредоносных сетей, контролируемых киберпреступниками. Злоумышленник перехватывает трафик и либо пропускает его через свою систему, собирая информацию по ходу, либо перенаправляет в другое место.

Киберпреступники, по сути, действуют как «посредники» между человеком, отправляющим информацию, и тем, кто ее получает. Эти атаки на распространены, особенно в общедоступных сетях Wi-Fi. Поскольку общедоступный Wi-Fi часто бывает незащищенным, невозможно узнать, кто

отслеживает или перехватывает веб-трафик, ведь кто угодно может войти в систему [7].

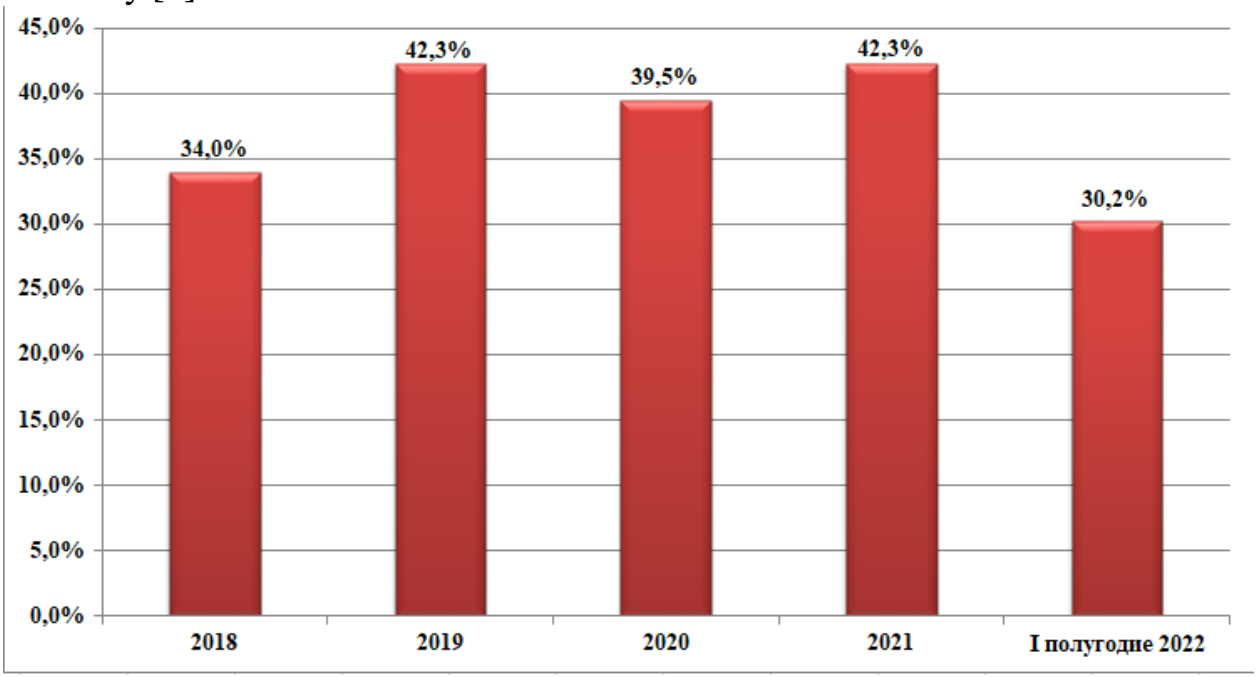

Рис. 1. Процент атакованных компьютеров автоматизированной системы управления в России за 2018-2022 гг.

К приёмам атак «человек посередине можно отнести:»

1. **Сниффинг пакетов** – сниффинг позволяет злоумышленникамвидеть пакеты данных, доступ к которым они не имеют.

2. **Инъекция пакетов** – перед инъекцией преступники сначала используют сниффинг, чтобы определить, как и когда отправить вредоносные пакеты. После инъекции вредоносные пакеты смешиваются с действительными в потоке данных.

3. **Снятие SSL** – злоумышленники могут использовать технику отключения SSL для перехвата легитимных пакетов, модификации запросов на основе HTTPS и направления их в небезопасное место назначения, эквивалентное HTTP [8].

Помимо приёмов атаки существует несколько видов атак «человек посередине». К ним относятся:

1. **Спуфинг** (подмена) IP-адресов предполагает, что злоумышленник изменяет IP-пакеты, чтобы выдать себя за компьютерную систему жертвы.

2. **IP-спуфинг** (подмена IP-адресов). Это подмена IP-адресов, выполняемая посредством создания IP-пакетов с ложным IP-адресом источника для имитации другой компьютерной системы.

3. **ARP-спуфинг.** При подмене протокола разрешения адресов (ARP) злоумышленник использует фальсифицированные сообщения ARP, чтобы связать свой MAC-адрес с IP-адресом жертвы.

4. **DNS-спуфинг.** «Отравление» DNS-кэша предполагает, что злоумышленник меняет IP-адрес DNS-сервера, чтобы иметь возможность перенаправлять веб-трафик жертвы с предполагаемого реального веб-сайта на мошеннический.

5. **HTTPS-спуфинг.** Когда пользователь подключается к защищенному сайту с префиксом https://, злоумышленник отправляет в браузер поддельный сертификат безопасности. Это «обманывает» браузер, заставляя считать, что соединение является безопасным.

6. **Внедрение пакетов.** Киберпреступник создает пакеты, которые кажутся нормальными, и внедряет их в сеть с целью доступа и отслеживания трафика или инициирования DDoS-атак.

7. **SSL-стриппинг.** Киберпреступник перехватывает TLS- сообщение от приложения или веб-сайта и изменяет его так, чтобы сайт загружался по незащищенному соединению по протоколу HTTP.

8. **SSL-спуфинг.** Этот способ включает в себя подделку адреса защищенного сайта, чтобы жертва перешла по поддельному адресу.

9. **Общедоступный Wi-Fi.** Общедоступная сеть Wi-Fi часто бывает незащищенной, поэтому киберпреступники могут видеть веб-трафик слюбого подключенного к сети устройства и получать информацию.

10. **SSL BEAST.** Происходит заражение компьютера вредоносным кодом JavaScript. Затем программа перехватывает файлы cookie и токены аутентификации для дешифрования, открывая доступ ко всему сеансу жертвы [7].

Методы обнаружения атак типа «человек посередине» и пути предотвращения

Атаки «человек посередине» трудноуловимы, но их присутствие всё же оставляет следы в сетевой активности, которые могут обнаружить от профессионалов в области кибербезопасности, до конечных пользователей.

Признаки, по которым можно обнаружить киберпреступника:

- **неожиданное или повторяющееся отключение:** злоумышленники принудительно отключают пользователей, чтобы перехватить имя и пароль, когда те попытаются повторно подключиться. Отслеживая неожиданные или повторяющиеся отключения, вы можете заранее определить подобное опасное поведение;
- **странные адреса в адресной строке браузера:** если что-то в адресе выглядит хотя бы немного странно, перепроверьте свои подозрения. Возможно, вы имеете дело с перехватом DNS;
- **вход в общедоступную или незащищенную сеть Wi-Fi:** будьте очень осторожны с сетями, к которым подключаетесь, и по возможности избегайте общедоступного Wi-Fi. Злоумышленники создают поддельные сети с известными идентификаторами, чтобы обманом заставить людей подключиться. Если вы подключитесь к Wi-Fi злоумышленника, он сможет легко увидеть все, что вы отправляете по Wi-Fi [9].

Помимо использования надежных решений и методов обеспечения безопасности, необходимо применять инструменты для проверки систем и выявления уязвимостей, которыми могут воспользоваться злоумышленники. К ним можно отнести:

Hetty. Hetty – это быстрый набор инструментов HTTP с открытым исходным кодом и мощными функциями для поддержки исследователей

безопасности.

К особенностям можно отнести: имеет модуль отправителя, который позволяет отправлять http-запросы вручную, основываясь либо на выключенных запросах из журнала прокси, либо создавая их с нуля; простая установка и простой в использовании интерфейс [8].

Bettercap. Bettercap – это комплексный и масштабируемый инструмент для разведки и атаки сетей. Инструмент обладает возможностями мониторинга сети и другими функциями, такими как создание поддельных точек доступа, сниффер паролей, DNS-спуфер, перехват рукопожатия и т.д.

К особенностям можно отнести: мощный встроенный сетевой сниффер для идентификации аутентификационных данных и сбора учетных данных; простой в использовании и интерактивный пользовательский веб-интерфейс, позволяющий проводить широкий спектр mitm-атак, сниффить учетные данные, контролировать http и http-трафик и т.д.;

Proxy.py. Proxy.py – это легкий прокси-сервер с открытым исходным кодом для WebSockets, HTTP, HTTPS и HTTP2. Инструмент позволяет исследователям проверять веб-трафик, включая зашифрованные TLS приложения, потребляя при этом минимум ресурсов.

К особенностям можно отнести: быстрый и масштабируемый инструмент, способный обрабатывать десятки тысяч соединений в секунду; имеет легкий дизайн; кроме того, он опирается на стандартные библиотеки Python и не требует никаких внешних зависимостей.

Mitmproxy. Mitmproxy – это простое в использовании решение HTTPS-прокси с открытым исходным кодом. В целом, этот простой в установке инструмент работает как SSL прокси HTTP «человек посередине» и имеет консольный интерфейс, который позволяет вам проверять и изменять поток трафика на лету.

К особенностям можно отнести: интерактивный и надежный инструмент анализа и модификации HTTP-трафика; гибкий, стабильный, надежный, простой в установке и использовании инструмент; позволяет перехватывать и модифицировать HTTP и HTTPS запросы и ответы на лету;

BurpSuite. Burp – это автоматизированный и масштабируемый инструмент для сканирования уязвимостей.

К особенностям можно отнести: позволяет исследователям тестировать веб-приложения и выявлять уязвимости, которые злоумышленники могут использовать и проводить MITM-атаки; перехват и проверка необработанного сетевого трафика в обоих направлениях между веб- браузером и сервером; выбор использования встроенного браузера Burps или внешнего стандартного веб-браузера; отображение отдельных перехваченных HTTP-запросов и ответов.

Современные тенденции таковы, что количество сетей и подключенных к ним устройств растет, а это означает, что у злоумышленников больше возможностей использовать методы «человека посередине». Знание явных признаков атаки «человек посередине» и применение методов обнаружения может помочь вам обнаруживать атаки до того, как они нанесут ущерб.

Список источников

1. Man-in-the-Middle: советы по обнаружению и предотвращению / Хабр (habr.com) Режим доступа: URL: https://habr.com/ru/company/varonis/blog/526632/
2. Что такое атака Man-in-the-Middle (MITM)? Определение и предотвращение (securitylab.ru). - URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/351898.php?ysclid=lfb4wm35ab610763453
3. Как защититься от атаки «человек посередине» – Kaspersky Daily | Блог Касперского. Режим доступа: URL: https://www.kaspersky.ru/blog/chto-takoe-chelovek-poseredine/740/?ysclid=lfb4wumanx593056603
4. Туркина, А. А. Некоторые аспекты "импортозамещения" в сфере ит / А. А. Туркина // Анализ и современные информационные технологии в обеспечении экономической безопасности бизнеса и государства : Сборник научных трудов и результатов совместных научно-исследовательских проектов / РЭУ им. Г.В. Плеханова. – Москва: Издательство "Аудитор", 2016. – С. 543-547. (дата обращения16.10.2022).
5. Все об атаке "Человек посередине" (Man in the Middle, MitM) (anti-malware.ru). URL: https://www.anti- malware.ru/analytics/Threats_Analysis/man-in-the-middle-attack.
6. Федорченко, А. В. Корреляция информации в SIEM-системах на основе графа связей типов событий / А. В. Федорченко, И. В. Котенко // Информационно-управляющие системы. – 2018. – № 1(92). – С. 58-67. (дата обращения 10.10.2022).
7. https://www.keepersecurity.com/ru_RU/threats/man-in-the-middle-attacks-mitm.html.
8. https://itsecforu.ru/2021/07/11/%F0%9F%95%B5%EF%B8%8F-%D0%BE%D0%B1%D0%B7%D0%BE%D1%80-%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%BE%D0%B2-mitm-%D0%B0%D1%82%D0%B0%D0%BA-%D0%B4%D0%BB%D1%8F-%D0%B8%D1%81%D1%81%D0%BB/.
9. https://habr.com/ru/companies/varonis/articles/526632/.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горлов А.П. – к.т.н. доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Кузина В.В. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03. – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Медведева В.Д. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03. – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Лысов Д.А. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Горлов А.П.– написание статьи, научное редактирование текста (25%).

Кузина В.В. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Медведева В.Д. – идея, сбор материала, обработка материала,частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Обеспечение защиты передачи конфиденциальной информации по открытым каналам связи

Павел Николаевич Горошко [1]✉, Николай Александрович Роговой [2], Даниил Александрович Матвеев [3]
[1, 2, 3]Брянский государственный технический университет, Брянск, Россия
[1]png32@yandex.ru✉, https://orcid.org/0009-0001-7195-1992
[2]kolyanike32@gmail.com, https://orcid.org/0009-0004-9245-1972
[3]danya.matveev.01@list.ru, https://orcid.org/0009-0002-9332-8779

Аннотация. В статье рассматриваются основные методы защиты передачи информации, включая шифрование симметричными и асимметричными алгоритмами, протоколы аутентификации и защиты целостности данных. Описывается использование виртуальных частных сетей (VPN) и протокола Secure Sockets Layer/Transport Layer Security (SSL/TLS) для защиты передачи данных через открытые каналы связи.

Ключевые слова: информационная безопасность, открытые каналы связи, шифрование, защита конфиденциальности, функциональный канал.

Обеспечение защиты передачи конфиденциальной информации по открытым каналам связи является важной задачей в современном мире информационных технологий. С каждым годом все больше данных передается по интернету и по открытым каналам связи, что делает их уязвимыми для несанкционированного доступа и кражи конфиденциальной информации.

Актуальность этой проблемы подчеркивается ростом количества случаев утечек данных, когда злоумышленники получают доступ к конфиденциальной информации, такой как личные данные клиентов, финансовая информация и т.д. Такие утечки данных могут привести к серьезным финансовым и репутационным последствиям для компаний и организаций.

Кроме того, защита передачи конфиденциальной информации является обязательным требованием законодательства во многих странах. Например, в Европейском союзе существует Общее регулирование о защите данных (GDPR), которое требует, чтобы компании обеспечивали защиту конфиденциальной информации при ее передаче по открытым каналам связи.

В связи с этим, обеспечение защиты передачи конфиденциальной информации по открытым каналам связи является актуальной и необходимой задачей для компаний и организаций. Для этого используются различные методы защиты, такие как шифрование данных, использование виртуальных частных сетей (VPN), двухфакторная аутентификация и т.д. Важно также проводить регулярный аудит системы на уязвимости и обучать сотрудников безопасным

практикам использования системы, чтобы минимизировать риски несанкционированного доступа к конфиденциальной информации.

Функциональный канал – это канал связи между компонентами системы, который предназначен для передачи данных. Каналы связи могут быть использованы злоумышленниками для получения несанкционированного доступа к системе и данным. Поэтому функциональный канал становится опасным, когда он становится уязвимым для атаки.

Существует несколько факторов, которые могут сделать функциональный канал опасным:

1. Недостаточная защита канала: если функциональный канал не защищен адекватным образом, злоумышленник может перехватить передаваемые данные, в том числе личные данные пользователей, пароли, финансовые данные и т.д.

2. Неизолированные каналы: если функциональные каналы не изолированы друг от друга, злоумышленник может использовать уязвимость в одном канале, чтобы получить доступ к другому каналу.

3. Несоответствие прав доступа: если права доступа к функциональному каналу не настроены правильно, злоумышленник может получить доступ к каналу, к которому у него нет права доступа.

4. Необновленное программное обеспечение: если программное обеспечение, используемое для функциональных каналов, не обновляется, то в системе могут быть уязвимости, которые могут быть использованы злоумышленниками.

5. Нарушения конфиденциальности: если в функциональном канале передаются данные с конфиденциальной информацией, то злоумышленник может использовать уязвимость в канале, чтобы получить доступ к этим данным.

Для защиты функциональных каналов необходимо проводить регулярный аудит системы на уязвимости, использовать шифрование для передачи данных, изолировать каналы друг от друга и настроить права доступа для каждого канала. Кроме того, необходимо обновлять программное обеспечение и обучать пользователей безопасным практикам использования системы.

Существует несколько способов обеспечения безопасности передачи конфиденциальной информации по открытым каналам связи. Рассмотрим некоторые из них:

1. Использование шифрования: шифрование является одним из наиболее эффективных способов защиты передаваемых данных. Шифрование заключается в преобразовании исходных данных в форму, которая не может быть понятой без специального ключа. При передаче зашифрованных данных по открытому каналу связи злоумышленники не смогут прочитать содержимое сообщения.

2. Использование протоколов безопасности: протоколы безопасности, такие как SSL (Secure Sockets Layer) и TLS (Transport Layer Security), используются для защиты передачи данных в Интернете. Эти протоколы обеспечивают шифрование данных, аутентификацию и защиту от подделки данных.

3. Использование виртуальных частных сетей (VPN): VPN используется для создания безопасного соединения между двумя узлами по открытому каналу связи. VPN-соединение обеспечивает шифрование и аутентификацию данных.

4. Использование электронной подписи: электронная подпись используется для защиты целостности и подлинности данных. Электронная подпись гарантирует, что данные не были изменены после создания подписи и что подпись была создана законным обладателем ключа.

5. Ограничение доступа к данным: доступ к конфиденциальной информации должен быть ограничен только для авторизованных пользователей. Для этого можно использовать систему аутентификации и авторизации, такую как LDAP (Lightweight Directory Access Protocol) или Active Directory.

6. Использование защитных механизмов: защитные механизмы, такие как брандмауэры и антивирусное программное обеспечение, также могут помочь защитить данные, предотвращая несанкционированный доступ к сети или заражение вредоносным программным обеспечением.

7. Обучение пользователей: наиболее уязвимым звеном в цепочке безопасности являются пользователи. Обучение пользователей основам информационной безопасности, таким как использование надежных паролей и неоткрытие вредоносных вложений в электронной почте, может помочь предотвратить многие угрозы безопасности.

Повышение уровня защищенности конфиденциальной информации при передаче по открытым каналам связи требует проведение комплексных мероприятий разного характера. Наиболее полной защищенности можно добиться при использовании всех вышеописанных методов защиты. Важно постоянно анализировать эффективность защитных мероприятий, осуществлять контроль за проведением этих мероприятий.

В целом, обеспечение защиты передачи конфиденциальной информации по открытым каналам связи является сложной задачей, но с помощью правильных методов и технологий, а также соблюдения соответствующих мер предосторожности, можно минимизировать риск утраты конфиденциальной информации.

Список источников

1. Истомин, К. В. Защита конфиденциальной информации при ее передаче по открытым каналам связи / К. В. Истомин, О. Р. Уторов // Безопасность информационного пространства : Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых, Курган, 30 ноября – 01 2016 года / Министерство образования и науки Российской Федерации Координационный совет по подготовке (переподготовке) и повышению квалификации кадров в области защиты информации в Уральском федеральном округе федеральное государственное бюджетное образовательное учреждение высшего образования «Курганский государственный университет» Научный редактор - Д.И. Дик. – Курган: Курганский государственный университет, 2016. – С. 140-143.

2. Хабибуллина, Э. Р. Обеспечение защиты информации при передаче ее по каналам связи / Э. Р. Хабибуллина // Информационные технологии обеспечения комплексной безопасности в цифровом обществе : Сборник материалов III Всероссийской молодежной научно-практической конференции, Уфа, 21–22 мая 2020 года / Отв. редактор А.С. Исмагилова. – Уфа: Башкирский государственный университет, 2020. – С. 86-89.

3. Кравченко, А. С. Вопросы обеспечения защиты информации при передаче по открытым каналам связи / А. С. Кравченко, А. Г. Фадеев // Математические методы и информационно-технические средства : Материалы X Всероссийской научно-практической конференции, Краснодар, 20–21 июня 2014 года. – Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования "Краснодарский университет Министерства внутренних дел Российской Федерации", 2014. – С. 158-160.

Статья поступила в редакцию 26.03.23; принята к публикации 10.05.2023.

Информация об авторах

Горошко П.Н. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Роговой Н.А. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Матвеев Д.А. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Горошко П.Н. - обработка материала, частичное написание статьи (40%).

Роговой Н.А. - обработка материала, частичное написание статьи (40%).

Матвеев Д.А. - идея, сбор материала, научное редактирование текста (20%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.55

Текущие проблемы проведения аудита информационной безопасности в России

Максим Дмитриевич Грива
Брянский государственный технический университет, Брянск, Россия
maks.griva.04@mail.ru

Аннотация. В статье разбираются проблемы, касающиеся проведения аудита информационной безопасности на предприятии.

Ключевые слова: проблемы аудирования, аудит информационной безопасности, информационная безопасность.

На сегодняшний момент вопрос с информационной защитой в России стоит достаточно остро. Разрабатываются новые системы защиты, улучшаются старые. Но главной проблемой, которая была и есть, является уязвимость изнутри, а именно люди, работающие на предприятии. В связи с этим необходимо проведение различных аудитов специалистами информационной безопасности, так как данную проблему невозможно решить на сто процентов, как например улучшить программу для защиты от вирусов.

Однако некоторые меры игнорируются так как отношение к информационной безопасности в малых и средних компаниях достаточно посредственно, в пример можно привести такие случаи когда работники оставляют пароли на бумажных носителях на рабочих местах. В связи с этим в данной статье будут описаны основные проблемы информационного аудита и возможные методы по их решению.

Проблемы аудита информационной безопасности

Проблемы, связанные с аудитом информационной безопасности сегодня, можно разделить на 7 основных областей:

1. Ограниченный охват: Многие компании фокусируют свой аудит информационной безопасности на соблюдении различных правил и стандартов, вместо того чтобы проводить комплексный аудит. В результате у компаний может возникнуть ложное чувство, они думают, что соответствуют требованиям и находятся в безопасности, даже если их мер защиты недостаточно для текущих и возникающих киберугроз.

2. Отсутствие стандартизации: Не существует стандартизированного подхода к проведению аудитов информационной безопасности. Многие компании разрабатывают свои собственные методологии, что может привести к противоречивым и ненадежным результатам аудита. Отсутствие стандартизации также затрудняет сравнение результатов аудита в разных организациях или сопоставление с лучшими отраслевыми практиками.

3. Недостаточный технический опыт: Аудиторы по информационной безопасности должны обладать техническими знаниями, необходимыми для понимания меняющегося ландшафта угроз и способов выявления и снижения рисков. К сожалению, многие организации либо не располагают собственными знаниями, либо полагаются на людей, не обладающих необходимыми навыками и опытом для проведения тщательных проверок безопасности.

4. Стоимость: Комплексный аудит безопасности может быть дорогостоящим и отнимать много времени. Многие организации могут предпочесть менее углубленный аудит, чтобы сэкономить на расходах, который может не дать информации, необходимой для устранения критических пробелов в безопасности.

5. Сложность регулирования: В России сложная нормативно-правовая база с множеством законов, подзаконных актов и стандартов, регулирующих информационную безопасность, включая Федеральный закон "О персональных данных" и Федеральный закон "Об информации, информационных технологиях и защите информации". Соблюдение этих законов может быть сложной задачей и может потребовать дополнительных ресурсов и времени для навигации.

6. Ограниченная доступность квалифицированных специалистов по кибербезопасности: В России имеется ограниченный количество квалифицированных специалистов по кибербезопасности, и спрос на этих специалистов часто превышает предложение на рынке. Это может затруднить поиск квалифицированных аудиторов для проведения всесторонней оценки практики обеспечения безопасности компаний.

7. Сопротивление изменениям: Некоторые российские компании могут сопротивляться внедрению новых мер безопасности или соблюдению передовой практики либо из-за непонимания возникающих рисков опасности, либо из-за опасений по поводу финансовых, технических или операционных последствий для их бизнеса.

Чтобы решить эти проблемы, организации должны уделять приоритетное внимание информационной безопасности и работать над тем, чтобы регулярно проводить всеобъемлющие, стандартизированные и технически обоснованные аудиты. Это требует выделения ресурсов на создание собственной технической экспертизы, использования услуг надежных сторонних экспертов по безопасности и инвестирования в инструменты, такие как платформы, управляемые искусственным интеллектом, которые могут помочь выявить потенциальные "слепые зоны" безопасности. Организациям также следует постоянно отслеживать меняющийся ландшафт угроз, чтобы убедиться, что их система безопасности не отстает.

Подводя вывод можно сказать, что проведение аудитов в целом является сложной комплексной задачей для решения которой необходимо соблюсти множество факторов, однако данная задача вполне выполнима если оглядываться на предложенные решения.

Список источников

1. Аверченков В. И., Рытов М. Ю., Кувылкин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти 2010 С. 5-99

2. УЦСБ 5 июля 2019 URL: https://www.ussc.ru/news/novosti/osobennosti-provedeniya-audita-informatsionnoy-bezopasnosti-obektov-kii/

3. РСИЦ 22 марта 2022 URL: https://www.ec-rs.ru/blog/informacionnaja-bezopasnost/analiz-i-otsenka-informatsionnoy-bezopasnosti/

Статья поступила в редакцию 26.03.23; принята к публикации 10.05.2023.

Научная статья
УДК 623:74

Использование комплекса формирования колебаний для постановки помех на основе динамического хаоса «Айсберг 2.0» для подавления каналов связи беспилотных летательных аппаратов

Иван Сергеевич Гришин[1]✉, Вадим Александрович Наумчик[2], Никита Сергеевич Хрущев[3], Юрий Юрьевич Громов[4]
[1,2,3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[4]Тамбовский государственный технический университет, Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0000-6355-4551
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0002-4833-4870
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0004-5814-2893
[4]gromov@is.tstu.ru, https://orcid.org/0000-0003-3313-2731

Аннотация. В статье рассматриваются вопросы организации подавления сигналов на каналы связи беспилотных летательных аппаратов путем постановки помех, создаваемых генераторами хаотических колебаний. Представлен программно-аппаратный комплекс постановки помех «Айсберг 2.0», сформирован принцип работы комплекса.

Ключевые слова: автоматизированные системы, беспроводная передача данных, сигнал, помехозащищенность, хаотические колебания.

Одними из задач, решаемыми беспилотными летательными аппаратами (БПЛА), являются анализ радиоэлектронной обстановки, разведка местности, численности и разнообразия сил противника. Данные задачи решаются наличием на борту БПЛА бортовой и стационарной подсистем, которые обеспечивают радиосвязь и передачу данных между БПЛА и пунктом управления.

Для радиоэлектронного подавления БПЛА может быть применен комплекс формирования колебаний для постановки помех на основе динамического хаоса «Айсберг 2.0».

Динамический хаос – непериодические колебания, возникающие в нелинейных детерминированных системах, демонстрирующие высокую чувствительность к начальным условиям. Эти колебания имеют ряд общих черт со случайными процессами, в частности, сплошной спектр мощности, но их природа связана не со случайностью, а с нелинейными свойствами, порождающими нерегулярные колебания в динамических системах. Так же динамический хаос является детерминированным, то есть значение сигнала можно точно рассчитать для каждого момента времени [3]. Динамический хаос возможно использовать в самых различных целях: кодирование информации, создание скрытых и защищенных систем связи, создание источников помех. Для выполнения этих задач необходимо реализовать специальные устройства

формирования хаотических колебаний или генераторы. Известно большое количество различных математических моделей генераторов хаотических колебаний, самой известной из которых является модель Лоренца. Эти математических модели достаточно хорошо исследованы в теории, но для получения генераторов на практике в виде рабочего изделия необходимо пройти долгий путь разработки и отладки электронного устройства, построенного на дискретных элементах.

Другим способом создания устройств формирования хаотических колебаний является использование электронно-вычислительных средств (микропроцессоров, ПЛИС). Данный способ исключает долгий процесс разработки устройства на дискретных элементах. При написании программы формируемый сигнал задается математическими уравнениями, что дает больше уверенности в качестве выходного сигнала. Ограничением служит лишь скорость выполнения команд у вычислительного устройства, а также разрядность цифроаналогового преобразователя и скорость его работы [3].

Наиболее известной и исследованной нелинейной системой дифференциальных уравнений с хаотическими колебаниями является система Лоренца. Специалист по физике атмосферы Э.Н. Лоренц предложил простую модель тепловой конвекции в атмосфере. В общем случае тепловые процессы описываются уравнениями теплопроводности. Лоренц сделал ряд допущений и получил трехмерную модель тепловой конвекции в обыкновенных дифференциальных уравнениях [3].

На рис. 1 изображена фазовая траектория модели при заданных параметрах. По рисунку видно, что имеется два состояния равновесия, так называемый «странные аттракторы Лоренца». У данной траектории имеется несколько особенностей.

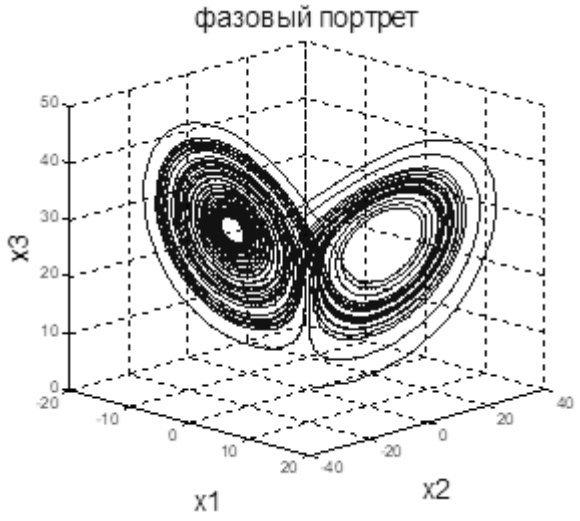

Рис. 1. Движение системы в фазовом пространстве

Первая особенность данной траектории заключается в том, что каждая из точек равновесия не является притягивающей. Однако траектория не уходит далеко от точек равновесия и занимает ограниченную область. Таким образом, получаются нерегулярные непериодические движения системы – в системе

имеет место хаос.

Второй особенностью является то, что внутри данного аттрактора траектория движения очень чувствительна к начальным условиям. При малейшем расхождении в начальных условиях движение системы будут сильно расходиться почти сразу. Такие аттракторы получили название «странные аттракторы» [3].

Программно-аппаратный комплекс «Айсберг 2.0» (рис. 2) представляет собой набор генераторов хаотических колебаний, сигналы от которых поступают на специальный блок коммутации сигналов. Блок коммутации образует различные комбинации входных сигналов, такие как сумма, произведение, либо выводит каждый из сигналов на определенное время, формируя тем самым сигнал, представляющий собой последовательность идущих друг за другом хаотических сигналов. В качестве аппаратной части устройства выступает программируемая логическая интегральная схема (ПЛИС). Она представляет собой набор логических элементов, расположенных на одном кристалле. В матрицах переключений задаются соединения логических элементов друг с другом через соединительные шины. Блоки ввода-вывода обеспечивают передачу и прием информации от внешних устройств [3].

Программирование ПЛИС заключается в конфигурации матриц переключений таким образом, чтобы получилось необходимое логическое устройство. ПЛИС, в отличие от процессоров, выполняют запрограммированные задачи параллельно, а не последовательно, что обеспечивает большую скорость вычислений.

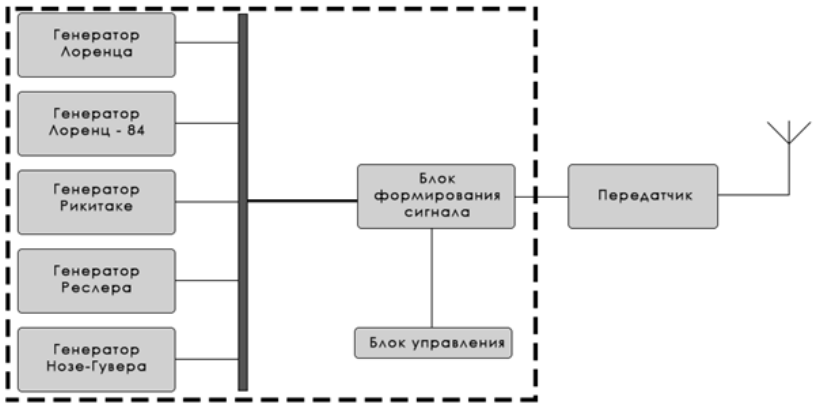

Рис. 2. Структурная схема устройства генератора «Айсберг 2.0»

Основной особенностью разработанного устройства «Айсберг 2.0» являются:

– универсальность;

– возможность расширения;

– интеллектуальное формирование сигнала [4].

Универсальность заключается в возможности в одном устройстве содержать несколько генераторов сигналов. Возможность расширения подразумевает быстрый способ обновления устройства путем его замены на новое более мощное, либо просто обновления программы с новыми

генераторами колебаний. Интеллектуальное формирование сигнала позволяет получать на выходе устройства колебания как с отдельного генератора, так и сумму сигналов, либо формирование сигнала как последовательность колебаний различной длительности и следующих в различном порядке.

Список источников

1. Шахтарин Б.И. и др. Генераторы хаотических колебаний: учебное пособие // Москва: Гелиос АРВ, 2007. 248 с.

2. Кобылкина П.И., Сидоркина Ю.А., Морозова В.Д. Источники хаотических колебаний с дискретным временем // Научный вестник МГТУ ГА. Сер. Радиофизика и радиотехника, 2003. № 62. С. 140-147.

3. Бардашов А.В., Киселев М.Д., Манюхин В.А., Тулинов И.С., Кольчугин К.Ю., Громов Ю.Ю. Реализация устройства формирования хаотических колебаний на ПЛИС // Приборы и системы. Управление, контроль, диагностика. - № 8. – 2017. – С.14 – 25.

4. https://www.nika-penza.ru/files/vol1-2020.pdf.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Гришин И.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Наумчик В.А. – оператор научной роты войск радиоэлектронной борьбы.

Хрущев Н.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Громов Ю.Ю. – директор Института автоматики и информационных технологий.

Вклад авторов

Гришин И.С. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Наумчик В.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Хрущев Н.С. – сбор материала, обработка материала, частичное написание статьи (25%).

Громов Ю.Ю. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.9

Математическое обеспечение проектирования специальных микросхем

Артем Сергеевич Грошев [1]✉, Олег Геннадьевич Орлов [2], Сергей Викторович Стоянов [3], Владимир Иванович Силонов [4], Алексей Евгеньевич Анисимов [5]

[1,2,3,4,5,] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия

[1]groshik@mail.ru✉, http://orcid.org/0000-0003-0027-3442

[2] ogo2787@mail.ru, https://orcid.org/0000-0003-1820-8110

[3] ssv@mail.ru, https://orcid.org/0000-0003-0220-7811

[4] kaspell@mail.ru, https://orcid.org/0000-0003-1710-8145

[5] Alex_x1999x@mail.ru, https://orcid.org/0000-0003-1120-1027

Аннотация. В статье рассматривается математическое обеспечение систем автоматизации проектирования радиационно-стойких микросхем. приводится опыт работы в этой области. Указывается библиотека с учетом норм технологического процесса предприятия.

Ключевые слова: САПР, графическая подсистема, модули, процедуры.

В настоящее время КМОП БИС находит широкое применение в аппаратуре общего и специального назначения. Эти схемы должны обеспечивать работоспособность и соответствующие технические показатели в широком диапазоне температур, больших механических нагрузках, в условиях химического, радиационного и других воздействий. Данные требования и возрастающая сложность узлов КМОП БИС, изменение методологии их проектирования и производства требуют постоянного совершенствования средств автоматизации проектирования.

Резкое сокращение количества предприятий, которые могли самостоятельно реализовывать полный цикл «проектирование – производство» различных классов микросхем привел к необходимости применения технологии «разделения функций», когда проектирование и изготовление БИС осуществляется различными предприятиями.

В этих условиях актуальна разработка средств автоматизации проектирования базовых элементов КМОП БИС двойного назначения, представляющие собой как базовые двоичные элементы, так и функциональные блоки на функционально-логическом и схемотехническом уровнях в условиях радиационного воздействия [6].

Разработаны математические модели элементов с учетом конструктивно-технологических параметров и характеристик ВВФ в соответствии с КГС «Климат-7» [1, 2, 3, 4, 5].

Для статических видов ионизирующего излучения экспериментально определены все функциональные зависимости параметров модели от дозы и вида излучения для аттестованного техпроцесса в уравнении ВАХ МОПТ. Для определения коэффициентов аппроксимации были изготовлены кристаллы с типовыми тестовыми структурами, разработана методика измерений и проведены необходимые испытания.

Для учета импульсных видов ВВФ используются генераторы ионизационных токов. Величина которых в зависимости от конструкции и параметров излучения определяется полученными соотношениями.

Моделирование базовых элементов на функционально-логическом уровне с учетом радиации предложено проводить в соответствии с разработанной методикой. Вначале осуществляется предварительный логический анализ с последующим переходом на схемотехнический уровень иерархии для моделирования базовых элементов. На этом этапе рассчитываются изменение времени переключения тестовых элементов, нагрузочных способностей, помехоустойчивости и др. за счет воздействия радиации, температуры и т.п. Далее проводится логический анализ, моделирование неисправностей с учетом реальных параметров, генерация тестов, поиск и анализ дефектов.

Этап функционально-логического моделирования и генерации тестов базовых элементов является наиболее трудоемким. Для реализации задачи синтеза тестов необходимо решать задачу моделирования неисправностей. При этом важнейшим требованием является обеспечение единства построения средств логического анализа, моделирования неисправностей, анализа схем на тестопригодность. Степень тестопригодности схемы оценивается количеством невыявленных неисправностей из числа возможных [6].

С помощью разработанных средств моделирования создана иерархическая библиотека стандартных элементов с учетом радиационного воздействия для создания широкой номенклатуры КМОП БИС для ЦОС, которая позволяет конструировать интегральные схемы любой сложности [6].

Данная библиотека имеет 3 уровня иерархии, каждый из которых объединяет элементы по их сложности. Нулевой уровень – элементарные структуры, включающие в себя двоичные элементы и логические ячейки (инверторы, «И-НЕ», «ИЛИ-НЕ», исключающее ИЛИ и их комбинации), триггеры и т.п. Первый уровень – более сложные элементы счетчики, дешифраторы, сумматоры и т.д. Третий уровень – макрофрагменты функционально-законченных блоков: контроллеры, АЛУ, умножители и т.п.

Список источников

1. Чубур К.А. Разработка математических моделей физических процессов в разнородной многослойной структуре при радиационном воздействии / Чубур К.А., Струков И.И., Евдокимова С.А., Белокуров В.П., Платонов А.Д., Черкасов О.Н., Зольников К.В. // Моделирование систем и процессов. 2022. Т. 15. № 1. С. 125-133.

2. Чубур К.А. Математическая модель поглощения энергии излучения многослойной структурой и решение сеточным методом / Чубур К.А., Струков

И.И., Евдокимова С.А., Волков В.С., Платонов А.Д., Черкасов О.Н., Чевычелов Ю.А. // Моделирование систем и процессов. 2022. Т. 15. № 1. С. 133-140.

3. Журавлева И.В. Полупроводниковые технологии для реализации радиационно-стойких СБИС / Журавлева И.В., Попова Е.А. // Моделирование систем и процессов. 2022. Т. 15. № 1. С. 44-52.

4. Журавлева И.В. Развитие технологии систем на кристалле для современной электронной компонентной базы / Журавлева И.В., Попова Е.А. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 12-20.

5. Полуэктов А.В. Моделирование колебательных процессов в пакете MVSTUDIUM / Полуэктов А.В., Зольников К.В., Анциферова В.И. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 139-148.

6. Крюков В.П. Проектирование базовых элементов комплементарных БИС двойного назначения. – Воронеж, 2002.

Статья поступила в редакцию 23.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Грошев А.С. - преподаватель «Базовая кафедра технического и программного обеспечения вычислительных и информационных систем» ФГБОУ ВО «ВГЛТУ».

Орлов О.Г. - преподаватель СПО кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Стоянов С.В. - аспирант *ФГБОУ ВО «ВГЛТУ»*.

Силонов В.И. - Системный администратор «Базовая кафедра технического и программного обеспечения вычислительных и информационных систем» ФГБОУ ВО «ВГЛТУ».

Анисимов А.Е. - преподаватель СПО кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Грошев А.С. - идея, сбор материала, обработка материала, научное редактирование текста.

Орлов О.Г. - частичное написание статьи (25%).

Стоянов С.В. - частичное написание статьи (25%).

Силонов В.И. - частичное написание статьи (25%).

Анисимов А.Е. - частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.5

Анализ стратегий компьютерной безопасности стран Евросоюза

Максим Леонидович Гулак[1]✉, Светлана Владимировна Минина[2]
[1]Брянский государственный технический университет, Брянск, Россия
[2]Брянский государственный университет им. акад. И.Г. Петровского, Брянск, Россия
[1]gml13@yandex.ru✉, http://orcid.org/0009-0009-3131-4292
[2]s_minina@mail.ru, https://orcid.org/0009-0002-2243-5040

Аннотация. Проведен сравнительный анализ стратегий кибербезопасности некоторых стран Европейского Союза и стратегии самого Евросоюза, взгляд правительств этих государств на проведение наступательных операций в киберпространстве. Рассмотрены стратегические цели, обозначенные в стратегиях кибербезопасности стран ЕС.

***Ключевые слова*:** кибербезопасность, глобальный индекс кибербезопасности, угроза кибербезопасности, информационная безопасность, ENISA.

Стратегия кибербезопасности – документ, который фиксирует и определяет государственную политику, направленную на обеспечение безопасности государства в киберпространстве.

В статье рассмотрены и исследованы стратегии кибербезопасности стран-участниц Европейского союза, занимающих лидирующие позиции в Глобальном индексе кибербезопасности, а именно Германия, Франция, Испания и Эстония [1].

Необходимо также учитывать, что Германия, Франция и Испания являются крупнейшими экономиками Европы, а Эстония, помимо того, что заняла 3-е место в Глобальном индексе кибербезопасности среди европейских государств, является штаб-квартирой Киберцентра НАТО [2].

В международном стандарте ISO/IEC 27032:20125 даются следующие определения терминов «киберпространство» и «кибербезопасность»:

Кибербезопасность (или безопасность киберпространства) – сохранение конфиденциальности, целостности и доступности информации в киберпространстве.

Киберпространство – это сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и услуг в сети Интернет с помощью технологических устройств и подключенных к нему сетей, которые не существуют в какой-либо физической форме.

Начнем рассмотрение стратегий кибербезопасности со Стратегии кибербезопасности Европейского Союза, как альянса государств.

Стратегия кибербезопасности ЕС на цифровое десятилетие (2020) (The EU's Cybersecurity Strategy for the Digital Decade 2020) принята Европейской Комиссией 16 декабря 2020 в Брюсселе и определяет направления повышения устойчивости к киберугрозам и обеспечения использования гражданами и предприятиями защищенных цифровых технологий [1].

В Стратегии описаны способы использования ЕС своих инструментов и ресурсов для обеспечения технологической независимости. Также в Стратегии изложены направления сотрудничества ЕС с государствами-партнерами, разделяющими ценности демократии, верховенства закона и прав человека.

Среди прочих вопросов рассмотрено текущее состояние и запланировано развитие безопасной цифровой трансформации в среде сложных угроз, устойчивой инфраструктуры и критически важных сервисов, потенциал для предотвращения, сдерживания и реагирования на киберугрозы, развития и продвижения киберпространства, кибербезопасность в органах, институтах и агентствах ЕС.

В Стратегии обозначены и проблемы в области кибербезопасности. Приведем некоторые из них:

- из-за геополитической напряженности усугубляется положение с имеющимися угрозами, что проявляется в «установлении национальными государствами цифровых границ»;
- возникновение рисков глобального масштаба как следствие выбора злоумышленниками объектов КИИ в качестве мишени;
- наличие цифровой составляющей в расследовании почти всех видов преступлений;
- наиболее частые и желанные цели для кибератак – финансовый сектор и цифровые услуги;
- недостаточный уровень взаимного обмена информацией о киберугрозах, который мог бы помочь более объективно оценить состояние кибербезопасности в ЕС.

В документе указано, что Стратегия кибербезопасности ЕС призвана обеспечить глобальный и открытый Интернет с надежными гарантиями безопасности, для чего предлагается реализовать предложения по использованию базовых инструментов, представляющих собой политические, инвестиционные и регуляторные инициативы, затрагивающие такие области деятельности ЕС как:

- устойчивость, технологический суверенитет и лидерство;
- оперативные возможности для предотвращения, сдерживания и реагирования;
- сотрудничество в целях развития глобального и открытого киберпространства.

В Стратегии кибербезопасности ЕС было отмечено, что необходим пересмотр основ политики ЕС в области кибербезопасности, в результате чего в 2022 году была принята Стратегия кибероборонь Евросоюза.

Проведение Россией специальной военной операции заставило ЕС пересмотреть свой подход к обеспечению безопасности в целом и

кибербезопасности в частности: «ЕС необходимо быть более самостоятельным в этой сфере, поэтому необходимо действовать более скоординировано и уделять больше внимания вопросам защиты от цифровых угроз». Для этого были определены четыре направления деятельности:

1. Совместная работа для усиления кибероборонны.
2. Безопасность оборонной экосистемы.
3. Инвестирование в возможности кибероборонны.
4. Развитие партнерских отношений в сфере кибероборонны.

Стратегия кибербезопасности Германии [3] имеет определенные нюансы и особенности.

Особое внимание в ней уделяется четырем сферам: общество, частный бизнес, правительство, международные отношения Европейского Союза.

С учетом этого в Стратегии кибербезопасности ФРГ предусмотрены руководящие принципы:

1. Построение кибербезопасности как совместной задачи правительства, научно-исследовательской области, частного сектора и общества.
2. Укрепление цифровой независимости.
3. Безопасная цифровая трансформация.
4. Установление прозрачных и измеримых целей.

Национальная стратегия кибербезопасности Испании [4] определяет следующие направления и сферы деятельности:

1. «Киберпространство за пределами общего глобального пространства» – дается общее представление о сфере кибербезопасности.
2. «Угрозы и вызовы в киберпространстве» – определяются основные угрозы киберпространству (кибершпионаж, киберпреступность).
3. «Предложение, принципы и цели в области кибербезопасности» – общие указания в области кибербезопасности.
4. «Направления действий и меры» – установлены 7 направлений действий и определены меры по развитию каждого из них.
5. «Кибербезопасность в системе национальной безопасности».

В документе указывается, что безопасность киберпространства – это важнейшая цель, достижение которой гарантирует обеспечение национальной безопасности и возможность для государства строить цифровое общество.

Французская национальная стратегия цифровой безопасности [4] разделена на 5 стратегических направлений:

1. Важнейшие интересы, безопасность и защита государственных информационных систем и критически важных инфраструктур, кризис кибербезопасности.

Должна обеспечиваться защита интересов Франции в киберпространстве и безопасность критической инфраструктуры.

2. Цифровое доверие, конфиденциальность, персональные данные, кибервраждебность.

Должно развиваться использование киберпространства в соответствии с заявленными ценностями и обеспечиваться защищенность цифровой жизни граждан.

3. Повышение осведомленности и квалификации, базовая подготовка.

Будет повышаться осведомленность детей о цифровой безопасности, начиная со школьного возраста. Начальное, высшее и дополнительное образование будут иметь раздел, посвященный цифровой безопасности.

4. Бизнес цифровых технологий, промышленная политика, экспорт и интернационализация.

Создание среды, благоприятной для исследований и инноваций, поддержание и международное продвижение французских цифровых продуктов и услуг.

5. Европа, цифровая автономность, стабильность киберпространства.

Становление Франции одной из движущих сил европейской стратегической автономии, безопасного, открытого и стабильного киберпространства.

Стратегия кибербезопасности Эстонии [4] была одной из первых стратегий в мире.

Документ включает такие разделы, как:

1. Текущее состояние кибербезопасности.
2. Координация и реализация стратегии.
3. Стратегические цели.
   - Устойчивое цифровое общество.
   - Индустрия кибербезопасности, исследований и разработок
   - Ведущий международный участник
   - Киберграмотное общество.

Авторы документа указывают, что в создание Стратегии были вовлечены все заинтересованные стороны: государственный сектор экономики (гражданский и оборонный), поставщики услуг, отраслевые предприниматели и научные круга.

В стратегии говорится, что Эстония – международно признанный лидер в области кибербезопасности, что способствует поддержанию национальной безопасности и обеспечивает рост конкурентоспособности компаний в этой области.

Список источников

1. Global Cybersecurity Index 2020, ITU: – Режим доступа: https://www.itu.int.

2. The European Union Agency for Network and Information Security. – Режим доступа: https://www.enisa.europa.eu.

3. Cyber Security Strategy for Germany, 2021. – Режим доступа: https://www.bmi.bund.de.

4. Стратегии кибербезопасности государств Европейского Союза. – Режим доступа: https://www.infowatch.ru/analytics/analitika/strategii-kiberbezopasnosti-gosudarstv-evropeyskogo-soyuza.

Статья поступила в редакцию 17.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Гулак М.Л. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Минина С.В. – к.филол.н., доцент кафедры немецкого языка ФГБОУ ВО «БГУ».

Вклад авторов

Гулак М.Л. – идея, сбор материала, обработка материала, частичное написание статьи (50%), научное редактирование текста.

Минина С.В. – обработка (перевод) материала, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.051

Анализ методов обнаружения внешних угроз информационной безопасности в корпоративных сетях

Алексей Александрович Елин[1], Павел Игоревич Карасев[2], Хайдар Абдулваххаб Х. Шамсулдин [3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]elin.a.a@edu.mirea.ru, https://orcid.org/0009-0006-9088-2212
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3]fit_tstu@mail.ru, https://orcid.org/0009-0007-4529-9674

Аннотация. В статье рассматриваются типы вторжений в корпоративные сети и методы их обнаружения, а также проблемы, с которыми сталкиваются эти методы.

Ключевые слова: информационная безопасность, корпоративные сети, методы обнаружения вторжений.

Сохранение безопасности корпоративной сети является важным аспектом для организаций, которые обрабатывают и хранят конфиденциальную информацию. Различные виды атак могут привести к утечке данных, нарушению работы систем и серьезному повреждению функциональности сети. В связи с этим, организации должны принимать меры по обеспечению безопасности своих корпоративных сетей, используя современные методы и инструменты защиты от внешних угроз.

Для обеспечения безопасности корпоративной сети необходимо понимать различные типы вторжений, которые могут произойти. Эти типы можно разделить на следующие группы:

1. Атаки на уязвимости ПО - эти атаки направлены на эксплуатацию уязвимостей в программном обеспечении, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к сети.
2. Атаки на пользователей – злоумышленники могут использовать социальную инженерию, фишинговые атаки и другие методы, чтобы обмануть пользователей и получить доступ к корпоративным ресурсам.
3. Атаки на сеть – такие атаки направлены на использование уязвимостей в самой сети, например, перехват и подмена трафика, денай-оф-сервис атаки и другие.
4. Вредоносное ПО – это программы, предназначенные для повреждения, уничтожения или кражи данных, которые могут быть установлены на компьютерах пользователей или серверах в корпоративной сети.

После анализа основных типов вторжений, рассмотрим способы обнаружения таких атак. В настоящее время, организации применяют различные методы обнаружения вторжений в свои корпоративные сети.

Одним из таких является система обнаружений вторжений (Intrusion Detection System, IDS), которая позволяет мониторить сетевой трафик и анализировать его на наличие аномалий, сигнализируя о возможных атаках. Эта технология может быть применена для обнаружения различных типов угроз, включая атаки на уязвимости ПО, атаки на пользователей и вредоносное ПО.

Другой метод - системы профилактики и предотвращения вторжений (Intrusion Prevention System, IPS), которые не только обнаруживают вторжения, но и принимают меры для их предотвращения. IPS-системы могут быть особенно полезны для предотвращения атак на сеть, в том числе попыток использования уязвимостей ПО для вторжения в сеть.

Также часто используются системы мониторинга безопасности (Security Information and Event Management, SIEM), которые собирают и анализируют информацию о событиях в сети, и позволяют оперативно реагировать на возможные угрозы. SIEM-системы могут быть эффективны для выявления атак на пользователей, таких как фишинговые атаки, а также для обнаружения различных типов вредоносного ПО.

Кроме того, существуют специализированные инструменты, такие как сканеры уязвимостей, которые сканируют сеть на наличие уязвимостей и помогают обнаружить потенциальные точки входа для злоумышленников. Это полезный инструмент для обнаружения уязвимостей ПО, которые могут быть использованы для атак на сеть.

Многие организации используют комбинацию этих методов для обеспечения максимальной защиты своих корпоративных сетей. Однако, каждый из них имеет свои ограничения и проблемы, которые могут затруднить их эффективное применение.

Системы обнаружения вторжений часто сталкиваются с проблемой ложных срабатываний, которые могут быть вызваны аномальным поведением сети, не связанным с вторжением. IDS также могут не обнаружить новые типы атак или вредоносных программ без сигнатур для обнаружения, и могут быть обойдены злоумышленником методами обхода сигнатур.

Системы профилактики и предотвращения вторжений рискуют блокировать легитимный трафик, что может привести к проблемам доступа к ресурсам и сервисам. Кроме того, системы IPS могут иметь проблемы с обработкой большого объема трафика, что может приводить к замедлению работы сети.

Системы мониторинга безопасности могут иметь проблемы с отсутствием интеграции между различными инструментами мониторинга и службами информационной безопасности. Это может привести к тому, что некоторые события могут оставаться незамеченными или неправильно классифицироваться. Такие системы могут быть дорогостоящими в использовании, и требуют специалистов по безопасности для проведения мониторинга и анализа данных.

Сканеры уязвимостей также не являются идеальными, поскольку они могут пропустить некоторые уязвимости, не поддающиеся сканированию, или находящиеся за пределами их области видимости. База данных уязвимостей может быть неполной или не обновленной, что может привести к тому, что сканеры не смогут обнаружить только что появившиеся уязвимости. Помимо этого, сканеры уязвимостей могут давать ложные срабатывания, требующие дополнительной проверки и анализа.

Существуют решения, которые могут помочь снизить количество ложных срабатываний и повысить эффективность использования методов обнаружения вторжений, решая многие из связанных с ними проблем.

Для повышения эффективности системы обнаружения вторжений можно применять алгоритмы машинного обучения, которые учатся на основе предыдущих событий, чтобы отличать аномальное поведение, связанное с вторжением, от других типов аномалий. Такой подход позволяет уменьшить количество ложных срабатываний. Решить проблему обхода сигнатур можно, используя системы, которые анализируют поведение в сети для обнаружения аномальных действий, совместно с IDS.

Для уменьшения риска блокировки легитимного трафика, системы IPS могут использовать многоуровневые архитектуры, такие как блокирование на уровне сетевого устройства или на уровне приложения, а также технологии, такие как глубокая инспекция пакетов (DPI), для более точной идентификации угроз и их предотвращения. Также можно использовать технологии балансировки нагрузки и механизмы автоматического восстановления после блокировки легитимного трафика.

Централизованное управление может улучшить системы мониторинга безопасности, интегрируя различные инструменты и службы. Это обеспечивает быстрое реагирование на события в режиме реального времени и снижает риск неправильной классификации событий. Облачные решения и аутсорсинг услуг могут помочь снизить затраты, но требуют тщательного анализа и выбора надежных поставщиков услуг, учитывая риски конфиденциальности данных и доступа к сети.

Комбинация различных сканеров уязвимостей может увеличить вероятность обнаружения угроз и снизить вероятность ложных срабатываний. Регулярное обновление баз данных и применение различных методов сканирования, включая сетевые устройства, приложения и код, также важны для выявления скрытых уязвимостей.

Вывод: механизмы обнаружения вторжений не гарантируют полной защиты корпоративных сетей, но их комбинация может снизить вероятность угроз и ложных срабатываний. Регулярное обновление и анализ систем безопасности важны для выявления и устранения проблем. Правильный подход к обеспечению безопасности сетей снизит риски угроз и защитит данные компании.

Список источников

1. Биячуев Т.А., Осовецкого Л.Г., Безопасность корпоративных сетей, 2004 г. - 161 с.

2. Чжэньвэй Ю, Джеффри Дж. П. Цай, Обнаружение вторжений: подход машинного обучения, 2011 г, - 184 с.

3. Бирюков А.А., Информационная безопасность: защита и нападение, 2017 г, - 434 с.

Статья поступила в редакцию 21.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Елин А.А. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.03.01 – Информационная безопасность» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Шамсулдин Хайдар Абдулваххаб Х. - аспирант «ТГТУ».

Вклад авторов

Елин А.А. - идея, сбор материала, обработка материала (50%).

Карасев П.И. - написание статьи, научное редактирование текста (40%).

Шамсулдин Хайдар Абдулваххаб Х. - частичное написание статьи (10%).

Конфликт интересов отсутствует.

Научная статья
УДК 623:74

Использование системы автоматизированного комбинирования цифровых фильтров для обеспечения качественной передачи сигналов с беспилотных летательных аппаратов

Альберт Русланович Зайдуллин[1]✉, Илья Александрович Омельченко[2], Вадим Александрович Наумчик[3], Александр Александрович Гусев[4]
[1,2,3,4]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0005-2857-9290
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0002-5941-9589
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0002-4833-4870
[4]nauchnajarota@yandex.ru, https://orcid.org/0009-0002-9414-3290

Аннотация. В статье рассматривается применение автоматизированной системы подбора цифровых фильтров для обеспечения качественной передачи сигналов с БПЛА. Описан алгоритм расчета соотношения сигнал/шум для систем, в которых невозможно определить отдельный шумовой сигнал. Так же описан алгоритм подбора цифровых фильтров, имеющих наилучше соотношение сигнал/шум. Приведены обобщенные результаты тестов комбинаций цифровых фильтров.

Ключевые слова: фильтрация, сигналы, алгоритмы, комплекс.

На текущий момент беспилотные летательные аппараты (БПЛА) в сфере радиоэлектронной борьбы используются для осуществления радиопомех. Поэтому очень важным становится вопрос обеспечения качественной передачи сигналов с БПЛА, поскольку это может повлиять на дальнейшее функционирование системы и привести к тяжелым последствиям.

В настоящее время в подавляющем количестве устройств и систем, требующих использования цифровых фильтров, применяется как правило один конкретный фильтр либо четко определенная их последовательность либо комбинация. Это происходит с целью экономии вычислительных ресурсов устройств и почти всегда оправдано, но в некоторых случаях, для получения наибольшего качества фильтрации в ущерб общему быстродействию, необходимо использовать автоматизированный подбор наилучшего фильтра или оптимальной последовательности фильтров из большого количества заранее спроектированных, так как высокий уровень подавления помех в сигнале позволяет сократить шанс появления вредных серьезных воздействий на беспилотные летательные аппараты (БПЛА) [1]. Используя технологию SDR (программно-определяемая радиосистема – любое устройство передачи данных, в котором некоторые или все функции физического уровня являются программно-определяемыми) автоматизированный подбор цифровых фильтров

можно организовать на устройствах без привязки к их массогабаритным показателям. Для тестирования системы автоматизированного подбора и комбинирования цифровых фильтров операторами Научной роты войск радиоэлектронной борьбы ВС РФ была разработана программа Combination Signal Filter. Программа написана на фреймворке Qt, с использованием библиотеки Audiofile с открытым исходных кодом, что исключает возможность каких-либо подкладок. Так же она обладает свойством кроссплатформенности, что позволяет запускать ее практически на любых платформах, в том числе и на миникомпьютерах. В качестве входного обрабатываемого сигнала в ней используется аудиофайл формата .wav. В качестве возможных шумов рассматривается как постоянный шум (аддитивный белый гауссовский шум или АБГШ) с относительно стабильной амплитудой, так и случайные импульсы, вызванные внешними факторами. Программа имеет 2 основных модуля: ручного подбора фильтров и автоматизированного подбора [4].

Оба модуля программы используют следующий набор цифровых фильтров [4]:

– арифметическое среднее, идея которого состоит в том, что шумы в сигнале имеют частые флуктуации и при усреднении в значительной степени должны себя подавить (сгладить), а сам сигнал изменяется незначительно в пределах умеренного;

– бегущее арифметическое среднее – аналогично предыдущему фильтру, но работает по принципу буфера, в котором хранятся несколько последних измерений для усреднения, при каждом вызове фильтра буфер сдвигается, в него добавляется новое значение и убирается самое старое, далее буфер усредняется по среднему арифметическому;

– экспоненциальное бегущее среднее, при котором к предыдущему фильтрованному значению прибавляется новое, помноженное на коэффициент, отражающий важность нового значения по сравнению с предыдущим;

– медианный фильтр третьего порядка, выбирающий без вычислений среднее значние из трех предыдущих временных дискретов сигнала;

– фильтр Калмана – последовательный рекурсивный алгоритм, использующий принятую модель динамической системы для получения оценки, которая может быть существенно скорректирована в результате анализа каждой новой выборки измерений во временной последовательности [3];

– LMS фильтр с линейной функцией - инструмент специального назначения, позволяющий буквально предсказывать поведение значения за период.

Модуль автоматизированного подбора служит для поиска оптимальной комбинации цифровых фильтров. Главным критерием, по которому ведется оптимизация служит соотношение сигнал/шум. Из-за сложности при отдельной идентификации шума во входящем сигнале, соотношение сигнал шум вычисляется следующим образом [4]:

1. Для того что бы не тратить большие объемы вычислительной мощности для дальнейшей работы создается выборка, в которую отбирается некоторое количество равнораспределенных временных дискретов. В программе это

количество равно 100.

2. Из полученной выборки выделяют максимальное значение и записывают его амплитуду.

3. Выделяют так же 90% дискретов с наименьшей амплитудой.

4. Из выбранных 90% выделяют среднеарифметическое значение – именно оно и принимается как уровень шума.

Для нахождения оптимальной последовательности фильтров программа выполняет следующие действия [4]:

1. Обрабатывает исходный сигнал каждым из фильтров и записывает соответствующие соотношения сигнал/шум.

2. Далее каждый из результатов обработки повторно обрабатывается каждым из фильтров. При этом собираются данные о разности соотношений сигнал/шум до и после второй фильтрации.

3. Собранные данные выводятся в графический интерфейс и показаны на рис. 1. Так же туда выводится информация о наибольшем итоговом соотношении сигнал/шум среди всех комбинаций.

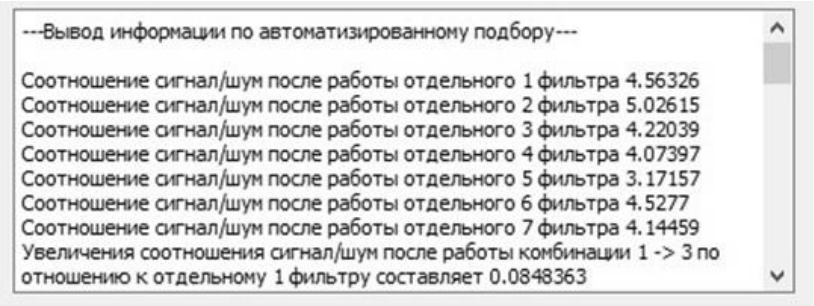

Рис. 1. Вывод информации по работе модуля автоматизированного подбора

В результате серии тестов над разными аудиофайлами были сделаны следующие выводы [4]:

– в большинстве случаев при комбинировании фильтров система показала превосходство связок: медианный фильтр третьего порядка -> арифметическое бегущее среднее; арифметическое бегущее среднее -> фильтр Калмана;

– зачастую наибольшее соотношение сигнал/шум обеспечивали комбинации дающие малые значения при других исходных сигналах.

В модуле ручного подбора, показанном на рисунке 3, предлагается самостоятельно выбрать комбинацию фильтров, которые будут использоваться. В графический интерфейс при этом выводятся показатели соотношения сигнал/шум для каждого из пяти возможных этапов фильтрации. Так же в данном режиме работы производится сохранение аудиофайлов, получившихся в результате фильтрации. По этим файлам можно производить субъективную оценку качества фильтрации.

Данная система подбора фильтров была успешно внедрена в программу SDRPro, входящую в программно-аппаратный комплекс «Рубеж».

Таким образом, использование системы автоматизированного подбора цифровых фильтров позволяет повысить качество сигналов, передаваемых с беспилотных летательных аппаратов.

Список источников

1. Затучный Д.А., Ребров Е.Д. Моделирование траектории полета беспилотного летательного аппарата с учётом возможных навигационных помех искусственного и естественного происхождения // Труды Международного симпозиума «Надежность и качество», 2021. Т. 1. 346 с.

2. Сизиков В.С., Лавров А.В. Устойчивые методы математико-компьютерной обработки изображений и спектров. Учебное пособие. – Санкт-Петербург: Университет ИТМО. 2018 . 70 с.

3. Иванов Д.С., Карпенко С.О., Овчинников М.Ю. Алгоритм оценки параметров ориентации малого космического аппарата с использованием фильтра Калмана // Препринты ИПМ им. М.В.Келдыша, 2009. № 48. 32 с.

4. Мерочкин А.С., Будников Р.К., Самойлов В.Д., Клонин И.П., Громов Ю.Ю. Математическое моделирование процесса автоматизированного комбинирования цифровых фильтров // Надежность и качество: труды международного симпозиума. – Пенза, 2022, - Т. 1. – С. 82 – 84.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Зайдуллин А.Р. – оператор научной роты войск радиоэлектронной борьбы.

Омельченко И.А. – старший оператор научной роты войск радиоэлектронной борьбы.

Наумчик В.А. – оператор научной роты войск радиоэлектронной борьбы.

Гусев А.А. – младший научный сотрудник научной роты войск радиоэлектронной борьбы.

Вклад авторов

Зайдуллин А.Р. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Омельченко И.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Наумчик В.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Гусев А.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.5

Шифрование на основе ДНК для мобильных сетей

Антон Иванович Заревич[1]✉, Александр Владимирович Полуэктов[2], Филипп Владимирович Макаренко[3]
[1, 2, 3]Воронежский государственный лесотехнический университет имени Г.Ф. Морозова, Воронеж, Россия
[1]antonzarevich@ngs.ru✉, https://orcid.org/0009-0000-5354-5598
[2]palv2006@yandex.ru, http://orcid.org/0009-0005-4032-5031
[3]Phillipp@mail.ru, https://orcid.org/0009-0001-9311-8942

Аннотация. Молекулярно-биологические модели, такие как эволюция ДНК, могут стать основой архитектур, обеспечивающих высокую степень диффузии и хаоса, а также устойчивость к криптоанализу. Такие механизмы шифрования могут обслуживать как крупные, так и небольшие приложения и могут существовать как на уровне приложений, так и на уровне сети. В статье кратко описываются основы собственного механизма шифрования, который использует принципы репликации ДНК и стеганографии (криптографии со скрытыми словами) для получения конфиденциальных данных. Основа подхода включает организацию закодированных слов и сообщений с использованием пар оснований, организованных в гены, расширяемый геном, состоящий из хромосомных ключей на основе ДНК, и процесс кодирования, репликации и эволюции сообщений на основе ДНК. Такая модель шифрования обеспечивает «Безопасность за счет неизвестности».

Ключевые слова: шифрование, ДНК-вычисление, криптография, вычислительная биология.

Введение

К мобильным одноранговым сетям (MANET) предъявляются ряд требований по различению доверенных одноранговых узлов, конфиденциальной передаче и приёму информацию, незапланированному и непредсказуемому входу и выходу узлов. Использование эволюционных вычислений и подхода, основанного на принципах подобия ДНК (дезоксирибонуклеиновой кислоты) [1], являются ключевыми в разработке современных архитектур MANET.

В статье представлена новая техника шифрования. Из-за динамического, эволюционного характера подхода ДНК потенциальные злоумышленники должны постоянно перехватывать инструкции по декодированию между источником и получателем. Отсутствие одного поколения информации для расшифровки генома серьезно искажает процесс расшифровки. Отсутствие нескольких поколений в конечном итоге делает предыдущие анализы расшифровки бесполезными [2, 3].

Процесс шифрования

На рис. 1 показано сообщение MANET от Джека к Джилл, маршрутизируемое в два разных момента времени через безопасные и потенциально вредоносные узлы. Настоящая одноранговая сеть допускает маршрутизацию в присутствии ненадежных одноранговых узлов. В этом случае трафик сообщений находится между Джеком и Джилл. Узлы A, B и C являются надежными узлами в момент времени t_1, а узлы α и β являются потенциально вредоносными узлами. В момент времени t_2 ситуация обратная.

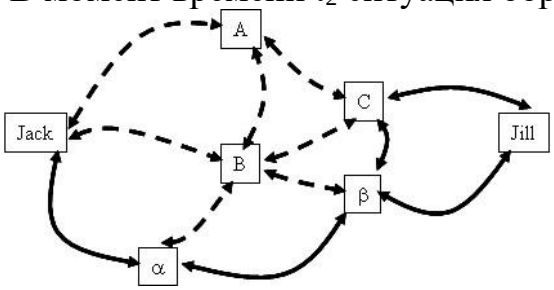

Рис. 1. Маршрутизация MANET через защищенные узлы в момент времени 1 (—) и безопасные узлы в момент времени t2 (---)

Процесс шифрования включает в себя следующие этапы.

- Два или более пользователей определяют словарь открытого текста и словарь на основе ДНК. Пользователи определяют метод, с помощью которого открытый текст представлен четырьмя основаниями ДНК. Словарь ДНК является источником сообщений и ключей шифрования (хромосом).
- Сообщения предварительно кодируются из открытого текста в ДНК с использованием системы линейных уравнений, связывающих позицию слова в сообщении и порядковую позицию в словаре.
- Хромосомы шифруют множественные перестановки сообщения
- Перестановки проверяются на пригодность, и наиболее подходящая перестановка выбирается для передачи источником.
- Получатель расшифровывает сообщение теми же хромосомами
- Геном расширяется за счет мутации хромосом друг с другом или с информационными последовательностями.

Система основана на операциях над словами, а не над отдельными символами. Единственными отдельными символами, которые зашифрованы, являются односимвольные слова.

Пользователи инструмента шифрования ДНК наделены начальным геномом, который представляет собой эквивалент небольшого словаря для инициирования сообщений, предполагаемого получателя, способного владеть секретным общим ключом и секретной последовательностью шифрования/дешифрования для инициирования связи. Хромосомы «длиннее» по сравнению с последовательностями сообщений.

Пусть D представляет словарь (лексикографически упорядоченный набор) всех слов, таких что D_0 представляет первое слово в словаре, а отправитель и получатель составляют сообщения W_i слов (генов). Функция U преобразует слова в последовательности оснований ДНК B_q, как показано ниже:

$$D_{i-1} < D_i < D_{i+1} \; \forall \; i < n, \; W_i, \subseteq D_n, \; D_i = U(W_i, B_q)$$

Существует однозначное соответствие между словарем открытого текста и словарем ДНК, построенным из B_q={A, T, C, G} и бинарным кодированием оснований показанным в таблице 1. Обратите внимание, что A и T, C и G являются инвертируемыми.

Таблица 1

Кодирование оснований ДНК

Основание	**Двоичное значение**	**Основание**	**Двоичное значение**
Аденин	0011	Тимин	1100
Цитозин	1001	Гуанин	0110

При заданном алфавите из n символов, слов длиной m символов, каждое слово открытого текста кодируется в слово ДНК (ген) длиной x пар оснований, создавая ci возможных комбинаций слов ДНК для каждого слова открытого текста и общее количество комбинаций слов ДНК Y для словаря как показано ниже.

$$\log_2 n = x,\ c_i = 2^{x*м},\ Y = \Sigma c_i\ ,\ i=1,\ldots,i_{max}$$

Для n=8 с набором символов, состоящим из {a, e, i, o, u, n, s, t}, и m=3, всего будет 584 записи. Выбранные статьи из такого словаря показаны в таблице 2. Последовательности бессмысленных слов могут быть вставлены между словами открытого текста. По мере увеличения набора символов и длины символов количество возможных слов (в основном бессмысленных слов) увеличивается экспоненциально. Фактические слова могут быть дополнены вкраплениями бессмысленных слов для повышения безопасности.

Таблица 2: Примеры записей словаря ДНК.

Порядковый номер	**Слово**	**Код ДНК**
146	i	TTT
147	ia	TTAKAT
148	san	TTATAT

Выводы

Представлен метод шифрования, основанный на принципах построения ДНК, который обладает высокой устойчивостью к криптографическим анализам. Этот метод криптографии предназначен для использования в мобильных одноранговых сетях и не требует использования открытого ключа.

Список источников

1. Catherine Taylor Clelland, Viviana Risca, Carter Bancroft. Hiding messages in DNA microdots // Nature. – 1999-07-01. – Vol. 399. – P. 533—534. – doi:10.1038/21092.

2. L. M. Adleman. Molecular computation of solutions to combinatorial problems // Science. — 1994-11-11. – Vol. 266, iss. 5187. – P. 1021-1024. – ISSN 1095-9203 0036-8075, 1095-9203. – doi:10.1126/science.7973651.

3. Де Кристофаро Э., Фабер С., Цудик Г. Безопасное геномное тестирование с помощью сопоставления частных подстрок, скрывающих размер и положение. Материалы 12-го семинара ACM по вопросам конфиденциальности в электронном обществе. – ноябрь 2013. – Нью-Йорк, , США. стр. 107-118. doi:10.1145/2517840.2517849.

Статья поступила в редакцию 27.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Заревич А.И. - к.т.н., базовой кафедры технического и программного обеспечения вычислительных и информационных систем ФГБОУ ВО «ВГЛТУ».

Полуэктов А.В. - преподаватель базовой кафедры технического и программного обеспечения вычислительных и информационных систем ФГБОУ ВО «ВГЛТУ».

Макаренко Ф.В. - к.ф.-м.н., базовой кафедры технического и программного обеспечения вычислительных и информационных систем ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Заревич А.И. - идея, сбор материала, обработка материала, написание статьи (80%).

Полуэктов А.В. - частичное написание статьи, научное редактирование текста (20%).

Макаренко Ф.В. – подготовка иллюстрирующих материалов и табличных данных (10%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.9

Особенности проектирования микросхем двойного назначения

Владимир Константинович Зольников [1]✉, Юрий Акимович Чевычелов [2], Матвей Сергеевич Маслов [3], Артем Петрович Лапшин [4], Максим Эдуардович Харченко [5]
[1,2,3,4,5] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия
[1]wkz@rambler.ru✉, https://orcid.org/0000-0003-3409-0342
[2] yua.ch@yandex.ru, https://orcid.org/0000-0003-3409-0331
[3] maslov.matvei@gmail.com, https://orcid.org/0000-0003-3408-0315
[4]Lap.04@mail.ru, https://orcid.org/0000-0003-3409-0442
[5] maks@gmail.com, https://orcid.org/0000-0003-3409-0344

Аннотация. В статье рассматривается особенности проектирования микросхем двойного назначения. Двойное назначение заключается в возможности использовать микросхемы при воздействии механических нагрузок, температуры и радиации. Указывается библиотека с учетом норм технологического процесса предприятия.

Ключевые слова: САПР, микросхема, модули, процедуры.

В настоящее время цифровая обработка сигналов (ЦОС) применяется в цифровой фильтрации, кодировании речи, обработке изображений и т.п. Отличительными чертами ее являются большой объем вычислений, работа в реальном масштабе времени, гибкость настройки и т.п. Поэтому целый ряд фирм проводит работы по разработке ядер ЦОС на основе которых в короткие сроки и с максимальной эффективностью создаются сигнальные процессоры для самых различных применений. Несмотря на всю привлекательность использования таких СБИС, их применение ограничивается чувствительностью к внешним воздействующим факторам (ВВФ): температуре, радиации и т.п. Особенно чувствительны они к совместному воздействию температуры и радиации, которые характерны для космического пространства. Поэтому в настоящее время стоит задача создать комплект функционально полного комплекта СБИС, который обладал повышенной стойкостью к ВВФ. Для этого, прежде всего, необходимо создать средства проектирования таких СБИС на основе существующих САПР.

Чтобы решить задачу проектирования СБИС для ЦОС приходится использовать САПР сквозного проектирования зарубежных фирм, таких как Cadence Design System, Synopsys, Avante!, Mentor Graphics и др. Из представленных систем в НИИЭТ внедрена система, представляющая собой совокупность аппаратных и программных средств с пакетом программ сквозного проектирования фирмы Cadence Design System.

Такой выбор обусловлен тем, что САПР Cadence наиболее полно поддерживает концепцию дублирования и открытости. Дублирование заключается в использовании IP – блоков (Intellectual Property), которые являются примитивами элементов и могут быть многократно использованы для многократного повторения в новых разработках. Открытость системы предполагает широкие возможности интеграции в нее программных модулей собственных разработок или программных пакетов САПР третьих фирм.

Особенностью проектирования СБИС двойного назначения на основе ядра ЦПОС является использование элементов, учитывающих реакцию ИС на ионизирующее воздействие, температуру, включая их совместное действие, и влияние электрического режима. С этой целью в САПР включены дополнительные модули и создана библиотека стандартных элементов, учитывающих реакцию ИС на ионизирующее воздействие (ИИ), температурное поле кристалла и электрический режим эксплуатации ИС. Дополнительные модули, разработанные в НИИЭТ рассчитывают поглощенную дозу радиации, повышение температуры, вызванной этой дозой и развивающиеся термомеханические эффекты. Кроме того, они способны оценить эквивалентность воздействия различных видов радиации, учесть спектрально-энергетические и амплитудно-временные характеристики.

Библиотека базовых логических элементов спроектирована в соответствие с Правилами проектирования для технологического процесса Топология ядра реализована на основе разработанной библиотеки с использованием двухуровневой металлической разводки. В состав библиотеки входят такие элементы как логические ячейки, мультиплексоры, различные модификации защелок, триггеры, ключи, буферы. Библиотека ориентирована на использование программного продукта GDT. Особенности учета радиационного воздействия заключаются в добавлении в стандартные элементы генераторов токов и паразитных биполярных транзисторов. Учет нелинейности процессов отклика реакции элементов ИС на радиационное воздействие заключается в использовании дополнительных паразитных конденсаторах и резисторах. Для определения влияния радиационного воздействия были созданы тестовые структуры, экспериментальные исследования которых позволили определить зависимость электрических и электрофизических параметров от ВВФ.

В описании библиотеки для каждого библиотечного элемента приводится: название элемента, электрическая схема, условное графическое обозначение, таблица емкостей входов и выходов, таблица времен задержек переключения из низкого уровня в высокий и из высокого в низкий с учетом емкости нагрузки. В качестве единичной нагрузки выбрана входная емкость логического элемента «инвертор». Следует отметить, что деградация элементов от дозы радиации учитывается изменением нагрузочной способности, которая в целом имеет экспоненциальную зависимость от дозы ИИ.

Список источников

1. Макаренко Ф.В. Реализация оптимального построения комбинационного устройства и оценка надежности по выходному напряжению /

Макаренко Ф.В., Ягодкин А.С., Зольников К.В., Денисова О.А. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 130-139.

2. Козюков А.Е. Общие подходы оценки стойкости к воздействию ионизирующего излучения космического пространства для зарубежной электронной компонентной базы предприятий –разработчиков / Козюков А.Е., Гамзатов Н.Г., Гречаный С.В., Зольников К.В., Струков И.И., Ачкасов А.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 58-66.

3. Козюков А.Е. Повышение стойкости электронной компонентной базы к дозовым эффектам радиационного воздействия / Козюков А.Е., Зольников К.В., Мещеряков С.Г., Грошев А.С., Сысоев Д.В. // Моделирование систем и процессов. 2021. Т. 14. № 1. С. 16-22.

4. Макаренко Ф.В. Обзор логических базисов и микросхем при построении комбинационного устройства с учётом надёжности / Макаренко Ф.В., Ягодкин А.С., Зольников К.В., Денисова О.А., Полуэктов А.В. // Моделирование систем и процессов. 2022. Т. 15. № 1. С. 115-124.

5. Победа С.А. Создание поведенческой модели LDMOS транзистора на основе искусственной MLP нейросети и ее описание на языке VERILOG-A / Победа С.А., Черных М.И., Макаренко Ф.В., Зольников К.В. // Моделирование систем и процессов. 2021. Т. 14. № 2. С. 28-34.

Статья поступила в редакцию 23.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Зольников В.К. - д.т.н., профессор «Базовая кафедра технического и программного обеспечения вычислительных и информационных систем» ФГБОУ ВО «ВГЛТУ».

Чевычелов Ю.А. - д.т.н., профессор кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Маслов М.С. - преподаватель СПО кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Лапшин А.П. - аспирант ФГБОУ ВО «ВГЛТУ».

Харченко М.Э. - аспирант ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Зольников В.К. - идея, сбор материала, обработка материала, научное редактирование текста.

Чевычелов Ю.А. - частичное написание статьи (25%).

Маслов М.С. - частичное написание статьи (25%).

Лапшин А.П, - частичное написание статьи (25%).

Харченко М.Э. - частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.53

Актуальные проблемы в обеспечении безопасности КИИ в органах государственной власти

Анастасия Леонидовна Зрелова ✉
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия
nastyzr@gmail.com✉

Аннотация. Статья посвящена проблеме защиты объектов критической информационной инфраструктуры в Российской Федерации, в частности произошедшим за последний год киберпреступлениям, совершенным по отношению к федеральным органам исполнительной власти. Проведен анализ наиболее распространённой модели атак, определены причины увеличения количества кибератак на государственные органы Российской Федерации. Определена основная цель проводимых атак: выведение из строя и создание условий недоступности публичных ресурсов госорганов, значимых для населения. Определены самые распространенные виды атак (DDoS-атаки, атаки с помощью вирусов, программ-вымогателей и атаки типа «дефейс», т.е. подмена важной веб-страницы на другую информацию). Рассмотрены различные системы безопасности для объектов КИИ и покрываемые ими требования мер защиты, установленные приказами ФСТЭК России.

Ключевые слова: кибератаки, объекты критической информационной инфраструктуры, федеральные органы исполнительной власти РФ, модель атаки.

Последние три года происходит увеличение частоты кибератак на различные объекты Российской Федерации. По отчетам аналитических центров в первом полугодии 2022 года количество кибератак на объекты критической инфраструктуры увеличилось на 150%. Под атаку киберпреступников попали как коммерческие организации, так и госструктуры России. В их число вошли Министерство культуры РФ, ФНС, ГРЧЦ. По исследованию Центра подготовки руководителей и команд цифровой трансформации РАНХиГС, почти половина (46,6%) госструктур столкнулась с атаками хакеров. По оценкам других экспертов, атакам подверглись около 90% госструктур, но достигнуть цели смогли лишь 10% атак.

Центр противодействия кибератакам Solar Jsoc приписывает атакам самый продвинутый 5-й уровень в модели уровней злоумышленников Solar JSOC, в которых злоумышленниками являются кибернаемники, преследующие интересы иностранного государства [1].

Наиболее опасными можно считать атаки на критически важные ключевые сферы жизнедеятельности государства и общества, т.е. на субъекты критической информационной инфраструктуры. Сбой в работе данных субъектов может

повлиять на здоровье, безопасность и благосостояние граждан России, а также на обеспечение нормальной работы и развитие государства.

Согласно с.2 ФЗ №178 «О безопасности критической информационной инфраструктуры Российской Федерации» субъектами критической информационной инфраструктуры являются – «государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей» [2].

Основной целью проводимых атак стала компрометация ИТ-инфраструктуры и кража конфиденциальной информации, в том числе документации из закрытых сегментов и почтовой переписки ключевых сотрудников ФОИВ, выведение из строя и недоступность публичных ресурсов госорганов, значимых для населения.

Самыми распространенными были DDoS-атаки, атаки с помощью вирусов и программ-вымогателей, которые проникали в систему через почту организации или вредоносные сайты, а также использовались фишинговые атаки, атаки на корпоративную сеть и взлом паролей, утечка данных и несанкционированный доступ, проводились атаки типа дефейс, т.е. киберпреступниками производилась подмена важной веб-страницы на другую информацию.

Среди причин увеличения количества атак можно выделить следующие:

- всплеск хакерской активности из-за геополитической ситуации в мире;
- ослабление контроля за информационными активами в период пандемии COVID-19;
- уход иностранных вендоров, приведший к потере функциональности ряда сервисов и отсутствию обновлений, устраняющих уязвимости.

Можно отметить и изменение качественного уровня кибератак. Киберпреступники стали использовать новый инструментарий (часть разработанного вредоносного ПО ранее не встречалось). Повышается уровень скрытности злоумышленников за счет использования недетекрируемого вредоносного ПО, легитимных программ и проведения анализа средств защиты информации в органах власти.

Невозможно детектировать данные атаки стандартными средствами из-за разработок новых ВПО, ориентированных на деятельность государственного органа, исследований сторонних организаций (подрядчиков) и применения российских внешних ресурсов.

При анализе атак, производимых в 2021-2022 году, можно выделить некоторые технические особенности.

На стадии подготовки к атакам на органы государственной власти проводилось изучение особенностей административной работы с антивирусами. Данный этап позволял злоумышленникам незаметно производить отключение антивирусного ПО во время совершения атаки, также изучение работы антивируса позволяло использовать данное ПО для сбора дополнительной информации об атакуемой инфраструктуре.

После попадания в локальную сесть компании злоумышленники производили полную компрометацию инфраструктуры. Для этого использовались различные тактики, а именно использование:

- различных встроенных программ (Powershell, Windows Command Shell, Планировщик задач);
- валидных учетных записей;
- технологии подписки на события WMI;
- тактик для предотвращения обнаружения;
- уязвимостей (например, Zerologon (CVE-2020-1472);
- различных удаленных серверов;
- сбор данных.

После полной компрометации инфраструктуры злоумышленники производили сбор конфиденциальной информации со всех источников.

Для кибератак злоумышленники использовали различные вредоносные ПО. Чаще всего использовалась программа-загрузчик, обращающаяся к Облаку Mail.ru, ассоциированному с вшитой учетной записью. ПО реализовано в виде DLL-библиотеки, которая связана с OpenSSL и libcur.

При запуске данное ПО начинало анализ системы и искало приложения DISK-O производства Mail.ru Group. При обнаружении данного приложения формировалась идентификационная строка CloudDiskWIndows %InstallVer% %installationID%, специфичная для легитимного DISK-O. Разработчики данного вредоносного ПО подстраивали фазы активности программы под часовую зону атакуемой организации, т.е. программа только с 9 до 16:00 по местному времени. В данный промежуток времени ПО отправляло Heartbeat и запрашивало test/test.dat с интервалом в 27 минут.

Использовалось также похожее вредоносное ПО, осуществляющее взаимодействие с сервером управления через облако Яндекс.Диск.

Выгружались данные компаний через облачные хранилища «Яндекс» и Mail.ru Group, а свою активность вредоносное ПО маскировало под легитимные утилиты Яндекс.Диск и Disk-O.

В связи с увеличением и усложнением кибератак с 30 марта 2022 года Указ Президента Российской Федерации от 30.03.2022 года № 166 «О мерах по обеспечению технологического независимости и безопасности критической информационной инфраструктуры Российской Федерации» (далее — Указ № 166) изменил требования значимым объектам критической информационной инфраструктуры. Указ № 166 изменил структуру требований и подходов к обеспечению защиты значимых объектов КИИ [3].

Одними из главных изменений стали: запрет на покупку иностранных программ и программно-аппаратных комплексов для использования на значимых объектах КИИ; согласование требований к ПО и правил закупок иностранного ПО; до 1 января 2025 года все значимые объекты КИИ должны перейти на российской программное обеспечение и программно-аппаратные комплексы.

Для защиты объектов КИИ были разработаны требования по обеспечению безопасности этих объектов. Данные требования установлены приказом ФСТЭК России от 25.12.2017 № 239 (далее — требования ФСТЭК).

Выполнение требований ФСТЭК можно разделить на 5 этапов:

1. Определение принадлежности организации к субъектам КИИ.
2. Разработка мероприятий по взаимодействию с ФСБ России.
3. Категорирование объектов КИИ.
4. Создание системы безопасности значимых объектов КИИ.
5. Обеспечение безопасности значимого объекта КИИ в ходе его эксплуатации.
6. Обеспечение безопасности значимого объекта КИИ при выводе его из эксплуатации.

В настоящее время существуют различные средства, обеспечивающие безопасность объектов КИИ. Все средства можно разделить на несколько категорий:

- средства защиты информации от несанкционированного доступа (например, vGate);
- межсетевые экраны (например, АПКШ "Континент");
- средства обнаружения вторжений (например, Secret Net Studio);
- средства антивирусной защиты (PT MultiScanner);
- средства контроля защищенности (MaxPatrol 8);
- средства выявления инцидентов (ViPNet TIAS);
- средства защиты каналов передачи данных (ViPNet Client).

Создаются программно-аппаратные комплексы для реализации основных функций безопасности значимых объектов КИИ, например PT Platform 187, UserGate и АПКШ "Континент". Данные комплексы содержат несколько средств защиты информации и предоставляют централизованное управление всеми средствами защиты.

Таким образом, для обеспечения безопасности объекта КИИ необходимо соблюдение требований ФСТЭК, применение программно-аппаратных комплексов и постоянный мониторинг уязвимостей и мониторинг киберугроз.

Список источников

1. Отчет об исследовании серии кибератак на органы государственной власти РФ. — URL: https://rt-solar.ru/upload/iblock/53e/Otchet-Solar-JSOC-ob-issledovanii-serii-kiberatak-na-organy-gosudarstvennoy-vlasti-RF-_-web.pdf.

2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ (последняя редакция).

3. Указ Президента Российской Федерации от 30.03.2022 года № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

4. Приказ ФСТЭК «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 № 239.

Статья поступила в редакцию 23.04.2023; принята к публикации 10.05.2023.

Информация об авторе

Зрелова А.Л. – магистрант кафедры «Защищенные системы связи» Института магистратуры, направления подготовки 11.04.02 –Инфокоммуникационные технологии и системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

Научная статья
УДК 004.056.55

Исследование крупномасштабных ИТ-систем

Алексей Сергеевич Катруш[1]✉, Екатерина Олеговна Карамышева [2]✉, Павел Игоревич Карасев [3]✉, Мустафа Абдулкадим Ал-Амееди[4]✉
[1,2,3]МИРЭА - Российский технологический университет, Москва, Россия
[4]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]katrush.a.s@edu.mirea.ru✉, https://orcid.org/0009-0005-9813-3294
[2]karamysheva@mirea.ru✉, https://orcid.org/0009-0003-0891-3787
[3]karasev@mirea.ru✉, https://orcid.org/0009-0009-3628-6980
[4]fit_tstu@mail.ru✉, https://orcid.org/0009-0002-1066-6650

Аннотация. Крупномасштабные IT системы обычно характеризуются огромным объемом данных, большим количеством одновременно работающих пользователей, требованиями к масштабируемости и требованиям к пропускной способности, такими как задержка и т. д.

Ключевые слова: большие системы, крупномастабные системы, построение систем.

На этапе проектирования очень важно представлять, какие интеграции с платформой будут реализованы в будущем. Еще один важный аспект архитектуры системы касается требований безопасности и соответствия платформы. Данные решения, необходимо принимать с самого начала проектов, чтобы не повлиять на процессы разработки в будущем.

Сегодняшние крупномасштабные ИТ-системы опираются на шаткое основание специальных, оппортунистических методов и технологий. Есть по крайней мере три конкретных проявления этих недостатков. Во-первых, высокий уровень неудач при разработке крупномасштабных ИТ-систем. Многие системы не развернуты и не используются из-за невозможности заставить их работать, так как первоначальный набор требований не может быть выполнен. Вторым проявлением этих недостатков является преобладание операционных сбоев, с которыми сталкиваются крупномасштабные системы в результате уязвимостей в системе безопасности или, что чаще, программных или операционных ошибок. Третьим признаком этих недостатков является недостаточная масштабируемость систем; то есть, их параметры производительности не могут быть расширены для поддержания адекватного отклика по мере увеличения числа пользователей. Эта проблема становится особенно очевидной в настоящее время. Без должного внимания эти проблемы будут только усугубляться по мере более широкого развертывания крупномасштабных ИТ-систем [1].

Проблема крупномасштабных систем

Крупномасштабные системы состоят из сотен или тысяч компьютеров и миллионов строк кода, и почти непрерывно выполняют поставленные задачи. Они все чаще охватывают несколько отделов внутри организаций (общекорпоративные) или несколько организаций (межкорпоративные), или соединяют предприятия с населением в целом. Многие из этих систем и приложений стали известны как «критическая инфраструктура», что означает, что они являются неотъемлемой частью самого функционирования общества и его организаций и что их отказ будет иметь широкомасштабные и немедленные последствия. Критический характер этих приложений вызывает обеспокоенность по поводу рисков и последствий системных сбоев и требует лучшего понимания природы систем и их взаимозависимостей [2].

ИТ-системы, используемые в критически важных внутриорганизационных и межорганизационных приложениях, имеют несколько общих характеристик. Во-первых, все они большие, распределенные, сложные и подвержены высоким и разнообразным уровням использования. Во-вторых, они выполняют критически важные функции, предъявляющие исключительные требования к достоверности и надежности, такие как необходимость работы с минимальными простоями или повреждением информации и/или необходимость продолжать функционировать даже во время обслуживания. В-третьих, системы зависят от автоматизации на основе ИТ для расширения, мониторинга, эксплуатации, обслуживания и других вспомогательных действий.

Все эти три характеристики порождают проблемы при построении и эксплуатации крупномасштабных ИТ-систем. Например, приложения, работающие в распределенных системах, гораздо сложнее разработать, чем соответствующие приложения, работающие в более централизованных системах.

Методы, для решения проблем, связанных с построением крупномасштабных ИТ-систем.

Для построения крупномасштабных ИТ-систем следует использовать набор инструментов, известных как абстракция, модульность и многоуровневость, чтобы помочь им справиться со сложностью проектирования систем. Ограничения этих подходов проверяются крупномасштабными системами различными способами:

Абстракция — это процесс упрощения описания элемента системы, чтобы скрыть ненужные детали и позволить больше сосредоточиться на атрибутах, важных для системного анализа или проектирования. Хитрость заключается в том, чтобы выбрать подходящую абстракцию, которая сохраняет необходимые атрибуты элемента, не становясь при этом нереалистичной. Используя абстракцию, например, можно сформировать упрощенную абстрактную модель пакетного маршрутизатора и на самом деле доказать взаимосвязь таких маршрутизаторов. Однако, когда алгоритм или система настраиваются для повышения производительности, они обычно отходят от своей простой абстрактной формы, отказываясь от многих преимуществ рассуждений об абстракции.

Модульность относится к декомпозиции системы на более мелкие подсистемы, которые можно разрабатывать отдельно (и параллельно). Модули инкапсулируют внутренние детали компонента системы и определяют набор интерфейсов для обеспечения взаимодействия между компонентами. Таким образом, изменения во внутренней конфигурации одного модуля не обязательно требуют изменений в других модулях. Снижая сложность межсистемных зависимостей, модульность способствует более быстрой реконфигурации систем в соответствии с эксплуатационными требованиями. Однако по мере роста масштабов и сложности ИТ-систем становится все труднее четко разделить функциональность, а набор интерфейсов может усложниться, что увеличивает вероятность ошибок при реализации или вероятность того, что конкретные обстоятельства не будут учтены в достаточной мере [3].

Таким образом, вышеперечисленные методы помогут избежать проблем при проектировании и эксплуатации крупномасштабных ИТ-систем.

Список источников

1. Проблема построения крупномасштабных ИТ-систем. https://oracle-patches.com/is/razrabotka-informacionnyh-sistem-faktor-masshtabiruemosti (дата обращения 07.04.2023)

2. А. А. Каменщиков, А. Я. Олейников, Т. Д. Широбокова, “Исследование особенностей проблемы интероперабельности в крупномасштабных информационных системах”, ИТиВС, 2018, № 3, 16–28

3. Модульность. https://studopedia.org/14-75719.html (дата обращения 10.04.2023)

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Катруш А.С. – аспирант кафедры КБ-1 «Защита информации», направления подготовки «09.06.01 – Информатика и вычислительная техника».

Карамышева Е.О. – старший преподаватель кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Карасев П.И. – к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Мустафа Абдулкадим Ал-Амееди – аспирант «ТГТУ».

Вклад авторов

Катруш А.С. – идея, сбор материала, обработка материала (30%).

Карамышева Е.О. – написание статьи, научное редактирование текста (30%).

Карасев П.И. – написание статьи, научное редактирование текста (20%).

Мустафа Абдулкадим Ал-Амееди – частичное написание статьи (20%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.55

Принцип нагрузочного тестирования больших систем

Алексей Сергеевич Катруш [1] ✉, Екатерина Олеговна Карамышева [2] ✉, Павел Игоревич Карасев [3] ✉, Алмали Ахмед Аднан Латиф[4] ✉
[1,2,3]МИРЭА - Российский технологический университет, Москва, Россия
[4]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]katrush.a.s@edu.mirea.ru ✉
[2]karamysheva@mirea.ru ✉
[3]karasev@mirea.ru ✉, https://orcid.org/0009-0009-3628-6980
[4]fit_tstu@mail.ru ✉, https://orcid.org/0009-0007-4529-9674

Аннотация. Большие системы, начиная от электронной коммерции и заканчивая телекоммуникационной инфраструктурой должны поддерживать одновременный доступ для тысяч или даже миллионов пользователей. Отказ от масштабирования может привести к катастрофическим последствиям и проблемам, а также к неблагоприятному освещению в СМИ. К обеспечению качеств этих систем, нагрузочное тестирование является обязательной процедурой тестирования в дополнение к обычному функциональному тестированию.

Ключевые слова: большая система, нагрузочное тестирование, стресс тестирование.

Большая система - термин, используемый в таких областях, как информатика, разработка программного обеспечения и системная инженерия, для обозначения систем с беспрецедентным количеством строк исходного кода, количества пользователей и объемов данных. Масштаб таких систем порождает множество проблем: они будут разрабатываться и использоваться многими заинтересованными сторонами в различных организациях, часто с противоречивыми целями и потребностями; они будут построены из разнородных частей со сложными зависимостями и возникающими свойствами. Большие системы будут постоянно развиваться, а сбои программного обеспечения и персонала будут нормой, а не исключением [1].

На этапе проектирования очень важно представлять, какие интеграции с платформой будут реализованы в будущем. Еще один важный аспект архитектуры системы касается требований безопасности и соответствия платформы. Данные решения, необходимо принимать с самого начала проектов, чтобы не повлиять на процессы разработки в будущем.

Проблема больших систем

Большие системы состоят из миллионов строк кода, и почти непрерывно выполняют поставленные задачи. Они все чаще охватывают несколько отделов

внутри организаций (общекорпоративные) или несколько организаций (межкорпоративные), или соединяют предприятия с населением в целом. Многие из этих систем и приложений стали известны как «критическая инфраструктура», что означает, что они являются неотъемлемой частью самого функционирования общества и его организаций и что их отказ будет иметь широкомасштабные и немедленные последствия. Критический характер этих приложений вызывает обеспокоенность по поводу рисков и последствий системных сбоев и требует лучшего понимания природы систем и их взаимозависимостей.

Тестирование системы

Тестирование производительности является ключом к пониманию того, как работает система. Без хорошего тестирования производительности невозможно узнать, как система справится с ожидаемыми или неожиданными требованиями.

Нагрузочное тестирование и стресс-тестирование — это два вида тестирования производительности.

Нагрузочное тестирование — это тестирование работы приложения, программного обеспечения или веб-сайта при использовании под ожидаемой нагрузкой. Мы намеренно увеличиваем нагрузку, ищем порог хорошей производительности. Это проверяет, как система работает, когда она сталкивается с нормальным трафиком.

Стресс-тестирование — это проверка того, как система работает в условиях экстремального давления — неожиданной нагрузки. Мы увеличиваем нагрузку до ее верхнего предела, чтобы узнать, как она восстанавливается после возможного сбоя. Это проверяет, как система работает, когда она сталкивается с аномальным трафиком [2].

Знание того, когда использовать нагрузочное и стресс тестирование, зависит от целей, стоящих перед системой:

- Как работает система при заданном количестве запросов
- Что произойдет при неожиданном увеличении трафика

Чтобы убедиться, что большие системы остаются доступными при пиковых нагрузках, необходимо провести тестирование производительности.

Проведение нагрузочного тестирования

Нагрузочное тестирование, в общем, относится к практике оценки поведения системы под нагрузкой. Нагрузка – это скорость входящих запросов к системе.

Рис. 1. Нагрузочное тестирование

Для проведения нагрузочного тестирования, необходимо запустить специализированное программное обеспечение для нагрузочного тестирования на одном или нескольких компьютерах. Это программное обеспечение генерирует и передает большое количество запросов на систему. Затем программное обеспечение для нагрузочного тестирования измеряет время, затраченное системой на ответ на запросы, и подсчитывает количество возникающих ошибок. Отдельные программы мониторинга работают совместно для настройки системы и оценки использования ресурсов.

Типы нагрузочных тестов:

- Проверка емкости. Постепенное увеличение нагрузки на систему, для обнаружения порогового значения, когда система перестает стабильно работать в соответсвтиис требованиями.

- Выдержка теста. Поддержка постоянной пропускной способности системы в течение длительного периода (например, 24 часов), для выявления таких проблем, как утечки памяти.

Таким образом, для обеспечения «стойкости» больших систем проведение нагрузочного тестирования является наиболее важным, так как изначально предполагается большое количество одновременно выполненных запросов к системе.

Список источников

1. Большие системы// https://www.victor-safronov.ru/systems-analysis/glossary/large-scale-system.html (дата обращения: 09.04.2023).

2. Нагрузочное тестирование и стресс-тестирование// https://habr.com/ru/companies/variti/articles/448626/(дата обращения: 11.04.2023).

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Катруш А.С. – аспирант кафедры КБ-1 «Защита информации», направления подготовки «09.06.01 – Информатика и вычислительная техника».

Карамышева Е.О. – старший преподаватель кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Карасев П.И. – к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Алмали Ахмед Аднан Латиф – аспирант «ТГТУ».

Вклад авторов

Катруш А.С. – идея, сбор материала, обработка материала (30%).

Карамышева Е.О. – написание статьи, научное редактирование текста (30%).

Карасев П.И. – написание статьи, научное редактирование текста (20%).

Алмали Ахмед Аднан Латиф – частичное написание статьи (20%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

О вопросах обеспечения безопасности систем искусственного интеллекта

Анна Витальевна Качуро[1]✉, Дмитрий Андреевич Лысов[2], Алексей Петрович Горлов[3]
[1,2,3] Брянский государственный технический университет, Брянск, Россия
[1]hatelin@mail.ru✉, https://orcid.org/0009-0004-6022-1144
[2]lysovdmitriia@gmail.com✉, https://orcid.org/0009-0003-9666-7191
[3]apgorlov@gmail.com, https://orcid.org/0009-0003-3100-3466

Аннотация. В статье рассмотрена проблема безопасности систем искусственного интеллекта (ИИ). Рассмотрены актуальные задачи безопасности, стоящие перед проектированием систем ИИ, и методы защиты, которые могут быть использованы для предотвращения кибератак на эти системы.

Ключевые слова: безопасность, системы ИИ, кибератаки.

Искусственный интеллект (ИИ) – это область компьютерных наук, которая занимается разработкой алгоритмов и систем, которые способны выполнять задачи, которые обычно требуют интеллектуальных способностей человека. Это может включать в себя способность к самообучению, пониманию естественного языка, распознаванию образов, принятию решений и многим другим.

ИИ на сегодняшний день можно разделить на две основные категории: слабый ИИ (узконаправленный) и сильный ИИ (общий). Слабый ИИ – это системы, способные выполнять ограниченный набор задач в пределах определенной области. Примерами слабого ИИ могут служить голосовые помощники, системы автоматического перевода и автоматического распознавания речи, системы фильтрации спама и т.д. Сильный ИИ (общий ИИ) – это системы, которые могут решать широкий спектр задач, которые требуют интеллектуальных способностей человека. Сильный ИИ еще не достигнут, и на сегодняшний день исследования в этой области продолжаются.

Существует несколько методов разработки ИИ, включая правила и знания, статистические методы и машинное обучение. Правила и знания основаны на задании системе набора правил, которые она использует для принятия решений. Статистические методы и машинное обучение – это методы обучения ИИ путем анализа больших наборов данных, ради нахождения закономерностей и общих тенденций.

ИИ используется во многих областях, включая медицину, финансы, производство, транспорт и многие другие. Он может быть использован для улучшения производительности, повышения безопасности и создания новых продуктов и услуг. Однако, с развитием ИИ также возникают вопросы

безопасности, этики и приватности, которые нужно учитывать в процессе разработки и применения ИИ.

При проектировании систем искусственного интеллекта, для обеспечения безопасности, необходимо учитывать, ряд задач:

1. Защита данных и конфиденциальности. ИИ системы используют большие объемы данных, которые часто содержат личную информацию пользователей. Поэтому важно обеспечить защиту этих данных и конфиденциальность пользователей. Это может включать использование средств шифрования, методов обработки данных, которые сохраняют анонимность пользователей и защиту от несанкционированного доступа.

2. Безопасность и защита от кибератак. Системы ИИ могут стать мишенью кибератак, которые могут нарушить работу системы, получить доступ к конфиденциальной информации или использовать систему для злонамеренных целей. При проектировании системы ИИ необходимо учитывать возможность таких атак и разрабатывать меры безопасности для защиты системы.

3. Надежность системы. ИИ системы могут быть сложными и нестабильными, что может привести к непредвиденным последствиям. Поэтому при проектировании системы ИИ необходимо учитывать возможность ошибок и разрабатывать методы для их обнаружения и устранения.

4. Разработка эффективных систем контроля. Использование ИИ системы может привести к уменьшению контроля и участия человека в принятии решений. Поэтому необходимо разработать эффективные системы контроля, которые позволят людям принимать решения в случае необходимости и предотвратят возможные ошибки.

5. Соответствие правовым и этическим нормам. Использование ИИ системы должно соответствовать правовым и этическим нормам, чтобы избежать нежелательных последствий и негативного влияния на общество.

Защита систем искусственного интеллекта является одной из самых важных задач в области информационной безопасности. Системы ИИ могут быть уязвимы к кибератакам, которые могут нарушить их работу, украсть данные или повредить модели машинного обучения. Рассмотрим несколько методов защиты систем ИИ:

1. Защита сети. Системы ИИ могут быть подвержены атакам из интернета, поэтому важно обеспечить защиту сети, в которой функционирует система ИИ. Это может включать использование сетевых фильтров, брандмауэров и других инструментов для обнаружения и предотвращения кибератак.

2. Использование шифрования. Шифрование данных может помочь защитить систему ИИ от кибератак. Это может включать использование алгоритмов шифрования для защиты данных, хранящихся на серверах системы ИИ, а также зашифрованных соединений между системой ИИ и другими устройствами.

3. Аутентификация и идентификация. Аутентификация и идентификация могут помочь защитить систему ИИ от несанкционированного доступа. Это может включать использование паролей, сетевых ключей и других методов

аутентификации, а также определение уровней доступа к различным функциям системы ИИ.

4. Мониторинг и обнаружение атак. Может включать использование системы мониторинга, которая анализирует журналы системы, обнаруживает необычное поведение и отправляет предупреждения в случае возможной атаки.

5. Обучение пользователей. Обучение пользователей может помочь предотвратить кибератаки на систему ИИ. Пользователи системы ИИ должны быть обучены правилам безопасности, включая использование надёжных паролей, неоткрытие вредоносных файлов и другие методы защиты.

6. Резервное копирование данных. Резервное копирование данных может помочь защитить систему ИИ от кибератак, которые могут повредить или удалить данные. Резервные копии данных должны регулярно создаваться и храниться в надежных местах, чтобы в случае кибератаки можно было быстро восстановить данные системы ИИ.

7. Использование искусственного интеллекта для защиты от кибератак. Использование искусственного интеллекта для защиты от кибератак может помочь обнаружить и предотвратить кибератаки на систему ИИ. Это может включать использование ИИ для анализа трафика сети, обнаружения необычного поведения и быстрого реагирования на возможные атаки.

8. Регулярное обновление и патчи. Регулярное обновление и установка патчей для системы ИИ и ее компонентов может помочь защитить систему от уязвимостей, которые могут быть использованы злоумышленниками для атаки. Обновление и установка патчей также могут помочь обеспечить соответствие системы ИИ современным стандартам безопасности.

9. Соответствие стандартам безопасности. При проектировании и разработке системы ИИ необходимо учитывать существующие стандарты безопасности и следовать им. Некоторые стандарты, такие как GDPR (Общий регламент по защите данных), могут иметь прямое отношение к системам ИИ и их использованию.

В целом, защита системы ИИ от кибератак требует комплексного подхода, который включает в себя как технические, так и организационные меры. Это поможет обеспечить безопасность системы ИИ и защитить ее от потенциальных угроз безопасности.

Список источников

1. Brundage M., Avin S., Wang J., Belfield H., Krueger G., Hadfield G., Khlaaf H., Yang J., Toner H., Fong R., Maharaj T., Koh P. W., Hooker S., Leung J., Trask A., Bluemke E., Lebensbold J., O'Keefe C., Koren M., Ryffel T., Rubinovitz J.B., Besiroglu T., Carugati F., Clark J., Eckersley P., de Haas S., Johnson M., Laurie B., Ingerman A., Krawczuk I., Askell A., Cammarota R., Lohn A., Krueger D., Stix C., Henderson P., Graham L., Prunkl C., Martin B., Seger E., Zilberman N., Ó hÉigeartaigh S., Kroeger F., Sastry G., Kagan R., Weller A., Tse B., Barnes E., Dafoe A., Scharre P., Herbert-Voss A., Rasser M., Sodhani S., Flynn C., Gilbert T. K., Dyer L., Khan S., Bengio Y., Anderljung M. Towards Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims : OpenAI, Leverhulme Centre for the

Future of Intelligence, University of Montreal. 2020. URL: https://arxiv.org/pdf/2004.07213.pdf.

2. Oseni A., Moustafa N., Janicke H., Liu P., Tari Z., A. Vasilakos. Security and Privacy for Artificial Intelligence:Opportunities and Challenges : The University of New South Wales, RMIT University, The Cyber Security Cooperative Research Centre (CSCRC), The University of Technology Sydney, Australia, Penn State, University Park, USA. 2020. URL : https://arxiv.org/pdf/2102.04661.pdf.

3. Маршалл Э., Рохас Р., Стоукс Д., Бринкман Д. Безопасность искусственного интеллекта и машинного обучения: перспективы в корпорации Майкрософт : 2023. URL : https://learn.microsoft.com/ru-ru/security/engineering/securing-artificial-intelligence-machine-learning.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Качуро А.В. - студент кафедры «Системы информационной безопасности», направления подготовки «10.03.01 – Информационная безопасность» ФГБОУ ВО «БГТУ».

Лысов Д.А. - старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горлов А.П. – к.т.н. доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Качуро А.В. – идея, сбор материала, обработка материала, частичное написание статьи (40%).

Лысов Д.А. – написание статьи, научное редактирование текста (30%).

Горлов А.П. – написание статьи, научное редактирование текста (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Выявление особенностей использования методов искусственного интеллекта в средствах обеспечения информационной безопасности

Карина Владимировна Короткова [1]✉, Дмитрий Андреевич Лысов [2], Алексей Петрович Горлов [3]
[1, 2, 3] Брянский государственный технический университет, Брянск, Россия
[1] marus.korotkova@yandex.ru, https://orcid.org/0009-0007-2396-4469
[2] lysovdmitriia@gmail.com ✉, http://orcid.org/0009-0003-9666-7191
[3] apgorlov@gmail.com, https://orcid.org/0009-0003-3100-3466

Аннотация. В статье рассматриваются особенности применения методов искусственного интеллекта в инструментах обеспечения информационной безопасности. Авторы исследуют применение машинного обучения, нейронных сетей и других алгоритмов искусственного интеллекта для выявления угроз безопасности, обнаружения атак и предотвращения киберпреступлений. Статья анализирует возможности и ограничения применения искусственного интеллекта в информационной безопасности, а также базируется на сравнении эффективности использования искусственного интеллекта с традиционными методами защиты информации.

Ключевые слова: информационная безопасность, искусственный интеллект, средства защиты, машинное обучение, нейронные сети, обработка искусственного языка.

В современном мире информационная безопасность (ИБ) является одной из основных проблем, с которой сталкивается общество. Для примера продукты Kaspersky отражают более 900 млн онлайн-атак в квартал (данные за 3 квартал 2022 года) [1]. В свете растущих угроз киберпреступников, инструменты обеспечения ИБ становятся все более сложными и требуют более эффективных методов защиты.

Для того, чтобы эффективно обнаруживать, предотвращать и обрабатывать кибератаки, а также лучше понимать сложные сценарии атак в ИБ начинают активно внедрять методы искусственного интеллекта.

Искусственный интеллект (ИИ) для ИБ – это комплекс алгоритмов, использующих методы машинного обучения, нейронные сети и обработку естественного языка с целью улучшения кибербезопасности, включающий в себя множество методов, которые позволяют программам обучаться, анализировать информацию, принимать решения и выполнять задачи, которые требуют интеллектуальных способностей. Применение технологий ИИ значительно расширяет возможности компьютерных систем и программных продуктов, позволяет ускорить процессы и оптимизировать работу.

Методы ИИ могут анализировать данные о поведении пользователей и устройств в сети для выявления необычного поведения, которое может свидетельствовать о злонамеренной деятельности. Модели машинного обучения могут научиться распознавать обычные и аномальные сценарии поведения, даже если угроза еще не раскрыта. Однако, важно учитывать, что это новый и сложный подход, который требует соответствующих знаний и ресурсов для правильной настройки и обслуживания системы.

Один из примеров использования технологий ИИ для обнаружения необычного поведения – система мониторинга безопасности Amazon GuardDuty, которая использует машинное обучение и нейронные сети для автоматизированного выявления аномальной активности и угроз в облаках AWS [2]. Система анализирует миллионы запросов каждую секунду, чтобы выявить подозрительную активность, такую как сбор данных пользователей, попытки доступа к недоступным данным или обращения к заблокированным IP-адресам.

Еще одним примером является система Darktrace Enterprise, которая использует машинное обучение для создания модели нормального поведения пользователей, устройств и сетей в организации. Система анализирует данные о поведении пользователей и устройств в реальном времени и выдает уведомления об аномалиях, которые могут свидетельствовать о вредоносной деятельности [3].

Также алгоритмы ИИ используются для мониторинга и анализа больших объемов сетевого трафика в реальном времени. Они могут автоматически обнаруживать атаки и узнавать их характеристики с помощью анализа пакетов данных. Например, McAfee Advanced Threat Defense использует технологию машинного обучения, чтобы анализировать потенциальные индикаторы угроз, связанные с файлами и сетевым трафиком, для определения потенциальных угроз и защиты от ведущих видов рисков безопасности [4].

Алгоритмы машинного обучения могут использоваться для идентификации и классификации вредоносных программ. Антивирусная программа Kaspersky использует алгоритмы машинного обучения для проверки кодов на совпадения с базой данных вредоносных программ и для выявления неизвестных угроз по их поведению [5]. Они также могут использоваться для создания сигнатур вредоносных программ и распознавания неизвестных угроз. Например, Sophos Intercept X использует методы машинного обучения для создания сигнатур вредоносных программ и для обнаружения новых угроз без использования базы данных сигнатур [6]. Решение также использует метод обнаружения поведения вредоносных программ для выявления новых, еще неизвестных угроз.

Также, важно упомянуть о контроле доступа. Контроль доступа является обязательным элементом любой политики ИБ, а использование алгоритмов ИИ может значительно упростить процесс управления доступом. Одним из примеров использования ИИ для контроля доступа в больших компаниях является система автоматического распознавания лиц. В такой системе технологии ИИ используются для анализа видеоизображения с камер наблюдения и сравнения полученных данных с базой данных сотрудников, имеющих доступ к определенным зонам компании.

При прохождении через точки контроля доступа сотрудник должен предъявить свою идентификационную карту или пройти сканирование лица. Если данные не соответствуют информации в базе данных, система может автоматически заблокировать доступ сотрудника или сообщить о возможной угрозе безопасности. Такая система не только обеспечивает высокий уровень безопасности, но и позволяет уменьшить количество ошибок, связанных с человеческим фактором, например, когда охранник может не узнать сотрудника или допустить ошибку при проверке документов. Кроме того, система может автоматически составлять отчеты о движении людей в зоне контроля доступа, что может быть полезно для управления персоналом и оптимизации бизнес-процессов.

Алгоритмы ИИ могут использоваться для обнаружения и защиты конфиденциальных данных внутри организации. В пример можно привести IBM Security Guardium – решение для обнаружения утечек данных и контроля доступа, основанного на полномочиях, в целях предотвращения несанкционированного доступа к конфиденциальным данным внутри организации. IBM Security Guardium использует технологии ИИ, чтобы распознавать важные данные, которые организация должна защищать. Это может включать конфиденциальные данные, которые нельзя раскрыть без согласия сторон, финансовые данные, социальные номера и другие. Далее классифицирует их, исходя из их важности и чувствительности, чтобы определить, как они должны обрабатываться и храниться. Это позволяет организациям более эффективно защищать свои данные и управлять ими.

Многие ИИ-системы предлагают графические интерфейсы для визуализации данных, которые помогают анализировать угрозы и выводить данные в понятном для человека формате. Одним из примеров такой ИИ-системы, является система мониторинга кибербезопасности Splunk. Splunk предлагает графические интерфейсы для визуализации данных, которые помогают анализировать угрозы и выводить данные в понятном для человека формате. Например, система может отображать информацию о том, откуда идут атаки, какие уязвимости используются злоумышленниками и какие данные были скомпрометированы [7]. Такая система помогает компаниям быстро реагировать на угрозы и принимать соответствующие меры для защиты своих систем и данных. Кроме того, благодаря графическим интерфейсам, Splunk может быть использована даже теми специалистами, которые не имеют глубоких знаний в области кибербезопасности.

В целом, использование ИИ в кибербезопасности помогает улучшить защиту от вредоносных программ и атак, автоматизировать процессы обнаружения и анализа угроз, упростить управление правами доступа и существенно улучшить общую безопасность информации.

Однако, применение методов ИИ в ИБ также имеет свои ограничения. Некоторые алгоритмы ИИ могут давать некорректные результаты, что может привести к ошибочной и дорогостоящей реакции на угрозу безопасности. Кроме того, использование ИИ требует мощных вычислительных ресурсов и большой базы данных для обучения.

Сравнение эффективности использования ИИ с традиционными методами защиты информации также является важным аспектом. Использование методов ИИ может быть более эффективным, чем традиционные методы защиты, но оно также может быть дороже и труднее в настройке и обслуживании.

Список источников

1. Официальный сайт «Лаборатории Касперского»: сайт. – URL: https://securelist.com/it-threat-evolution-in-q3-2022-non-mobile-statistics/107963/ (дата обращения: 01.04.2023).

2. Amazon GuardDuty – Intelligent Threat Detection : сайт. – URL: https://aws.amazon.com/ru/guardduty/features/ (дата обращения: 01.04.2023).

3. Citsys - Using technology to Secure, Support & Grow business : сайт. – URL: https://www.citsys.com/darktrace/ (дата обращения: 01.04.2023).

4. McAfee Advanced Threat Defense. Обнаружение сложных вредоносных программ // Меню Antivirus, VPN, Identity & Privacy Protection | McAfee : сайт. – URL: https://www.mcafee.com/ru-ru/index.html (дата обращения: 01.04.2023).

5. Официальный сайт «Лаборатории Касперского» : сайт. – URL: https://www.kaspersky.ru/enterprise-security/wiki-section/products/behavior-based-protection (дата обращения: 11.04.2023).

6. Heritage-offshore : сайт. – URL: https://heritage-offshore.com/net-admin/obzor-zashhity-konechnyh-tochek-sophos-intercept-x/ (дата обращения: 11.04.2023).

7. Хабр : сайт. – URL: https://habr.com/ru/companies/tssolution/articles/323814/ (дата обращения: 11.04.2023).

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Короткова К.В. – студент кафедры «Системы информационной безопасности», направления подготовки «10.03.01 – Информационная безопасность» ФГБОУ ВО «БГТУ».

Лысов Д.А. – ст. преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горлов А.П. – к.т.н. доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Короткова К.В. – идея, сбор материала, обработка материала, частичное написание статьи (40%).

Лысов Д.А. – написание статьи, научное редактирование текста (30%).

Горлов А.П. – написание статьи, научное редактирование текста (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Исследование проблемы современных нейросетевых вирусов

Владимир Викторович Кулешов [1]✉, Павел Игоревич Карасев [2], Юрий Юрьевич Громов [3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]kuleshov.v.v1@edu.mirea.ru✉, http://orcid.org/0009-0006-5650-3450
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3]gromovtambov@yandex.ru, https://orcid.org/ 0000-0003-3313-2731

Аннотация. В статье описаны возможности нейронных сетей в области создания контента как полезного и легального, так и вредоносного, в частности, вирусов. Указаны проблемы и трудности в массовом эксплуатации нейронных сетей, и какие последствия влечёт за собой развитие технологий.

Ключевые слова: нейронная сеть, вирус, антивирус, развитие нейронных сетей, опасность нейронных сетей.

В современном мире технологии стремительно развиваются. В цифровую эпоху появляется всё больше новых изобретений, стремящихся привнести что-то новое или облегчить жизнь человека. Одним из таких являются нейронные сети. Описанные ещё в середине прошлого века, в последние месяцы он обрели поистине широкую популярность. Если ещё в прошлом году нейронные сети в ежедневном обиходе не представлялись возможным, то сейчас каждый человек может использовать их повсеместно – от простого диалога, до написания сложных технических работ.

Сам принцип работы нейронных сетей заключается в приобретении знаний посредством обучения. Точно так же как и человек, нейронная сеть преобразует входную информацию в результат. С каждым новым циклом нейросеть «узнаёт» всё больше новой информации и строит закономерности при вводе. На основании полученных сведений она может спрогнозировать что в дальнейшем будет введено ей на вход, и выдать выход. Это позволяет использовать нейросеть в различных сферах: определение и распознавание объекта, прогноз биржевых котировок, диалог с человеком, создание музыки и картинок.

Кроме очевидных полезных возможностей, нейронные сети также несут и вред. К примеру, переписывание музыки с минимальным искажением позволяет использовать её без авторских прав, поскольку новый контент отличается. Злоупотребление генераций изображений может привести к подделыванию работ авторов в уникальной стилистике. Систему распознавания лиц также можно использовать и как систему с генерацией новых, создавая проблему ненастоящих личностей в интернете. Но это примеры относительно безвредных,

но тем не менее опасных действий нейронных сетей.

Намного опаснее тот факт, что обученная нейросеть без правил может генерировать и копировать абсолютно любую вещь. Подделка голоса, лица, характера человека, всё это вполне может и уже умеет делать нейронная сеть. Отлично обученная на биржевых курсах и их зависимостях, нейросеть может обрушить котировки как отдельных рынков, так и биржи в принципе. Натренированная нейронная сеть способна писать новые вредоносные программы.

Уже сейчас нейронные сети могут писать компьютерные вирусы, причём абсолютно легально. При запросе самому популярному на данный момент чат-боту нейронной сети ChatGPT привести пример полиморфного вируса, он выдаст запрошенное. Может быть такой вирус не будет работать «из коробки», но сама суть вируса будет приведена довольно точно. При должном обучении, нейросеть может модифицировать уже существующие вирусы и создавать новые. Сама суть обучения нейронной сети позволит испытывать ей новые вредоносные программы и сравнивать их со старыми, находя и внедряя сильные, и искореняя слабые стороны.

Эволюция вирусов, которая может произойти из-за нейронной сети, довольно сильно изменит подход к защите информации на персональных компьютерах и в сети. Обычные антивирусы на личных компьютерах могут лишиться сигнатурного анализа, поскольку свойства вирусов будут изменяться с каждым новым сгенерированным нейросетью вирусом. Эвристические алгоритмы же не смогут обеспечить должный уровень безопасности. Мало того, что будут потреблять большие вычислительные объёмы для работы в реальном времени, так ещё и нейронная сеть будет создавать новые вирусы как раз для противодействия существующим эвристическим методам. Антивирусы для противодействия таким угрозам придётся создавать на основе нейронной сети, чтобы не просто находить и удалять вредоносные программы, но и обучаться делать это максимально эффективно.

На самом деле всё не так плохо. Обучение нейронной сети очень трудо- и денежно-затратный процесс. Необходимо создавать корректные датасеты для обучения, а размер и количество таких датасетов должно быть огромным. Нужно подобрать или создать такой алгоритм обучения нейронной сети чтобы тот был предельно производительным. Сами вычислительные мощности, на которых будет обучаться и работать нейронная сеть превосходят многие существующие суперкомпьютеры. Персонал, который будет работать с такой нейросетью обязан быть высоко квалифицирован, высокооплачиваем и высокомотивирован.

Проще говоря, создавать и использовать нейронные сети для чего бы то ни было могут себе позволить только либо мегакорпорации, такие как Google, Microsoft и Amazon, либо государства ведущих стран человечества. Ни у кого больше не хватит столько ресурсов и людей правильно оперировать нейронными сетями.

Научно-технический прогресс, позволивший нам создать и эксплуатировать нейронные сети не стоит на месте. С каждым годом изобретаются и выпускаются всё более мощные вычислительные процессоры,

позволяющие проводить больше операций за меньшее время. Бывшие ранее в экспериментальных лабораториях, нейронные сети становятся и будут становиться всё более доступными обычным людям. Работа, что сейчас представляется возможной реализовать только на суперкомпьютерах, в скором времени может проводиться на домашних компьютерах или мобильных телефонах. Нейронные сети, доступ к которым возможен только через интернет, поскольку оные физически расположены на серверных массивах, уже через пару лет могут быть установлены и использованы на персональных компьютерах. И тогда любой человек сможет обучить и применить нейросеть как посчитает нужным.

Но кроме создания полезных вещей, станет возможным и генерация множества вредного и опасного, как например вирусов. Развивать потребуется не только средства обнаружения вирусов, но и средства противодействия им.

Список источников

1. Гудфеллоу Я., Бенджио И. "Deep Learning" - The MIT Press, 2017. – 652с.
2. Гибсон А., Паттерсон Д. " Deep Learning: A Practitioner's Approach" - O'Reilly Media, 2017. – 530с.
3. Сайт компании OpenAI: https://openai.com/ (дата обращения

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Кулешов В.В. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.03.01 – Информационная безопасность» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Громов Ю.Ю. – д.т.н. профессор, Институт автоматики и информационных технологий «ТГТУ».

Вклад авторов

Кулешов В.В. - идея, сбор материала, обработка материала, оформление текста (30%).

Карасев П.И. – рекомендации по оформлению статьи, научное редактирование текста (20%).

Громов Ю.Ю. – помощь в анализе информации, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.832

Обзор методов использования нейросетевого фишинга

Владимир Викторович Кулешов[1]✉, Павел Игоревич Карасев[2], Хайдар Абдулваххаб Х. Шамсулдин[3], Абд Али Хуссейн Наджми Абд Али[4]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3,4]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]kuleshov.v.v1@edu.mirea.ru✉, http://orcid.org/0009-0006-5650-3450
[2]karasev@mirea.ru, https://orcid.org/ 0009-0006-4255-5874
[3] fit_tstu@mail.ru , https://orcid.org/0009-0007-4529-9674
[4] fit_tstu@mail.ru

Аннотация. Статья обще описывает нейронные сети, их сферу использования. Упор работы сделан на опасности использования нейронных сетей в мошеннических схемах и социальной инженерии.

Ключевые слова: нейронная сеть, мошенничество, фишинг, подделка голоса, опасность нейронных сетей.

В эпоху цифровизации и цифрового общества, человечество стремится изобрести и использовать всё более новые технологии. Когда-то даже телефонный звонок и электронная почта были прорывом в сфере коммуникации, а сейчас даже спутниковой связью никого не удивить. Но даже с таким интенсивным развитием находится чем привлечь и увлечь простого обывателя.

Нейронные сети, само понятие которых появилось ещё в прошлом столетии, резко входят в наш обиход. Буквально во всех сферах жизни человека, от монотонной работы до творческих заданий, от простого «человеческого» общения до научных лекций, повсюду нейронные сети имеют свой потенциал использования. Во многих местах даже уже нейросети участвуют в обучении персонала и оптимизации производства, а картины, созданные программным образом, выигрывают призы на выставках.

Само собой, нейронные сети далеко не совершенны. Качество и работоспособность сети упирается как в аппаратную часть, так и в само обучение алгоритмов. Необходима работа специалистов, чтобы составить оптимальный датасет для обучения нейронной сети, подобрать подходящий алгоритм обучения, произвести множество итераций, и только после этого уже получать какой-либо результат.

Но даже сейчас, нейронные сети может обучать каждый, так как основные языковые модели распространяются в свободном доступе. Плюсы обучения таких «любительских» сетей присутствуют, как например создание готовых датасетов для последующего использования его в более мощных сетях, решение

каких-либо непопулярных задач, на которые у больших корпораций нет времени и интереса решать, обучение специалистов работе с нейронной сетью.

И, конечно же, кроме преимуществ в нейронных сетях есть и угрозы. Создание вирусов, подделка личности человека, незаконное копирование авторских работ, неограниченный доступ к полученной и обработанной информации – всё это уже сейчас начинает распространятся. Вирусы, написанные нейронной сетью шаблонные, легко обнаруживаемые, но их производство поставлено на поток, и чем больше вирусов обнаружено, тем больше обучена нейронная сеть создавать новые. Замена лица и голоса человека на видео спокойно может компрометировать его личность и привести к печальным последствиям от травли в интернете до уголовного преследования. Нейронная сеть, обученная на рисунках определённого автора может генерировать изображения в похожей стилистике, что приведёт к уменьшению уникальности творчества и падению интереса. Информация, взятая из интернета и обработанная ненадлежащим образом может привести в заблуждение человека, получающего информацию от нейронной сети, что тоже может привести к нежелательному исходу.

Существует действительно серьёзная проблема, которая может возникнуть уже в ближайшие годы, а именно – фишинг.

Сам фишинг есть ничто иное как мошенничество, с целью получить доступ к вашим данным, как паспортным, так и кредитным. Практически каждый обладатель электронной почты или мобильного телефона столкнулся со спамом или со звонком из «службы безопасности банка». В России это одно из самых распространённых преступлений, которое, однако, не всегда оказывается раскрытым и наказанным, по разным причинам.

Но вот нейронные сети могут вывести эту проблему на ещё больший уровень угрозы. Использование технологии Text-To-Speech (TTS), изначально разработанной для глухих и детей с проблемами чтения, переводит текст в голосовой вид. Изначально безобидная технология, но в руках злоумышленника, она может принести вред. Нейросеть, обученная вести диалог, с заложенными алгоритмами на основе человеческой социологии и психологии, может генерировать текст при общении с человеком. Использование же модулей TTS и распознавания речи, позволит ей общаться голосом с другим человеком, чтобы прийти к поставленной цели. Сам голос, при этом, может быть различным – от кинозвёзд до родственников жертвы. Вряд ли кто-то заподозрит обман, когда с незнакомого телефона слышится голос родного человека и просит о помощи. Или же рьяному фанату футболиста звонит его кумир с предложением, от которого нельзя отказаться.

Даже несмотря на то что такая нейронная сеть несовершенна, так как требует действительно больших усилий для обучения, их засилие может оказаться катастрофическим для современного телефонного общения. Использование технологии подделки номеров позволит преступникам звонить на телефон жертвы со знакомого номера, и вести диалог от лица, изначально не подразумеваемого злоумышленника.

Единственное что может уберечь нас от такого сценария развития событий, так это затраты на разработку таких комплексов нейронных сетей, которые действительно астрономические, и государственное регулирование на международном уровне, иначе компрометации личности могут подвергнуться первые лица высших эшелонов власти. Развитие человечества влечёт за собой научно-технический прогресс. Он стремится улучшить жизнь человека, сделав её лёгкой и беззаботной. Каждое новое поколение испытывает с одной стороны меньше трудностей предыдущего, с другой стороны, порождает новые. Раньше, проблема мошенничества была тривиальна – обман на рынке или фальшивомонетчество. Однако с новыми технологиями появляются новые способы преступного отъёма денег у людей, пусть даже и по их воле.

Использование достижений человеческой социальной инженерии и психологии совместно с нейронными сетями приведёт к изменению общества, повышению недоверия друг к другу и паранойе. Остаётся лишь быть бдительными и надеется, что найдутся средства анализа, которые предотвратят повсеместное использование таких технологий.

Список источников

4. Барто Эндрю Г., Саттон Ричард С. " Обучение с подкреплением" - ДМК Пресс, 2020. – 552с.

5. Лапань М. " Deep Reinforcement Learning Hands-On" - Packt Publishing, 2018. – 546с.

6. Сайт компании OpenAI: https://openai.com/ (дата обращения 17.04.2023) eadingrockets.org/article/text-speech-technology-what-it-and-how-it-works (дата обращения 17.04.2023)

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Кулешов В.В. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.03.01 – Информационная безопасность» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Шамсулдин Хайдар Абдулваххаб Х. - аспирант Института автоматики и информационных технологий «ТГТУ».

Вклад авторов

Кулешов В.В.- идея, сбор материала, обработка материала, оформление текста.

Карасев П.И. – рекомендации по оформлению статьи, научное редактирование текста.

Шамсулдин Хайдар Абдулваххаб Х. – помощь в анализе информации, рекомендации по обработке материала.

Абд Али Хуссейн Наджми Абд Али – сбор материала.

Конфликт интересов отсутствует.

Научная статья
УДК 004.9

Повышение работоспособности специальной аппаратуры

Филипп Владимирович Макаренко [1]✉, Андрей Александрович Андрюшин[2], Георгий Дмитриевич Миронов [3], Алексей Михайлович Плотников [4], Игорь Сергеевич Голубятников [5]

[1,2,3,4,5] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия

[1] phillipp@mail.ru✉, https://orcid.org/0000-0003-3409-0340

[2] andreyandrushin93@gmail.com, https://orcid.org/0000-0003-3409-0347

[3] dru3@mail.ru ,https://orcid.org/0000-0003-3409-0389

[4] PPlo.A@gmail.com ,https://orcid.org/0000-0007-3409-0318

[5] golubyatnickov@mail.ru ,https://orcid.org/0000-0003-3108-0241

Аннотация. В статье рассматриваются методы резервирования аппаратуры на основе дублирование с нагруженным резервным элементом для повышения надежности аппаратуры. Показаны достоинство и недостатки метода.

Ключевые слова: резервирование, дублирование, аппаратура.

В настоящее время используются многочисленные методы резервирования для повышения стойкости аппаратуры [1, 2, 3, 4, 5]. В общем случае рассмотрим Т-кратное резервирование.

N-кратное резервирование – это целая группа методов. Оно является наиболее распространенным решением для борьбы со сбоями и отказами, вызванными любыми причинами, в том числе и радиационным воздействием ИИ КП. Суть метода заключается в том, что в систему, которую необходимо защитить от одиночного эффекта, вводятся N резервных элементов, которые способны выполнять функции основного элемента. Резервирование может быть общим, когда резервируется система в целом, и раздельным (поэлементным), когда резервируются отдельные элементы системы. Методы, относящиеся к этой группе, различаются степенью резервирования, объектом резервирования, способом сравнения результата и пр.

Рассмотрим один из методов, который не требует значительных затрат на аппаратные сложности и обеспечивает надежную работу аппаратуры.

Дублирование с нагруженным резервным элементом

Также к группе методов N-кратного резервирования относится и метод дублирования с нагруженным резервным элементом. Он направлен на обнаружение сбоев и отказов, вызванных любыми причинами. Суть метода можно описать следующим образом. В систему, которую необходимо защитить от сбоев и отказов, вводится один резервный элемент, находящийся в режиме

нагруженного резерва, при этом, результаты работы основного и резервного элементов сравниваются специальным блоком, который выдает сигнал ошибки в случае рассогласования результатов.

На рисунке показана схема метода дублирования с нагруженным резервным элементом. В качестве объекта резервирования, как правило, используют систему целиком или элементы на уровне ИС. Метод применяется в системах, где важно не допустить выдачу ложного результата. При этом, допускается временная потеря работоспособности системы. Метод относится к группе системотехнических методов.

Достоинство метода – обеспечивает обнаружение ОС и отказов, вызванных не только ИИ КП, но и любого другого характера.

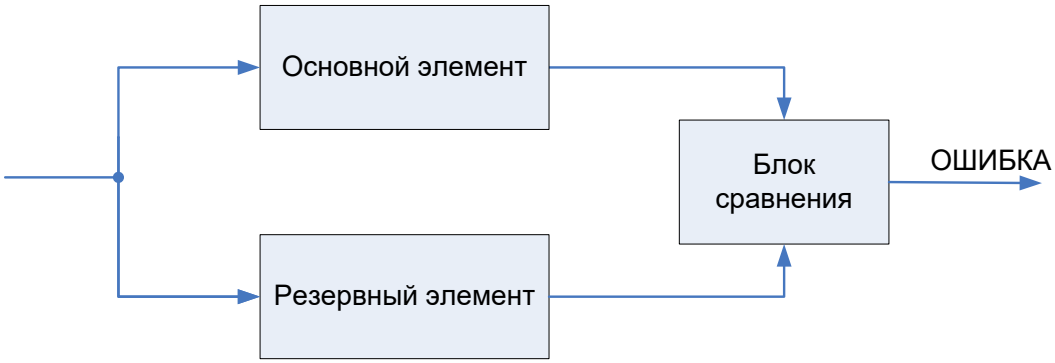

Рисунок. Схема метода дублирования с нагруженным резервным элементом

Недостатки метода:

- требует увеличение аппаратных затрат более, чем в два раза;
- ресурс нагруженного резервного элемента уменьшается так же, как и ресурс основного элемента, в результате чего общая надежность системы уменьшается;
- реакция на сигнал ошибки, например, переключение на следующий уровень резервирования, предполагает временную потерю работоспособности системы.

Список источников

1. Чубунов П.А. Компьютерное моделирование воздействия радиации на энергонезависимую память OXRAM / Чубунов П.А., Солодилов М.В., Рязанцев Р.Б., Литвинов Н.Н., Гамзатов Н.Г., Скворцова Т.В., Оксюта О.В. // Моделирование систем и процессов. 2022. Т. 15. № 3. С. 102-109.
2. Зольников В.К. Схемотехнические методы обеспечения стойкости экб к воздействию тяжёлых заряженных частиц /Зольников В.К., Макаренко Ф.В., Журавлева И.В., Попова Е.А., Гриднев Ю.В., Литвинова Ю.А. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 35-42.
3. Зольников В.К. Анализ чувствительности и результаты испытаний электронной компонентной базы к воздействию тяжелых заряженных частиц / Зольников В.К., Ягодкин А.С., Анциферова В.И., Евдокимова С.А., Скворцова Т.В., Грошева Е.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 43-51.

4. Зольникова А.Н. Методы обнаружения и исправления ошибок в нерегулярных структурах при воздействии тяжелых заряженных частиц / Зольникова А.Н., Евдокимова С.А., Оксюта О.В., Панина Н.В., Солодилов М.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 51-58.

5. Козюков А.Е. Общие подходы оценки стойкости к воздействию ионизирующего излучения космического пространства для зарубежной электронной компонентной базы предприятий –разработчиков / Козюков А.Е., Гамзатов Н.Г., Гречаный С.В., Зольников К.В., Струков И.И., Ачкасов А.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 58-66.

Статья поступила в редакцию 23.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Макаренко Ф.В. - к.ф.-м.н., доцент «Базовая кафедры технического и программного обеспечения вычислительных и информационных систем» ФГБОУ ВО «ВГЛТУ».

Андрюшин А.А. - преподаватель СПО кафедры «Информационные технологии» ФГБОУ ВО «ВГЛТУ».

Миронов Г.Д. - аспирант ФГБОУ ВО «ВГЛТУ».

Плотников А.М. - аспирант ФГБОУ ВО «ВГЛТУ».

Голубятников И.С. - преподаватель СПО кафедры «Информационные технологии» ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Макаренко Ф.В. - идея, сбор материала, обработка материала, научное редактирование текста.

Андрюшин А.А. - частичное написание статьи (25%).

Миронов Г.Д. - частичное написание статьи (25%).

Плотников А.М.- частичное написание статьи (25%).

Голубятников И.С. - частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004:056

Теоретическая подготовка специалистов как фактор успешного проведения процедуры пентеста

Елизавета Андреевна Музалевская[1], Екатерина Владимировна Кондрашова[2], Максим Михайлович Голембиовский[3], Михаил Юрьевич Рытов [4]
[1,2,3,4]Брянский государственный технический университет, Брянск, Россия
[1]lizamuz2002@yandex.ru✉
[2]kondrashova_katerina@bk.ru✉
[3]maksim32region@yandex.ru✉
[4]rmy@tu-bryansk.ru✉

Аннотация. В ходе проведения пентеста проверяются настройки систем защиты, выявляется наличие уязвимостей в системном и пользовательском программном обеспечении, а также проверить реакцию сотрудников на традиционные тактики, такие как целевой фишинг и иногда несанкционированный доступ.

Ключевые слова: пентест, фишинг, проникновение.

Пентест (penetration testing) – тест на возможность проникновения в систему.

В ходе его проведения проверяются настройки систем защиты, выявляется наличие уязвимостей в прошивках оборудования, системном ПО и пользовательском софте, а также изучается реакция сотрудников на традиционные уловки, включая таргетированный фишинг, а иногда и физический доступ неавторизованного персонала [1].

Одним из факторов влияния на проведение данной процедуры является теоретическая подготовка специалиста. От того насколько высок уровень подготовки тестировщика напрямую зависит то, как он будет действовать на практике.

При недостаточной квалификации может оказаться так, что результат проведенного пентеста будет положительным не по причине защищенности системы и отсутствия уязвимостей, а по причине того, что имеющиеся слабости системы не являются очевидными.

В табл. 1 представлена краткая образовательная траектория специалиста по проведению пентеста. Она представляет собой общее описание ключевых теоретических аспектов, которые следует знать тестировщику.

Таблица 1

Образовательная траектория специалиста по проведению пентеста

Раздел	Темы

Основные технологии, используемые браузерами	HTML, JavaScript, HTTP, веб-сокеты, CSS, SOP, CORS, cookies, хранилища и особенности их работы
Основные технологии разработки серверной части	PHP, фреймворки, системы управления контентом
Linux, Kali Linux	Основной функционал, управление сервисами, пользователями, правами, сетью и менеджеры пакетов
Windows Server	Механизмы управления сетью устройств и сетевым оборудованием, работа с Active Directory, сетевыми протоколами DNS, DHCP и ARP, а также их настройки
Корпоративные сети Cisco	Архитектура, настройка оборудования Cisco, маршрутизация VLAN и Trunk портов, мониторинг трафика и управление корпоративной сетью
Повышение кроссплатформенных привилегий	Изменение привилегий в различных операционных системах, закрепление в них, использование эксплойтов, переполнение буфера, замена DLL-файлов на вредоносные библиотеки. - вертикальное повышение – имитация пользователя уровнями выше; - горизонтальное повышение – имитация пользователя того же уровня; - понижение – имитация пользователя уровнями ниже.
Реверс-инжиниринг	Ассемблер и его особенности, специфика C++, типы циклов кода, дизассемблеры, отладчики, HEX-редакторы

Специалист, имеющий указанные теоретические знания сможет качественно провести процедуру пентеста.

Как один из вариантов подтверждения знаний специалиста используются международные экзамены CEH и OSCP. Сдача экзаменов CEH и OSCP опциональна, но позволяет закрепить пройденный материал и получить соответствующие сертификаты.

Если сотрудник имеет хотя бы один из указанных сертификатов, уровень его подготовки автоматически считается соответствующим.

При отсутствии сертификации уровень подготовки сотрудников можно проверить при помощи внутреннего тестирования. За основу могут быть взяты вопросы из тестов международной сертификации. В таблице 2 представлен пример составления анкеты на основе сертификации CEH. После каждого вопроса для проверки представлен верный ответ с пояснением, анкету с пояснениями также можно выдавать и сотрудникам после прохождения тестирования для восполнения пробелов в знаниях [3].

Таблица 2

Пример анкеты тестирования сотрудника относительно уровня теоретической подготовки

1. Что из нижеперечисленного является пассивным разведывательным действием? *(поставьте галочку рядом с верным ответом)*
A. Поиск информации в местной газете B. Звонок в отдел кадров C. Использование команды nmap -sT D. Проведение атаки типа «человек посередине»
Ответ A. Поиск информации в местной газете считается пассивным, поскольку он не оказывает прямого воздействия или установления какого-либо типа связи между жертвой и противником. Все другие ответы подразумевают прямое того или иного вида подключение к компании или ее сети.
2. Какое шифрование было выбрано NIST в качестве основного метода обеспечения конфиденциальности после алгоритма DES? *(поставьте галочку рядом с верным ответом)*
A. 3DES B. Twofish C. RC4 D. AES
Ответ D. Был выбран шифр Rijndael, который затем получил название Advanced Encryption Standard (AES).
3. Какой облачный сервис вы, скорее всего, будете использовать, если захотите поделиться документами с другим человеком? *(поставьте галочку рядом с верным ответом)*
A. Программное обеспечение как услуга (Software as a Service) B. Платформа как услуга (Platform as a Service) C. Хранение как услуга (Storage as a Service) D. Инфраструктура как услуга (Infrastructure as a Service)
Ответ C. Хранение как услуга предлагает возможность хранения документов или других неструктурированных данных, которыми затем можно поделиться с другими. Программное обеспечение как услуга хранит данные в приложении, как правило, и не позволяет обмениваться документами. Платформа как услуга или инфраструктура как услуга можент использоваться, но они требуют дополнительной работы, чтобы обеспечить загрузку файлов и их совместного использования. Хранение как услуга была бы самым простым способом.
4. В чем разница между традиционным брандмауэром и IPS? *(поставьте галочку рядом с верным ответом)*
A. Брандмауэры не генерируют журналы. B. IPS не может отбрасывать пакеты. C. IPS не следует правилам. D. IPS может проверять и отбрасывать пакеты.

Ответ D. IPS проверяет пакеты, чтобы сопоставить их с правилами, написанными для поиска вредоносного трафика. И IPS, и брандмауэр обычно генерируют журналы. IPS действительно следует правилам и может отбрасывать пакеты, что отличает IPS от IDS.
5. В чем заключается одно из преимуществ IPv6 перед IPv4 с точки зрения безопасности? *(поставьте галочку рядом с верным ответом)*
A. IPv4 имеет меньшее адресное пространство. B. IPv6 позволяет проверять подлинность заголовка. C. IPv6 более гибко относится к расширениям. D. IPv6 обычно представлен в шестнадцатеричном формате.
Ответ B. Хотя и все ответы верные, единственный ответ, относящийся к безопасности, – это вариант B. IPv6 позволяет аутентифицировать заголовки. Это гарантирует, что пакеты не были подделаны.

В случае если сотрудник допустил не более двух ошибок – уровень его подготовки считается соответствующим.

Удовлетворительным для объекта в целом может считаться результат, когда более половины сотрудников организации, задействованных в процедуре пентеста имеют соответствующую теоретическую подготовку

В случае если получен неудовлетворительный результат, необходимо повышать уровень теоретической подготовки сотрудников путем проведения тренингов, курсов повышения квалификации и прочих образовательных мероприятий.

Список источников

1. Дэвис Р. Искусство тестирования на проникновение в сеть / Дэвис Р. - Москва : ДМК Пресс, 2021. - 310 с. - ISBN 978-5-97060-529-5. -URL: https://www.iprbookshop.ru/124991.html (дата обращения: 13.03.2023).

2. Проверяем свои силы в тесте на CEH (Certified Ethical Hacker) // $ information Security Squad URL: https://itsecforu.ru/2021/10/19/проверяем-свои-силы-в-тесте-на-ceh-certified-ethical-hacker/ (дата обращения: 13.03.2023).

3. https://itsecforu.ru/2021/10/19/проверяем-свои-силы-в-тесте-на-ceh-certified-ethical-hacker/ https://itsecforu.ru/2021/10/19/проверяем-свои-силы-в-тесте-на-ceh-certified-ethical-hacker/.

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Музалевская Е.А. – студент кафедры «Системы информационной безопасности», направление подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Кондрашова Е.В. – студент кафедры «Системы информационной безопасности», направление подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Голембиовский М.М. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Рытов М.Ю. – заведующий кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Музалевская Е.А. – сбор материала, частичное написание статьи (25%).

Кондрашова Е.В. – сбор материала, частичное написание статьи (25%).

Голембиовский М.М. – научное редактирование текста, частичное написание статьи (25%).

Рытов М.Ю. – идея, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Пентест. Структура процесса и перечень факторов, оказывающих влияние на достоверность результатов

Елизавета Андреевна Музалевская[1]✉, Екатерина Владимировна Кондрашова[2], Артем Андреевич Рябцев [3], Кирилл Евгеньевич Шинаков[4]
[1, 2, 3,4]Брянский государственный технический университет, Брянск, Россия
[1] lizamuz2002@yandex.ru✉,
[2]kondrashova_katerina@bk.ru,
[3]ryabcev@yandex.ru,
[4] shinakov@it-craft.net

Аннотация. На сегодняшний день все большую популярность набирает такой метод усиления безопасности активов, как пентест. Все чаще появляется необходимость повышать уровень качества и скорости обнаружения уязвимостей в рамках отдельных систем для предотвращения угрозы реализации кибератак.

Ключевые слова: пентест, информационная безопасность, активы.

В настоящее время все большую популярность набирает такой метод усиления безопасности активов, как пентестирование. Пентест (penetration testing) – процедура оценки возможостей проникновения в систему, путем поиска уязвимостей оборудования и ПО.

Важность процедуры пентеста для современных компаний не может быть переоценена. Согласно отчету, представленному командой Solar JSOC [1], в 2022 году сформировался четкий тренд на переход от массовых атак к более точечным с использованием обнаруженных уязвимостей. По прогнозам тренд сохранится и в 2023 году, так как отечественные компании имеют ряд проблем, которые не получится оперативно решить. В частности, это долгий переход на отечественное ПО и сложности с обновлением сигнатур и модулей безопасности западных СЗИ.

Данная статистика свидетельствует о том, что имеется необходимость в кратчайшие сроки повышать уровень качества и скорости обнаружения уязвимостей в рамках отдельных систем для предотвращения угрозы реализации кибератак. Тестирование компьютерных систем на проникновение позволяет избежать финансовых и репутационных потерь компаниям.

По виду пентест подразделяется на внешний и внутренний.

Внешний пентест предполагает проверку пограничных ресурсов, расположенных в демилитаризованной зоне [2] (средства удаленного доступа, веб-сайты и др.), межсетевые экраны и другие устройства, доступ к которым имеется через публичные IP-адреса. Цель нарушителя в данном случае – проникновение во внутреннюю сеть либо получение контроля над внешними

ресурсами.

Внутренний пентест предполагает проверку внутренних серверов, сетевого оборудования, АРМ пользователей, средств виртуализации. Выявляются всевозможные недостатки в организации сети, проверяются WiFi-сети [2]. Помимо этого, проверку проходят те же ресурсы, что и при внешнем пентесте, но доступ осуществляется из внутренней сети (с использованием внутренних IP-адресов), т. е. нарушитель действует из сегмента локальной сети. Цель нарушителя в данном случае – контроль инфраструктуры или отдельных сервисов сети.

Организация самостоятельно выбирает какой из видов процедуры приоритетнее, в зависимости от типа обрабатываемой информации, потенциально актуальных нарушителей, технической оснащенности объекта, а также квалификации штата сотрудников. Но предпочтительно проводить пентест обоих видов сразу или же поочередно.

В общем виде процесс проведения пентеста состоит из 4 этапов, описываемых в таблице 1.

Таблица 1

Описание этапов проведения пентеста

Этап проведения пентеста	Описание этапа
Этап 1. Сбор информации	1) Составление карты сети: создание карты сети включает в себя добавление сетевых устройств (используется сканирование сети), рисование линий-связей между устройствами, рисование областей для объединения устройств в группы. 2) Определение возможных целей: как правило в качестве целей выбираются наиболее критические для компрометации объекты. 3) Перечисление слабых мест в службах, работающих на этих целях: другими словами, поиск объектов и средств, которые могут иметь уязвимость.
Этап 2. Целенаправленное проникновение	Этап предполагает проникновение в уязвимые сервисы (получение несанкционированного доступа к ним).
Этап 3. Постэксплуатация и повышение привилегий	1) Определение информации о скомпрометированных системах, которая может быть использована для дальнейшего доступа (закрепления в системе). 2) Повышение привилегий до самого высокого уровня доступа в сети (до уровня администратора).

Этап проведения пентеста	Описание этапа
Этап 4. Документирование	1) Сбор доказательств проникновения. 2) Подготовка окончательного отчета: после завершения тестовой части вторжения составляется подробный отчет. Этот отчет содержит детальное описание всех способов, которыми удалось взломать сеть и обойти меры безопасности, а также предложение мер, которые можно предпринять, чтобы закрыть выявленные бреши и гарантировать, что они больше не будут использованы кем-либо еще.

Профессиональные тестировщики придерживаются специальных методик и стандартов, принятых в сфере информационной безопасности. Существует 5 самых известных и авторитетных методологий пентеста: OSSTMM, NIST SP800-115, OWASP, ISSAF и PTES. Выбор зависит от бизнес-процессов организации и процессов информационной безопасности.

Используя существующие методологии и зная особенности проведения пентеста, организация может значительно повысить собственную защищенность от кибератак. Но степень обретаемой защищенности напрямую зависит от качества проведенной процедуры.

Качество и успешность проведенного пентеста в свою очередь зависит от составляющих его факторов. Каждый отдельный фактор оказывает решающее влияние на то, насколько достоверен будет полученный результат, и то, насколько эффективно будет защищена система посредством применения превентивных мер.

Факторы, нуждающиеся в оценке:

– Фактор 1. Теоретическая подготовка специалистов.
– Фактор 2. Практическая подготовка специалистов.
– Фактор 3. Наличие инструментов для проведения пентеста.

Только при комплексной высокой оценке всех упомянутых факторов возможно провести процедуру тестирования на проникновение быстро и эффективно. Однако наиболее важной является практическая подготовка специалистов, поскольку при наличии прочих факторов именно наличие данного является решающим. Преимущественно в рамках обучения специалистов в университете делается упор на теорию, однако практический опыт значительно важнее и требует постоянных вложений времени со сторон специалиста, поскольку технологии не стоят на месте и у злоумышленников появляются все новые и новые способы проникнуть в защищаемую инфраструктуру.

Таким образом, существует большое количество различных методологий и путей проведения процедуры пентеста. Выбор конкретного алгоритма зависит от типа объекта. Но наиболее важным условием успешности проведения процедуры является практическая подготовка специалистов ее проводящих,

которой стоит уделять постоянное внимание и направлять все силы на ее совершенствование.

Список источников

1. Атаки на российские компании. – URL: https://rt-solar.ru/analytics/reports/3089/ (дата обращения: 28.03.2023).

2. Основы тестирования КИИ на проникновение : учебное пособие / А.И. Елисеев [и др.]. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2019. — 84 с. — ISBN 978-5-8265-2090-1. — URL: https://www.iprbookshop.ru/99777.html (дата обращения: 13.03.2023).

Статья поступила в редакцию 10.04.23; принята к публикации 10.05.2023.

Информация об авторах

Музалевская Е.А. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Кондрашова Е.В. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Рябцев А.А. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Шинаков К.Е. – доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Музалевская Е.А. – идея, сбор материала (30%).

Кондрашова Е.В. – сбор материала, обработка материала (26%).

Рябцев А.А. – обработка материала, частичное написание статьи (23%).

Шинаков К.Е. – написание статьи, научное редактирование текста. (21%).

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Сравнительный анализ сертифицированных и импортных средств защиты информации (СЗИ от НСД, Siem, dlp, антивирусы и т.д.) в контексте оптимального создания системы информационной безопасности для значимых объектов критической информационной инфраструктуры

Никита Олегович Мусиенко[1], Дмитрий Андреевич Лысов[2], Вероника Вячеславовна Кузина[3]✉, Вероника Дмитриевна Медведева[4]
[1,2,3,4] Брянский государственный технический университет, Брянск, Россия
[1]musienkono@yandex.ru, https://orcid.org/0009-0001-3699-5404
[2] lysovdmitriia@gmail.com, https://orcid.org/0009-0003-9666-7191
[3]veronika.k02@bk.ru✉, https://orcid.org/0009-0003-9513-5222
[4]nicka.medvedeva2020@yandex.ru, https://orcid.org/0009-0007-4326-8073

Аннотация. В статье раскрывается проблема ускоренного импортозамещения программного обеспечения и аппаратных средств защиты информации. Критическая информационная инфраструктура России переходит на отечественное программное обеспечение. На повестку дня выносится вопрос о российских технологиях и средствах разработки, позволяющих компаниям создавать информационные системы, аналоги которых на российском рынке отсутствуют.

Ключевые слова: ФСТЭК России, информационная безопасность, критическая информационная инфраструктура, импортозамещение, сертификация, средство защиты информации, программное обеспечение, российское производство, кибербезопасность.

Текущая политическая ситуация в Российской Федерации заставила многие организации перейти на импортозамещение. Некоторые иностранные средства, используемые в России, уже не работают в полном объеме, а продление подписки на иностранное программное обеспечение вызывает проблемы с обновлением программных продуктов. Растущий масштаб кибератак также негативно влияет на стабильность государственного сектора, финансовых рынков и промышленности в целом. Поэтому тема ускоренного импортозамещения приобретает особую актуальность [5].

На реализацию отечественных интересов в информационной сфере согласно Доктрины ИБ направлены подписанные Президентом России указы: № 166 от 30.04.2022 **«О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»** [2] и № 250 от 01.05.2022 **«О дополнительных мерах по обеспечению информационной**

безопасности Российской Федерации» [1]. Эти документы призваны изменить подход к поддержанию кибербезопасности на российских предприятиях.

Статистические данные о реализации программы импортозамещения "Развитие государства" показывают, что к концу 2021 года доля российского программного обеспечения, используемого государственными предприятиями, должна была составить 50-70%, но в реальности она составила 30-35%. Многие государственные предприятия адаптировались к иностранной продукции, что затрудняло переход на российское программное обеспечение.

Однако во многих областях заменить зарубежные продукты довольно сложно. Сначала уход иностранных игроков затронул сектор сетевой безопасности, а затем и рынок информационной безопасности. Участники CISO Forum 2022 отметили, что в нашей стране нет собственных решений для контроля сетевого доступа (NAC), контейнеров, виртуальных рабочих столов (VDI), систем хранения данных, а также отсутствуют решения для защиты облачных сред.

Сравнение характеристик отечественных и иностранных средств защиты информации.

Исследуя полученные данные в рамках выявленной актуальной проблемы, целесообразно будет проанализировать такие средства защиты информации как SIEM – системы [6]. Такие инструменты выполняют ряд мер безопасности и требований в соответствии с документами ФСТЭК России [7].

Результаты анализа отечественных и зарубежных сертифицированных средств защиты информации.

1. **Преимущества отечественного продукта «Ребус-СОВ»:**

- функционирование как на уровне сети, так и на уровне узла;
- поддержка ОС Microsoft Windows, Astra Linux;
- гибкая настройка автоматической реакции на вторжения.

Недостатки:

- одних только сигнатурных методов обнаружения вторжений недостаточно.
- большое количество ложных срабатываний.

Преимущества зарубежного продукта «FortiGate»:

- производительность – все модели FortiGate оснащены процессором, который разгружает центральный процессор от наиболее трудоемких задач;
- FortiGate может исследовать сеть и предоставить администратору визуальное представление структуры сети.

Недостатки:

- отсутствие русской локализации.
- Многочисленные уязвимости, в том числе уязвимости, используемые удаленно;
- дорого продление подписок после первых трех лет.

2. Преимущества отечественного продукта «Positive Technologies Network Attack Discovery»:

- Улавливает активность злоумышленников даже в зашифрованном трафике;
- хранит записи трафика;
- выявляет отклонения от нормативных требований.

Недостатки: для полноценной работы с продуктом необходимы знания в сфере сетевой безопасности;

- для антивирусной проверки передаваемых по сети файлов нужно подключать сторонние решения.

Преимущества зарубежного продукта «Splunk Enterprise»:

- дает возможность устранять неисправности для повышения производительности;
- дает возможность собирать полезные оперативные данные из машинных данных.

Недостатки:

- ограничения по объему трафика;
- внедрение и поддержка Splunk требует ресурсов.

3. Преимущества отечественного продукта «RuSIEM»:

- своевременное информирование и реагирование на различные виды угроз;
- отслеживание аутентификации;
- отсутствие ограничений при выборе источников событий.

Недостатки:

- некоторые дашборды (графики, таблицы) неинформативны;
- мало предустановленных комплаенс-проверок и отчётов;
- обилие кнопок на боковой панели интерфейса затрудняет поиск необходимой функции.

Преимущества зарубежного продукта «FireEye»:

- постоянное и своевременное обновление информации об актуальных угрозах;
- комплексное решение ИБ, которое обеспечивает защиту, начиная от конечной точки и заканчивая целой сетью.

Недостатки: отсутствие русской локализации.

4. Преимущества отечественного продукта «Kaspersky Unified Monitoring and Analysis Platform (версия 1.5)»:

- создание уведомлений о выявлении признаков угроз ИБ;
- наличие встроенных сценариев автоматического реагирования на выявленные ИБ - события.

Недостатки:

- нет возможности создавать PDF-отчёты (только HTML) – добавление запланировано на первую половину 2022 года.
- обновление контента производится вручную –

поддержка автообновления запланирована на вторую половину 2022 года.

Преимущества зарубежного аналога «Foritnet (FortiSIEM)»:

- автоматизация процессов обнаружения угроз и аномалий;
- автоматизация процессов регистрации и контроля инцидентов, с последующей возможностью их расследования;

Недостатки:

- отсутствие русской локализации;
- отсутствует поддержка подключения к ФинСерт или ГосСОПКА.

В контексте оптимального создания системы информационной безопасности для значимых объектов критической информационной инфраструктуры рекомендуется использование следующихотечественных средств защиты информации:

1. Программный комплекс обнаружения вторжений «Ребус-СОВ».
2. Программное изделие «Система обнаружения и предотвращения вторжений Positive Technologies Network Attack Discovery».
3. «Система управления событиями безопасности «RuSIEM».
4. Программное изделие «Kaspersky Unified Monitoring and Analysis Platform (версия 1.5)».

Опираясь на Указы президента Российской Федерации № 166 от 30.04.2022 и № 250 от 01.05.2022, можно заметить, что затрагиваются проблемы, связанные с импортозамещением ПО и аппаратных средств защитыинформации.

В настоящее время поставки аппаратных средств защиты информации затруднены. С чем это связано?

- Во-первых, затруднены в связи с высокой стоимостью аппаратных средств защиты информации.
- Во-вторых, существуют трудности с аппаратным обеспечением. Компоненты для производства отечественного оборудования, такие как серверы, процессоры, модемы импортируются из-за рубежа. Несмотря на наличие процедур по замене компонентов, запустить высокотехнологичное производство без импортных технологий невозможно.

Возможно ли, при создании систем безопасности объектов критической информационной инфраструктуры использовать наложенные средства ИБ только российского производства? Какие средства могут помочь для решения данной задачи?

Сейчас перечень средств защиты информации для критической информационной инфраструктуры обозначает ФСТЭК. Несмотря на текущее применение наложенных средств отечественного производства, полное прекращение использования ПО – потребует больших организационных, экономических и политических изменений.

Список источников

1. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»: официальный сайт. – Москва, 2022. Режим доступа: URL.: http://publication.pravo.gov.ru/Document/View/0001202205010023 (дата обращения 18.09.2022).

2. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»: официальный сайт. – Москва 2022. Режим доступа: URL.: http://publication.pravo.gov.ru/Document/ View/0001202203300001 (дата обращения 20.09.2022).

3. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации (в ред. приказов фстэк россии от 9 августа 2018 г. n 138, от 26 марта 2019 г. n 60, от 20 февраля 2020 г. n35)»: официальный сайт. URL: https://fstec.ru/en/53- normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya- 2017-g-n-239 (дата обращения 28.09.2022).

4. Доля российского софта в госкомпаниях оказалась вдвое ниже нормативов: официальныйсайт. URL: https://www.comnews.ru/content/218138/2021-12-27/2021-w52/dolya-rossiyskogo-softa-goskompaniyakh-okazalas-vdvoe-nizhe-normativov.

5. Туркина, А. А. Некоторые аспекты "импортозамещения" в сфере ит / А. А. Туркина // Анализ и современные информационные технологии в обеспечении экономической безопасности бизнеса и государства : Сборник научных трудов и результатов совместных научно- исследовательских проектов / РЭУ им. Г.В. Плеханова. – Москва: Аудитор, 2016. – С. 543-547 (дата обращения16.10.2022).

6. Федорченко, А. В. Корреляция информации в SIEM-системах на основе графа связей типов событий / А. В. Федорченко, И. В. Котенко // Информационно-управляющие системы. – 2018. – № 1(92). – С. 58-67. (дата обращения 10.10.2022

7. . Приказ ФСТЭК России от 3 апреля 2018 г. № 55 «Об Утверждении Положения о системе сертификации средств защиты информации»: официальный сайт. Режим доступа: URL: https://www.garant.ru/products/ipo/prime/doc/71842006/ (дата обращения 22.10.2022).

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Мусиенко Н.О. – аспирант, ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы

информационной безопасности» ФГБОУ ВО «БГТУ».

Кузина В.В. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03. – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Медведева В.Д. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03. – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Мусиенко Н.О. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Лысов Д.А. – написание статьи, научное редактирование текста (25%).

Кузина В.В. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Медведева В.Д. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Обзор новых требований обеспечения информационной безопасности для значимых объектов критической информационной инфраструктуры в соответствии с Указом Президента РФ № 250 от 01.05.2022 г. «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Никита Олегович Мусиенко[1], Дмитрий Андреевич Лысов[2], Вероника Дмитриевна Медведева[3]✉, Вероника Вячеславовна Кузина[4]

[1,2,3,4]ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия

[1]musienkono@yandex.ru, https://orcid.org/0009-0001-3699-5404

[2]lysovdmitriia@gmail.com, https://orcid.org/0009-0003-9666-7191

[3]nicka.medvedeva2020@yandex.ru✉, https://orcid.org/0009-0007-4326-8073

[4]veronika.k02@bk.ru, https://orcid.org/0009-0003-9513-5222

Аннотация. Обзор положений Указа Президента РФ № 250 от 01.05.2022г. «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». В статье отражены результаты качественной оценки затрат на реализацию новых требований и оценка эффективности данных требований.

Ключевые слова: ГосСОПКА, ФСТЭК, ФСБ России, защита КИИ, кибератака, структурное подразделение, криптографическая защита,аудит.

В современном мире к процедуре обеспечения информационной безопасности критической информационной инфраструктуры Российской Федерации возникают новые вызовы и задачи, нацеленные не только на обеспечение бесперебойного функционирования таких инфраструктур, но и на их устойчивое развитие в соответствии с национальными интересами, зафиксированными в Доктрине информационной безопасности РФ [2].

Дополнительным вызовом также является глобальный тренд – рост числа кибератак, направленный в первую очередь на критически важные объекты государства. Одной из основных причин роста числа кибератак на компании в Российской Федерации является то, что многие зарубежные поставщики корпоративных средств информационной безопасности прекратили свою деятельность в России. Учитывая обострение политической ситуации в стране, рост кибератак увеличивается, их масштаб растёт, от этого страдает государственный сектор, информационные технологии, банки и промышленность.

Таким образом, существует острая необходимость в системной модификации подходов к обеспечению информационной безопасности в

критических сферах деятельности государства.

Решением такого вопроса стал Указ Президента РФ № 250 от 01.05.2022 г. «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [1].

Данный Указ направлен на проведение дополнительных мероприятий по совершенствованию процедур информационной безопасности для ряда критически важных компаний России. К таким компаниям относятся некоторые органы власти, предприятия с государственным участием, субъекты критической информационной инфраструктуры (КИИ), стратегические и системообразующие организации (далее – критически важные организации) [9].

Обзор положений Указа Президента РФ № 250

В соответствии с пунктом 1, документ устанавливает требования к руководителям критически важных организаций создать на базе организации структурное подразделение, выполняющее функции по обеспечению информационной безопасности основного органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствийкомпьютерных атак и реагированию на компьютерные инциденты, или возложить эти функции на существующее структурное подразделение. При этом, заместитель руководителя главного органа (организации) должен быть уполномочен обеспечивать информационную безопасность главного органа (организации), включая средства ГосСОПКА [8].

Перед исполнителем ставится ряд ключевых задач, нацеленных на модернизацию организационной безопасности внутри организации. Решение этих задач предусматривает расширение штата сотрудников по информационной безопасности за счет создания структурного подразделения, в том числе взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также защиту критических информационных инфраструктур [7].

В соответствии с новыми требованиями, расширяется и зона ответственности должностных лиц в отношении вопросов информационной безопасности. Пример изменения структуры организации представлен на рисунке 1. Взаимодействие со сторонними компаниями в рамках исполнения мероприятий по защите информации должно подтверждаться наличием соответствующих лицензий или аккредитаций.

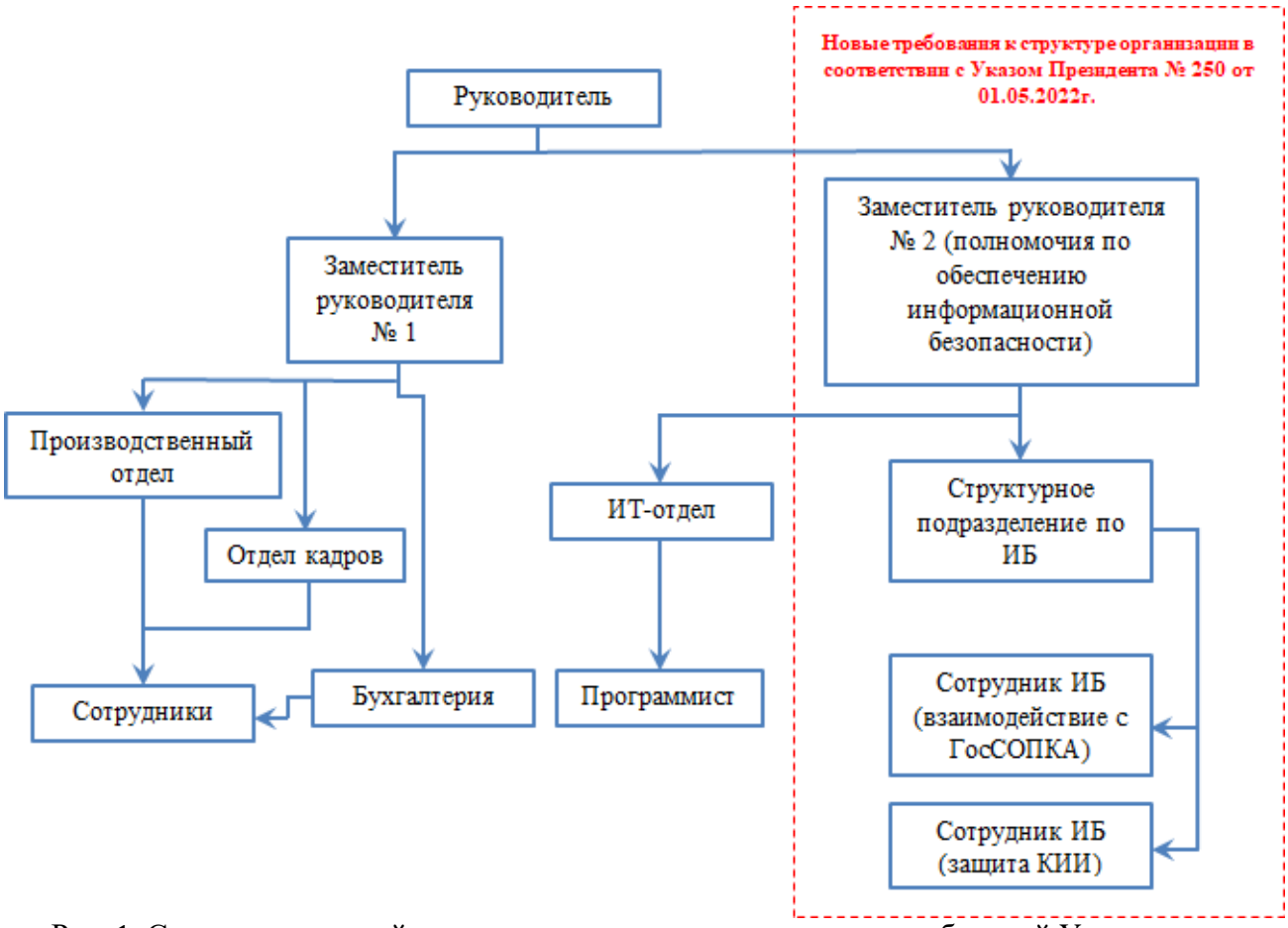

Рис. 1. Структура типовой организации после принятия новыхтребований Указа Президента РФ № 250 от 01.05.2022 г.

Ключевым фактором при реализации нововведений является оперативность внедряемых решений, за счет обеспечения незамедлительной реализации организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенции и направляются в организации с учетом меняющихся угроз в информационной сфере.

Основным требованием в рамках нововведений, является необходимость соблюдения особого порядка применения средства защиты информации.

Согласно пункту 6 рассматриваемого документа, запрещается использовать средства защиты информации, создаваемые иностранными государствами, которые действуют недружественным образом по отношению к Российской Федерации, российским юридическим и физическим лицам. При выборе иностранных средств защиты информации необходимо не только обращать внимание на страну-производителя, но также проверять аффилированность компании (состав собственников, членов органов управления, лиц имеющих право распоряжаться общим количеством голосов).

Оценка эффективности реализации новых требований Указа Президента РФ № 250.

Указ Президента РФ № 250 от 01.05.2022 г. «О дополнительных мерах

по обеспечению информационной безопасности Российской Федерации» позволяет повысить уровень информационной безопасности, а именно:

- вопрос обеспечения информационной безопасности в организации поднимается на более высокий уровень;
- возрастает роль руководителя организации в вопросах обеспечения информационной безопасности;
- появляются подразделения, ответственные за обеспечение ИБ;
- организовываются проекты по созданию унифицированной среды для безопасной разработки отечественного ПО и по КИИ для систематического исследования безопасности;
- создаются проекты, призванные помочь российским разработчикам в создании ПО для объектов критической информационной инфраструктуры.

В России выявлены масштабные кибератаки против госсектора. Это связано с политически мотивированными действиями хакеров, уходом поставщиков услуг безопасности и проблемой преследования киберпреступников, находящихся за рубежом. С момента начала спецоперации почти 90% инфраструктуры госсектора России подверглись кибератакам.

На этом фоне спрос на продукты безопасности со стороны российских разработчиков растет, а продажи увеличиваются из-за возросшей активности хакеров и конкуренции.

Указ нацелен на повышение уровня информационной безопасности критически важных организаций РФ. Реализация предусмотренных мер окажет существенное влияние на рынок ИБ-услуг. Резко возрастет спрос на специалистов по информационной безопасности, способных обеспечить реальную защиту информации. Для исполнения требований Указа были приняты следующие решения.

1. Компаниям необходимо провести работы по распределению ответственности за обеспечение ИБ на должностных лиц, а именно, на заместителя генерального директора, а также создать структурное подразделение, отвечающее за ИБ, обнаружение и реагирование на атаки.
2. Подготовить должностные инструкции в соответствии с нормативнымидокументами, введенными Правительством РФ.
3. Выполнить аудит защищенности информационных ресурсов, в том числе инвентаризацию оборудования, которое находится в эксплуатации, чтобы выявить иностранное аппаратное и программное обеспечение, средства защиты информации.
4. Необходимо проанализировать подрядчиков в области ИБ на наличие у них необходимых лицензий, а в дальнейшем – и на наличие аккредитации у центров ГосСОПКА. Компаниям в текущей ситуации следует быть готовыми к оперативному взаимодействию с регулирующими органами (ФСБ России, ФСТЭК России) и выполнению их указаний.

Список источников

1. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»: официальный сайт. – Москва, 2022. Режим доступа: URL.: http://publication.pravo.gov.ru/Document/View/0001202205010023 (дата обращения 18.09.2022).

2. Доктрина информационной безопасности Российской Федерации: официальный сайт. – Москва, 2000. Режим доступа: URL.: http://www.scrf.gov.ru/security/information/document5/ (дата обращения 05.10.2022).

3. Kaspersky ICS CERT: официальный сайт. Режим доступа: URL.: https://ics-cert.kaspersky.ru/media/Kaspersky-Threat-landscape-for-industrial-automation-systems-statistics-for-H2-2020-Ru.pdf (дата обращения 20.09.2022).

4. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА: официальный сайт. Режим доступа: URL: http://www.tadviser.ru (дата обращения 28.09.2022).

5. Сердюк В.Д. Аудит информационной безопасности (ИБ): официальный сайт. Режим доступа: URL:http://www.bytemag.ru/articles/detail.php?ID=6781 (дата обращения02.10.2022).

6. Горелик В.Ю, Безус М.Ю. О безопасности критической информационной инфраструктуры Российской федерации // Научно-образовательный журнал «StudNet» №9/2020. С. 1446-1447 (дата обращения 04.10.2022).

7. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26.07.2017 № 187-ФЗ: официальный сайт. Режим доступа: URL: http://www.pravo.gov.ru (дата обращения 05.10.2022).

8. Кузнецов П.У. Отдельные аспекты формирования правового обеспечения международной информационной безопасности // Вестн. УрФО. 2016. № 4 (22). С. 38-43 (дата обращения 08.10.2022).

9. Луийф Е. Безопасность критических информационных инфраструктур / Луийф Е., Жутауайте И., Хеммерли Б. М. // CRITIS 2018: 13-я Международная конференция. – Каунас, 2019 (дата обращения 10.10.2022).

10. Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. – РнД: Феникс, 2017. – 347 с. (дата обращения 12.10.2022).

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Мусиенко Н.О. – аспирант, ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Медведева В.Д. – студент кафедры «Системы информационной

безопасности», направления подготовки «10.05.03. – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Кузина В.В. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03. – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Мусиенко Н.О. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Лысов Д.А. – написание статьи, научное редактирование текста (25%).

Медведева В.Д. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Кузина В.В. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Обзор Указа Президента РФ № 166 от 30.03.2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» в контексте создания системы информационной безопасности для значимых объектов критической информационной инфраструктуры

Никита Олегович Мусиенко[1], Дмитрий Андреевич Лысов[2], Вероника Дмитриевна Медведева[3*], Вероника Вячеславовна Кузина[4]
[1,2,3,4]Брянский государственный технический университет,Брянск, Россия
[1]musienkono@yandex.ru, https://orcid.org/0009-0001-3699-5404
[2]lysovdmitriia@gmail.com, https://orcid.org/0009-0003-9666-7191
[3]nicka.medvedeva2020@yandex.ru✉, https://orcid.org/0009-0007-4326-8073
[4]veronika.k02@bk.ru, https://orcid.org/0009-0003-9513-5222

Аннотация. Обзор положений Указа Президента РФ № 166 от 30.03.2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». В статье рассматривается защита объектов критической информационной инфраструктуры на момент введения в действие Указа Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

***Ключевые слова*:** импортозамещение, критическая информационная инфраструктура, значимые объекты, указ, программное обеспечение,СОИБ ЗОКИИ.

В связи со сложившейся геополитической обстановкой многие организации в настоящее время сталкиваются с вынужденным импортозамещением. Некоторые иностранные решения, используемые в России, перестают полноценно функционировать, подписки на иностранное программное обеспечение не могут быть продлены, а обновления проблематичны [5].

Обзор положений Указа Президента РФ № 166

Начиная с 30 марта 2022 года, требования к критическим информационным инфраструктурам кардинальным образом изменились.Издан Указ Президента РФ № 166 от 30.03.2022 г. «О мерах по обеспечению технологической независимости и безопасности критическойинформационной инфраструктуры Российской Федерации» [1].

Данный Указ разработан в целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры.

Он запрещает закупку иностранного программного обеспечения для критической информационной инфраструктуры и требует от всех субъектов перехода на отечественное программное обеспечение и оборудование. В перечень объектов критической инфраструктуры (КИИ) Российской Федерации входят: государственные системы, предприятия оборонной промышленности, энергетики, топливной и атомной промышленности, транспорта и кредитно-финансовой сферы [2].

Указ полностью меняет всю структуру прежних требований и подходовк защите критически важных объектов КИИ.

1. С 31 марта 2022 года запрещает закупку иностранного программного обеспечения и программно-аппаратных комплексов, в целях использования на значимых объектах критической информационной инфраструктуры РФ. Исключения допускаются лишь по процедуре согласования [3].

2. С 1 января 2025 года государственным органам и заказчикам запрещает использовать иностранное программное обеспечение на собственных критически важных объектах КИИ. Вышеуказанные организации обязаны разработать планы импортозамещения для критически важных объектов.

3. Правительству Российской Федерации необходимо утвердить новые требования к программному обеспечению, а также правила согласования закупок иностранного программного обеспечения и закупок услуг, необходимых для использования этого программного обеспечения.

4. Правительству Российской Федерации требуется обеспечить преимущественное использование отечественного оборудования на значимых объектах критической информационной инфраструктуры.

Для гарантии безопасности объектов критической инфраструктуры необходимо создать систему обеспечения информационной безопасности значимых объектов КИИ, так называемую «СОИБ ЗОКИИ» [6].

Целью такой системы является организация устойчивого функционирования объектов КИИ. Средства и методы должны соответствовать категории значимости, необходимо следить за их адекватностью для противодействия текущим угрозам и угрозам завтрашнего дня. Процесс создания и функционирования СОИБ ЗОКИИ можно представить в виде алгоритма (рис. 1).

Рис. 1. Алгоритм создания и функционирования СОИБ ЗОКИИ

Согласно представленной методологии, этапом, предшествующим формированию СОИБ ЗОКИИ, является категорирование. Именно на этом этапе определяется необходимость создания СОИБ, выявляются объекты защиты, определяется их целевой уровень безопасности.

Следующей стадией идет непосредственно создание СОИБ ЗОКИИ, состоящее из четырёх этапов.

Этап 1. Планирование. На этапе планирования устанавливаются требования, которые необходимо выполнить для обеспечения безопасности каждого значимого объекта КИИ, и формируется план мероприятий.

Этап 2. Реализация. На данном этапе осуществляется внедрение организационных и технических мер, реализация плана мероприятий по обеспечению безопасности ЗОКИИ.

Этап 3. Мониторинг и контроль. Ключевым моментом для текущего этапа является аудит информационной безопасности. Его цель – определить, какое положение дел в области обеспечения ИБ существует сейчас и какие дальнейшие действия необходимо предпринять для создания либо улучшения системы защиты информации.

Этап 4. Совершенствование. Системы защиты должны противостоять угрозам как сегодняшнего, так и завтрашнего дня. Недостаточно просто внедрить процессы для обеспечения работы систем безопасности, но также следует постоянно совершенствовать процессы и повышать их зрелость.

В связи с глобальной политической и экономической ситуацией в мире, документы по КИИ и информационной безопасности постоянно изменяются и переписываются. Появляются новые рекомендации от ФСТЭК и ФСБ. Всем субъектам КИИ необходимо не только реализовать предлагаемые

рекомендации, но и построить полноценную систему безопасности [4].

Список источников

1. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»: официальный сайт. - Москва, 2022. URL.: http://publication.pravo.gov.ru/Document/View/0001202203300001?index=0&rangeSize=1 (дата обращения 05.03.2023).

2. Луийф Е. Безопасность критических информационных инфраструктур / Луийф Е., Жутауайте И., Хеммерли Б. М. // CRITIS 2018: 13-я Международная конференция. – Каунас, 2019 (дата обращения 05.03.2023).

3. Федеральный закон «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18.07.2011 N 223-ФЗ (последняя редакция): официальный сайт. URL.: https://www.consultant.ru/document/cons_doc_LAW_116964/ (дата обращения 06.03.2023).

4. Козырева, А. В. Защита объектов критической информационной инфраструктуры в 2022 году / А. В. Козырева // Вопросы устойчивого развития общества. – 2022. – № 5. – С. 1215-1223. (дата обращения 07.03.2023).

5. Елецкий, Е. Н. Импортозамещение объектов критической информационной инфраструктуры / Е. Н. Елецкий, К. А. Абоимов // Новейшие практики управления персоналом: материалы региональной студенческой конференции, Омск, 28 апреля 2022 года. – Омск: Омский государственный технический университет, 2022. – С. 22-27. (дата обращения 07.03.2023).

6. Безопасность объектов критической информационной инфраструктуры организации: официальный сайт. URL.: http://aciso.ru/files/docs/metodichka_2.0.pdf (дата обращения 09.03.2023).

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Мусиенко Н.О. – аспирант, ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Медведева В.Д. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03. – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Кузина В.В. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03. – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Мусиенко Н.О. – идея, сбор материала, обработка материала, частичное

написание статьи (25%).

Лысов Д.А. – написание статьи, научное редактирование текста (25%).

Медведева В.Д. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Кузина В.В. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 316:774

Реализация контроля технических каналов утечки информации, формируемых посредством аппаратных закладок

Вадим Александрович Наумчик[1]✉, Сергей Николаевич Горбунов[2], Роман Михайлович Башкиров[3], Юрий Юрьевич Громов[4]
[1,2,3]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[4]Тамбовский государственный технический университет, Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0002-4833-4870
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0009-7555-823X
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0001-4442-5217
[4]gromov@is.tstu.ru, https://orcid.org/0000-0003-3313-2731

Аннотация. В статье рассматривается одна из основных угроз безопасности информации - утечка информации по техническим каналам, создаваемым аппаратными закладками, дается их классификация, а также рассматриваются риски использования импортных микроэлектронных компонентов при производстве систем управления войсками и оружием.

Ключевые слова: утечка информации по техническим каналам; аппаратные закладки; радиоэлектронные средства; импортные микроэлектронные компоненты.

Целью комплексного технического контроля является определение достаточности и эффективности мероприятий по оперативной маскировке, выявление и принятие мер по закрытию технических каналов утечки информации, а также выявление и принятие мер по устранению нарушений установленных режимов и порядка использования радиоэлектронных средств и радиочастотного спектра.

Одной из основных задач комплексного технического контроля является проверка выполнения установленных норм и требований по противодействию техническим средствам разведки (в том числе при размещении радиоэлектронных средств (РЭС) гражданского назначения на территориях военных объектов), проведение проверок эффективности защиты информации, обрабатываемой на объектах технических средств передачи и обработки информации (ТСПИ), от утечки по техническим каналам. В соответствии с требованиями федеральных законов информация ограниченного доступа подлежит защите [1, 2]. Защита информации осуществляется путём принятия правовых, организационных и технических мер, направленных на предотвращение утечки информации, неправомерного воздействия на информацию (уничтожения, модифицирования (искажения, подмены) информации) и неправомерного блокирования доступа к информации.

К одной из основных угроз безопасности информации ограниченного доступа относится утечка информации по техническим каналам, под которой понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации.

На сегодняшний день самым распространенным и перспективным способом перехвата информации является применение аппаратных закладок.

Аппаратная закладка — устройство в электронной схеме, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных средств информационной системы [3]. Результатом работы аппаратной закладки может быть как полное выведение системы из строя, так и нарушение ее нормального функционирования, например несанкционированный доступ к информации, ее изменение или блокирование [5].

Также аппаратной закладкой может называться отдельная микросхема, несанкционированно подключаемая к атакуемой системе для достижения тех же целей. Аппаратные закладки можно классифицировать по различным основаниям (рис. 1) [5].

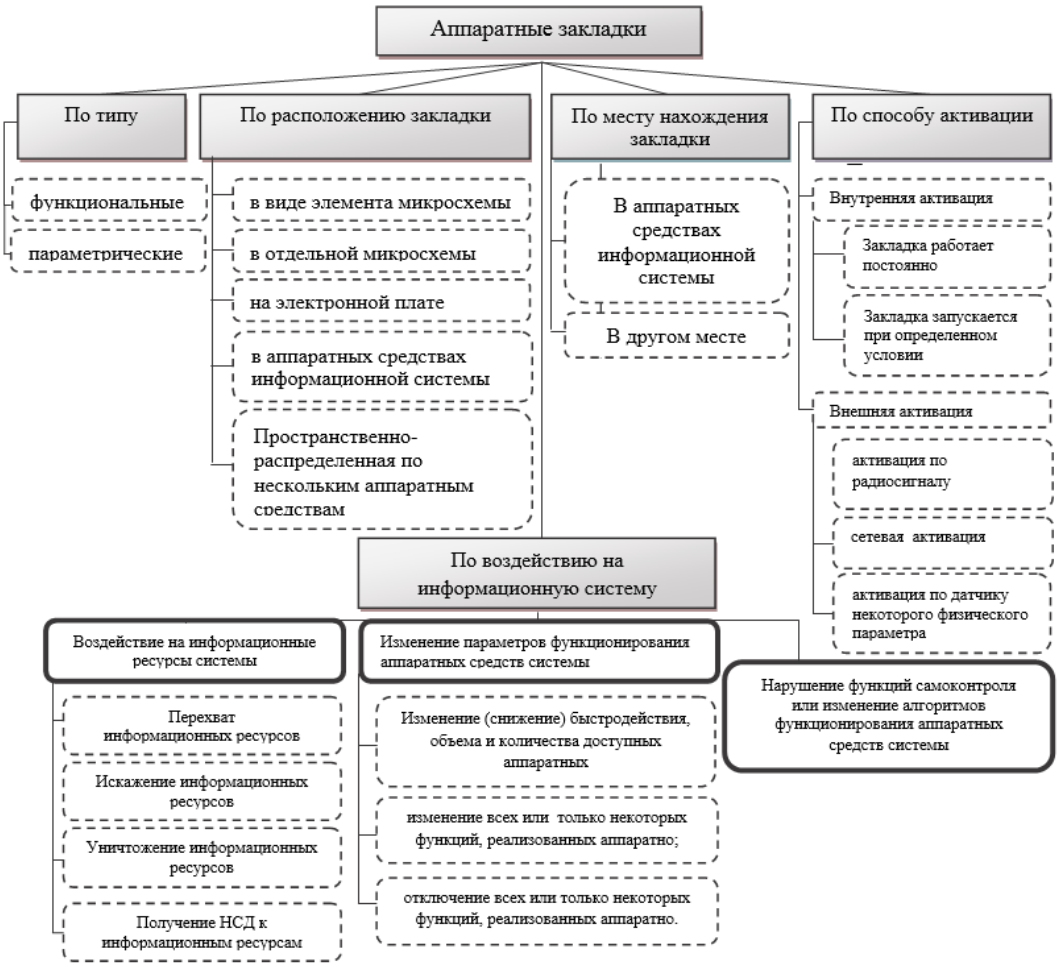

Рис. 1. Классификация аппаратных закладок

Схематическая сложность современного микроэлектронного оборудования, тенденции по миниатюризации его элементов ведут к тому, что

производители оборудования могут бескомпроматно и практически неограниченно наращивать функциональные возможности аппаратных закладок, а при подключении устройств к глобальной сети — осуществлять обновление алгоритма ихфункционирования, а также условий срабатывания.

Достижения в области разработки и внедрения аппаратных закладок напрямую связаны с научным заделом в области микроэлектроники, а также с мощностями электронной промышленности. В настоящее время такие страны, как США, Китай, Япония, в которых функционируют развитые производственные комплексы в области микроэлектронной и микропроцессорной техники, имеют потенциальную возможность встраивания аппаратных закладок в производимые ими на экспорт микроэлектронные компоненты [4]. В дальнейшем это позволит контролировать функционирование подавляющей части АСУ технологическими и критическими процессами, а также средств радиоэлектроники в других странах. При этом в отношении этих стран может быть реализован сценарий мгновенного вывода из строя их критической инфраструктуры за счет одновременного отключения входящих в ее состав микроэлектронных компонентов [6].

В связи с этим можно выделить следующие риски использования импортных микроэлектронных компонентов при производстве систем управления войсками и оружием [5]:

- встроенная технологическая и схемотехническая избыточность микроэлектронных компонентов, превышающая необходимый уровень для предоставления сервисов по прямому назначению, позволяет внедрять в них недекларированные функции, в том числе и враждебного характера;

- отсутствие технической документации на топологии микросхем и логику функционирования не позволяет в полной мере провести эффективный технический контроль наличия закладок;

- отсутствие гарантированно подтвержденной надежности микроэлектронных компонентов, а также их стойкости к воздействию электромагнитного оружия, позволит противнику эффективно применять это оружие против систем управления войсками и оружием. При этом противник может создать электромагнитную обстановку, гарантирующую выход из строя им же произведенных микроэлектронных компонентов.

В настоящее время фиксируются факты поставки в ВС России вычислительной техники, которая фактически произведена иностранным изготовителем, снабжена разнообразными аппаратными закладками (например, одновременно в BIOS-е и сетевой карте компьютера), однако которая, пройдя перемаркировку и установку отечественного ПО, считается де-юре «отечественного производства». При этом такие «отечественные производители», организующие подобные поставки, как правило, не имеют персонала должной квалификации для обнаружения и дезактивации встроенных в импортную технику аппаратных закладок, чем создают угрозу обороноспособности страны.

Список источников

1. Дождиков В.Г., Салтан М.И. Краткий энциклопедический словарь по информационной безопасности. М.: ИАЦ Энергия, 2010. 240 с.

2. Зайцев О. Современные клавиатурные шпионы // Компьютер Пресс. 2006. № 5. URL: http://compress.ru/article.aspx?id =15847.

3. Виноградов А.А. Функциональность, надежность, киберустойчивость в системах автоматизации критических инфраструктур // Конференция «Региональная информатика-2012». СПб.: ОАО «НПО «Импульс», 2012.

4. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. Санкт-Петербург. Наукоемкие технологии, 2017. 546 с.

5. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. – 2016. - № 3. – С. 292 – 376.

6. https://viperson.ru/uploads/attachment/file/950986/Makarenko_Ivanov_-_Netcentric_wars_2018.pdf#4.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Наумчик В.А. – оператор научной роты войск радиоэлектронной борьбы.

Горбунов С.Н. – старший оператор научной роты войск радиоэлектронной борьбы.

Башкиров Р.М. – младший научный сотрудник научной роты войск радиоэлектронной борьбы.

Громов Ю.Ю. – директор Института автоматики и информационных технологий.

Вклад авторов

Наумчик В.А. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Горбунов С.Н. – сбор материала, обработка материала, частичное написание статьи (25%).

Башкиров Р.М. – сбор материала, обработка материала, частичное написание статьи (25%).

Громов Ю.Ю. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 336.221

Интеграция смарт-контрактов в системы управления информационной безопасностью

Илья Сергеевич Новиков [1], Никита Сергеевич Ершов [2], Мустафа Абдулкадим Ал-Амееди[3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1] novikov.i.s2@edu.mirea.ru, https://orcid.org/0009-0005-1254-7227
[2] ershov@mirea.ru, https://orcid.org/0009-0009-3227-8326
[3] fit_tstu@mail.ru, https://orcid.org/0009-0002-1066-6650

Аннотация. В статье рассматривается интеграция смарт-контрактов в системы управления информационной безопасностью. Описываются основы работы смарт-контрактов, цели и задачи систем управления информационной безопасностью, а также области их соприкосновения. Статья обсуждает применение смарт-контрактов для автоматизации процессов управления безопасностью, контроля доступа, идентификации пользователей и управления инцидентами. Рассматриваются проблемы и вызовы, связанные с интеграцией смарт-контрактов, такие как технические и организационные препятствия, защита данных и приватности, а также нормативно-правовые аспекты.

Ключевые слова: смарт-контракты, информационная безопасность, блокчейн, управление доступом, идентификация пользователей, инциденты безопасности, реагирование на инциденты, прозрачность, доверие, интеграция, автоматизация, защита данных, приватность, нормативно-правовая база, стандарты, рекомендации, международное сотрудничество, организационные препятствия.

В эпоху цифровизации и развития блокчейн-технологий смарт-контракты стали важным инструментом автоматизации процессов и улучшения информационной безопасности. Цель данной статьи заключается в исследовании возможностей интеграции смарт-контрактов в системы управления информационной безопасностью и выявлении перспектив и вызовов, связанных с этим процессом. Актуальность темы обусловлена необходимостью поиска новых подходов к управлению информационной безопасностью, повышению прозрачности и доверия между сторонами, а также улучшению реакции на инциденты безопасности.

Смарт-контракты — это программные алгоритмы, запущенные на блокчейн-платформе, которые автоматически выполняются при наступлении определенных условий. Они основаны на следующих принципах:

— Децентрализация: смарт-контракты исполняются на распределенных

сетях, что исключает контроль одной стороны над контрактом и уменьшает риск мошенничества.

— Автономность: смарт-контракты самостоятельно выполняют заданные условия, без необходимости вмешательства сторон.

— Неизменность: данные, записанные в блокчейн, защищены от изменений и подделок благодаря криптографическим алгоритмам и консенсусным механизмам.

— Прозрачность: все стороны контракта могут видеть условия и состояние смарт-контракта, что обеспечивает открытость и доверие.

Системы управления информационной безопасностью (ИБ) направлены на защиту информационных активов организации от различных угроз. Основные цели и задачи систем ИБ включают:

— Защита конфиденциальности: предотвращение неправомерного доступа к чувствительной информации.

— Защита целостности: обеспечение точности и непротиворечивости информации, предотвращение ее несанкционированных изменений.

— Защита доступности: гарантия бесперебойного функционирования информационных систем и своевременного доступа к данным.

— Риск-ориентированный подход: определение и оценка рисков, адекватное управление ими и принятие мер по их снижению.

— Контроль и мониторинг: отслеживание активности пользователей и системы, обнаружение и реагирование на инциденты информационной безопасности.

Смарт-контракты и системы управления ИБ имеют несколько точек соприкосновения, связанных с общими принципами и целями:

— Автоматизация процессов: смарт-контракты могут быть использованы для автоматизации процессов управления информационной безопасностью, таких как контроль доступа, регистрация событий и управление инцидентами. Это позволяет сократить время реакции на инциденты, уменьшить вероятность ошибок и снизить затраты на управление безопасностью.

— Контроль доступа и идентификация пользователей: смарт-контракты могут быть применены для создания децентрализованных систем идентификации и аутентификации пользователей, что обеспечивает надежную защиту против несанкционированного доступа и утечки данных.

— Реагирование на инциденты: благодаря автоматическому исполнению условий смарт-контракты способны обеспечить быстрое реагирование на инциденты информационной безопасности, например, блокирование доступа или предоставление определенных привилегий при обнаружении аномальной активности.

— Прозрачность и доверие: смарт-контракты создают прозрачную и доступную среду для взаимодействия сторон, что позволяет обеспечить доверие между ними и контролировать соблюдение политик информационной безопасности.

— Защита данных и приватности: блокчейн-технология, лежащая в основе

смарт-контрактов, может обеспечить высокий уровень безопасности за счет криптографических методов шифрования данных и использования децентрализованных архитектур. Это помогает предотвратить мошенничество, хакерские атаки и другие угрозы.

Смарт-контракты могут быть использованы для автоматизации ряда процессов в системах управления информационной безопасностью, таких как контроль доступа, аудит, мониторинг и управление инцидентами. Благодаря автоматическому исполнению условий и возможности взаимодействия с другими системами, смарт-контракты обеспечивают более быстрое и надежное выполнение задач, снижая вероятность ошибок и затраты на управление безопасностью.

Так же Смарт-контракты могут играть ключевую роль в контроле доступа и идентификации пользователей. Они могут быть использованы для создания децентрализованных систем аутентификации и управления правами доступа, предоставляя гибкие и безопасные механизмы идентификации пользователей и контроля над доступом к ресурсам. Такие системы могут быть особенно полезны в условиях удаленной работы, когда традиционные методы аутентификации и авторизации могут быть недостаточно надежными.

Еще Смарт-контракты могут быть задействованы для управления инцидентами и реагирования на инциденты безопасности. В случае обнаружения аномальной активности или нарушения безопасности, смарт-контракты могут автоматически активировать предопределенные меры реагирования, такие как блокировка доступа, ограничение привилегий или уведомление ответственных лиц. Это позволяет сократить время реакции на инциденты и снизить риск дополнительных угроз.

Использование смарт-контрактов в системах управления информационной безопасностью может способствовать повышению прозрачности и доверия между сторонами. Благодаря прозрачности блокчейн-технологии, все стороны контракта могут видеть условия и состояние смарт-контракта, что обеспечивает открытость и доверие. Кроме того, смарт-контракты обеспечивают надежное и неизменное хранение информации, что позволяет контролировать соблюдение политик информационной безопасности и упрощает проведение аудита.

Но, к сожалению, сейчас существует несколько проблем интеграции смарт-контрактов в системы управления информационной безопасностью. Среди технических проблем стоит отметить сложность адаптации существующих систем к блокчейн-технологии, а также необходимость обеспечения совместимости между различными блокчейн-платформами и смарт-контрактами. Кроме того, вопросы приватности могут возникнуть в связи с тем, что данные в блокчейне, как правило, являются публичными и неподдельными. Нормативно-правовые аспекты также могут представлять вызов для интеграции смарт-контрактов в системы управления информационной безопасностью. Законодательство в области информационной безопасности и блокчейн-технологии продолжает развиваться, и в разных странах существуют различные подходы к регулированию этой сферы. Это может создавать правовую неопределенность и затруднять применение смарт-контрактов на

международном уровне.

В целом, интеграция смарт-контрактов в системы управления информационной безопасностью представляет собой сложную и многоаспектную задачу, требующую учета технических, организационных, правовых и этических факторов. Однако, несмотря на вызовы и проблемы, успешная интеграция смарт-контрактов может привести к значительным улучшениям в области информационной безопасности, обеспечивая более высокую степень автоматизации, прозрачности и доверия между участниками.

Список источников

1. Бутерин, В. (2013). Эфириум: Платформа децентрализованных приложений и смарт-контрактов нового поколения. Белая книга Ethereum. Получено из https://ethereum.org/ru/whitepaper/

2. Миллер, А., & Джулс, А. (2017). Смарт-контракты и компьютерная безопасность. IEEE Security & Privacy, 15(4), 76-82. doi: 10.1109/MSP.2017.3271458 (оригинал на английском языке)

3. Атцеи, Н., Бартолетти, М., & Чимоли, Т. (2017). Обзор атак на смарт-контракты Ethereum. В: Материалы 6-й международной конференции по принципам

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Новиков И.С.- студент кафедры КБ-1 «Защита информации», направления подготовки «10.03.01 – Информационная безопасность» РТУ «МИРЭА».

Ершов Н.С. - преподаватель кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Мустафа Абдулкадим Ал-Амееди - аспирант «ТГТУ».

Вклад авторов

Новиков И. С.- идея, сбор материала, обработка материала (60%).

Ершов Н.С. - написание статьи, научное редактирование текста (20%).

Мустафа Абдулкадим Ал-Амееди - частичное написание статьи (20%).

Конфликт интересов отсутствует.

Научная статья
УДК 621:396:41

Повышение информационной безопасности многофункциональной информационной системы «Наставник» за счет разграничения доступа и аутентификации

Елена Сергеевна Оверченко[1]✉, Константин Александрович Полкунов[2] Максим Михайлович Лазуткин[3], Николай Александрович Козлов[4]
[1]Южный федеральный университет, Таганрог, Россия
[2,3,4]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1]overchenko-elena@bk.ru✉, https://orcid.org/0009-0009-0208-9954
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0000-0541-8367
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0002-9741-6290
[4]nauchnajarota@yandex.ru, https://orcid.org/0000-0002-4194-6017

Аннотация. В статье описывается выбор модели безопасности для веб-приложения, а также обозреваются методы аутентификации и дается краткое представление о принципах их работы. В данной статье речь пойдёт о информационно-обучающей системе «Наставник» для подготовки специалистов средств радиоэлектронной борьбы. А в частности о проблемах информационной безопасности и подходах к их решению. В связи с развитием систем телекоммуникаций и веб-сервисов вопросы безопасности становятся все более актуальными и востребованными. Целью работы является выбор наиболее эффективного способа аутентификации и авторизации пользователей, а также создание модели разграничения доступа для многофункциональной информационной системы «Наставник».

Ключевые слова: модель разграничения доступа, аутентификация, авторизация.

Использование информационно-обучающей системы «Наставник» предполагает несколько категорий пользователей, таких как: обучаемые, преподаватели и разработчики. Которые в свою очередь должны иметь разный уровень доступа к определённым объектам информационной системы. Для решения данной задачи требуется создание модели разграничения доступа. В настоящее время основными моделями разграничения доступа являются дискреционная, мандатная и ролевая.

На данном этапе многофункциональная информационная система «Наставник» не имеет модели разграничения доступа, что создаёт некие трудности для контроля эффективности обучения.

Для повышения эффективности контроля учебного процесса используется система авторизации и регистрации пользователей. Рассмотрим основные компоненты этой системы. При нажатии на кнопку «начать тестирование»

пользователь переходит на страницу авторизации.

При успешной авторизации осуществляется переход на страницу с тестами. Проверка на подлинность пользователя и пароля осуществляется с помощью обращения к базе данных. База данных расположена на сервере и доступ имеет только администратор (рис. 1).

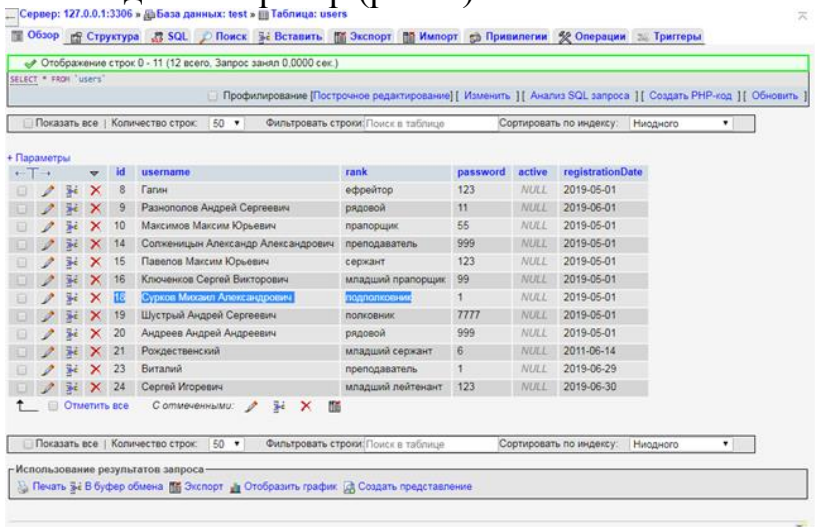

Рис. 1. Таблица «пользователи» из базы данных в формате SQL

Если пользователь не зарегистрирован, он может перейти на страницу регистрации. Если при регистрации или авторизации произошла какая-либо ошибка, появляются соответствующие информационные сообщения.

Возникает проблема контроля и отслеживания прогресса обучения военнослужащего. Решением которой является разграничение доступа и создание такой категории пользователей как преподаватели.

Рассмотрим наиболее известные модели разграничения доступа.

Дискреционные модели безопасности основаны на управлении доступа субъектов к объектам с помощью списков управления доступа или матрицы доступа [1].

Мандатное разграничение доступа – разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации содержащийся в объектах, и выдаче разрешений субъектам на обращение к информации такого уровня конфиденциальности. Реализация данных условий предоставляет невозможность возникновение информационных потоков от объектов с большим уровнем конфиденциальности к объектам с меньшим уровнем конфиденциальности [4].

Ролевое разграничение доступа является дальнейшим развитием политики дискреционного разграничения доступа: права доступа субъектов к объектам системы группируются по некоторым признакам, образуя роли.

Рассмотрев основные модели разграничения доступа, прослеживается вывод, что самой подходящей является модель мандатного разграничения доступа. Однако решив одну проблему, возникают новые трудности информационной безопасности в системе «Наставник». Способ аутентификации реализованный на данный момент не позволяет гарантировать безопасность информации подлежащей использованию только преподавательскому составу.

Аутентификация заслуживает особого внимания, когда речь идет о защите информации, поскольку ее задача – удостовериться, что пользователь действительно является тем, за кого себя выдает. Следующим этапом авторизация назначает пользователю его полномочия для действий в информационной системе [2]. В случае если эти права достанутся человеку, не имеющему данных полномочий, это может принести большие проблемы. Соответственно, необходимо решение, которое стабильно отличало бы нужного пользователя от всех остальных [5].

Однофакторная аутентификация [5].

В такой ситуации пользователю обычно нужно иметь при себе какое-либо устройство, позволяющее получать пароли, что неудовлетворительно в нашей ситуации, а система аутентификации значительно будет усложнена, так как хранить в базе данных постоянный пароль гораздо проще, чем генерировать его.

Для парольной защиты настоящим является тот пользователь, который знает условную комбинацию символов. Вполне очевидно, что этот вариант никак не гарантирует подлинности лица, допускаемого к работе с системой: достаточно узнать пароль тем или иным способом [5].

Цифровые сертификаты и ЭЦП

Цифровой сертификат – элемент криптографической защиты информации, электронное удостоверение, которое подтверждает, что открытый ключ шифрования принадлежит определенному пользователю. Электронная цифровая подпись также является средством аутентификации, так как среди ее функций есть подтверждение авторства: она удостоверяет, что документ действительно исходит от определенного лица и может рассматриваться как официальное выражение его намерений [5].

Аппаратные токены

Аппаратный токен – это устройство, предназначенное специально для аутентификации. В простейшем случае токен сам по себе является удостоверением, иначе говоря пользователь должен иметь его при себе и тем или иным образом предъявить системе – например, подключить к компьютеру или поднести к считывателю. В данном случае наиболее подходящим будут токены, которые генерируют одноразовые пароли для ввода вручную. Но стоит заметить, каким бы именно образом ни работал аппаратный токен, для системы будет подлинным тот пользователь, который держит устройство в руках [5].

Биометрия

Средства аутентификации, использующие биометрию, полагаются на параметры тела человека или на особенности его поведения. Таких параметров крайне много, начиная от печатного подчерка и заканчивая сканированием сетчатки глаза. Но стоит отметить, что неоспоримое качество аутентификации данного метода будет неоправданно затратно для системы «Наставник».

Многофакторная аутентификация

Основная идея двухфакторной аутентификации в том, чтобы слабые стороны одного метода аутентификации подкрепить сильными сторонами другого метода, что в свою очередь предоставляет качественную и стабильную работу.

Говоря о системе Наставник построенную на механизме паролей, которые пользователи должны помнить, можно усилить за счет аппаратных ключей, которые пользователи, имеющие доступ к информации с высоким уровнем конфиденциальности, должны иметь при себе. Тогда злоумышленник с токеном не будет знать пароля, а взломщик, укравший пароль, не будет иметь токена.

Список источников

1. Безуглая М.В., Патрушева О.М., Синадский Н.И., Сушков П.В. Расчет показателя сходства учетных записей пользователей социальных сетей на основе анализа атрибутов и структуры социальных связей // Безопасность информационного пространства, 2016. С. 19-23.

2. HTTP Authentication: Basic and Digest Access Authentication. URL: https://datatracker.ietf.org/doc/draft-ietf-http-authentication/03.

3. Девянин П.Н. Модели безопасности компьютерных систем: учебное пособие для студентов высшего учебного заведений: Академия, 2005. 144 с.

4. Кононов Д.Д., Исаев С.В. Расширенная ролевая модель безопасности, основанная на иерархии путей // Вопросы защиты информации. – 2016. - № 4 (115). – С. 13 – 18.

5. https://www.anti-malware.ru/analytics/Technology_Analysis/overview-of-user-authentication-systems-and-methods.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Оверченко Е.С. – ассистент кафедры лингвистического образования Южного федерального университета.

Полкунов К.А. – старший оператор научной роты войск радиоэлектронной борьбы.

Лазуткин М.М. – оператор научной роты войск радиоэлектронной борьбы.

Козлов Н.А. – оператор научной роты войск радиоэлектронной борьбы.

Вклад авторов

Оверченко Е.С. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Полкунов К.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Лазуткин М.М. – сбор материала, обработка материала, частичное написание статьи (25%).

Козлов Н.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.9

Оценка работоспособности электронной компонентной базы

Олеся Владимировна Оксюта [1]✉, Сергей Олегович Бучнев [2], Михаил Александрович Осипов [3], Павел Алексеевич Чубунов [4]
[1,2,3,4] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия
[1] kor_ole@mail.ru✉, https://orcid.org/0000-0003-1409-0842
[2] buchnevserega@yandex.ru, https://orcid.org/0000-0003-2407-23412
[3] osipovma@vglta.vrn.ru, https://orcid.org/0000-0003-3417-7315
[4] chu.p.@mail.ru, https://orcid.org/0000-0003-3414-4317

Аннотация. В статье рассматриваются методы испытаний на стойкость к воздействию излучения космического пространства по одиночным эффектам микросхем. Приводится алгоритм работы при испытаниях на воздействие тяжелых заряженных частиц. Рассматривается типовая последовательность действий при проведении испытаний цифровых сверхбольших интегральных микросхем на моделирующих установках.

Ключевые слова: испытания, радиация, микросхема.

В общем случае испытания электронной компонентной базы (ЭКБ) на стойкость к воздействию излучения космического пространства по одиночным эффектам проводятся в следующем составе и последовательности [1, 2, 3, 4, 5]:

- идентификация образцов ЭКБ;
- формирование выборки из работоспособных образцов изделий ЭКБ для испытаний;
- проведение облучений образцов в наихудших электрических режимах ионами требуемых характеристик и с контролем в процессе испытаний параметров и одиночных эффектов, обеспечивающих достоверность результатов испытаний;
- обработка экспериментальных данных;
- оформление результатов испытаний.

При этом типовая последовательность действий при проведении испытаний цифровых сверхбольших интегральных микросхем на моделирующих установках следующая [1, 2, 3, 4, 5, 6]:

1) Проведение идентификации образцов ЭКБ

2) Удаление крышек или части корпуса над полупроводниковыми кристаллами образцов СБИС (при необходимости);

3) Визуальный контроль поверхности кристаллов образцов СБИС с целью выявления возможных механических повреждений и наличия защитных покрытий из компаунда или лака;

4) Проведение контроля работоспособности образцов СБИС.

5) Подготовка оснастки для проведения испытаний на испытательной установке.

6) Прокладка линий связи (при необходимости) и проверка линий связи между испытываемыми изделиями в зоне облучения контрольно-измерительным и управляющим оборудованием.

7) Предварительный контроль параметров пучка протонов или ТЗЧ.

8) Установка образцов СБИС с оснасткой в зону облучения и проведение функционального и параметрического теста образцов СБИС в реальных условиях эксперимента, но в отсутствии действия излучения.

9) Установка средств мониторинга интегрального потока (флюенса) частиц (при необходимости).

10) Обеспечение необходимого разряжения в вакуумной камере зоны облучения (при необходимости).

11) Облучение образцов СБИС протонами или ТЗЧ.

12) Прекращение облучения, контроль радиационного фона и замена образцов СБИС.

13) Повторение процедур по 8–12 для новых значений энергий протонов или ЛПЭ ТЗЧ до окончания программы испытаний.

Основными источниками при испытаниях ЭКБ на стойкость к воздействию ИИ КП в части одиночных эффектов являются укорители протонов и ионов. Также допустимо использование источников фокусированного лазерного излучения при последующей калибровке по результатам испытаний на воздействие тяжелых заряженных частиц.

Список источников

1. Козюков А.Е. Общие подходы оценки стойкости к воздействию ионизирующего излучения космического пространства для зарубежной электронной компонентной базы предприятий –разработчиков / Козюков А.Е., Гамзатов Н.Г., Гречаный С.В., Зольников К.В., Струков И.И., Ачкасов А.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 58-66.

2. Козюков А.Е. Анализ потенциально возможных эффектов в ЭКБ от воздействия ИИ КП / Козюков А.Е., Чубунов П.А., Зольников К.В., Скворцова Т.В., Журавлева И.В. // Моделирование систем и процессов. 2021. Т. 14. № 2. С. 80-86.

3. Козюков А.Е. Экспериментально-аналитический метод оценки эффективности мер по повышению стойкости ЭКБ к воздействию ии кп по одиночным эффектам / Козюков А.Е., Чубунов П.А., Зольников К.В., Скворцова Т.В., Журавлева И.В. // Моделирование систем и процессов. 2021. Т. 14. № 2. С. 86-92.

4. Козюков А.Е. Классификация последствий воздействия ИИ КП на РЭА / Козюков А.Е., Чубунов П.А., Зольников К.В., Куцько П.П., Скворцова Т.В., Журавлева И.В. // Моделирование систем и процессов. 2021. Т. 14. № 3. С. 22-28.

5. Зольников В.К. Анализ чувствительности и результаты испытаний электронной компонентной базы к воздействию тяжелых заряженных частиц /

Зольников В.К., Ягодкин А.С., Анциферова В.И., Евдокимова С.А., Скворцова Т.В., Грошева Е.В. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 43-51.

6. Заревич А.И. Моделирование поведения мобильных роботов с использованием генетических алгоритмов / Заревич А.И., Макаренко Ф.В., Ягодкин А.С., Зольников К.В. // Моделирование систем и процессов. 2022. Т. 15. № 3. С. 7-16.

Статья поступила в редакцию 27.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Оксюта О.В. - к.т.н., доцент, и.о. зав. кафедрой, «Кафедра вычислительной техники и информационных систем» ФГБОУ ВО «ВГЛТУ».

Бучнев С.О. - преподаватель СПО кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Осипов М.А. - преподаватель СПО кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Чубунов П.А. - аспирант ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Оксюта О.В. - идея, сбор материала, обработка материала, научное редактирование текста

Бучнев С.О. - частичное написание статьи (25%).

Осипов М.А. - частичное написание статьи (25%).

Чубунов П.А. - частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 623:74

Организация специальных программных воздействий комплекса «Аналитик» с помощью устройств, переносимых на беспилотных летательных аппаратах

Илья Александрович Омельченко[1]✉, Сергей Николаевич Горбунов[2], Александр Александрович Гусев[3], Виктор Васильевич Шатских[4]
[1,2,3,4]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0002-5941-9589
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0009-7555-823X
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0002-9414-3290
[4]nauchnajarota@yandex.ru, https://orcid.org/0009-0009-7547-9419

Аннотация. Предлагается использование специального интеллектуального программного комплекса «Аналитик» в вопросах, касающихся организации специальных программных воздействий на условного противника, с целью перехвата аутентификационных данных посредством обеспечения мобильности программного комплекса размещая беспилотных летательных аппаратах.

Ключевые слова: интеллектуальный программный комплекс, специальные воздействия, атаки.

Одно из важнейших направлений в современной авиации связано с применением беспилотных летательных аппаратов (БПЛА), первые образцы которых появились еще в середине прошлого века, как отдельный вид перспективного оружия. В настоящее время БПЛА различных типов и назначения не только стоят на вооружении многих армий мира, но и начинают активно использоваться в гражданской сфере [5]. В данной статье предлагается развитие БПЛА для проведения специальных программных воздействий унифицировано на системы посредством вторжения в устройства по беспроводному каналу. Таким образом будет обеспечиваться мобильность платформы для проведения подобных атак на сетевые и ЭВМ объекты условного противника.

Специальный интеллектуальный программный комплекс аналитик предлагается доукомплектовать дроном и перенести на мобильную платформу сохранив все функциональные возможности. Схема соединения комплектующих представлена на рис. 1.

Рис. 1. Схема соединения комплектующих

На рис. 1 были представлены следующие комплектующие:

1) беспилотный летательный аппарат;

2) Raspberry Pi;

3) Edimax EW-7811Un беспроводной адаптер сети.

4) Alfa AWUS036H беспроводной адаптер сети.

В качестве беспилотного летательного аппарата достаточно использование Parrot AR.Drone 2, так как вес общей оснащенной конструкции составляет примерно 109 г. Кроме того, данная сборка, позволяет минимизировать потери маневренности используемого дрона и потери скорости полета на дополнительный вес оборудования, в связи с чем от дрона не требуется больших мощностей двигателей. Такой размер дрона позволит оставаться малозаметным при перемещения комплекса по воздушному пространству [1].

В связи с тем что комплекс «Аналитик» разработан на базе фреймворка Qt Creator и ядро RaspberryOS позволяет воспроизводить .exe файлы, то предлагается в качестве вычислительной платформы использовать плату Raspberry Pi.

Edimax EW-7811Un является адаптером беспроводного соединения и позволяет по отдельному соединению иметь возможность управлять интеллектуальным программным комплексом «Аналитик» удаленно по протоколу RDP или SSH.

Alfa AWUS036H – это беспроводной двудиапазонный адаптер сети, который работает на частоте 2.4 GHz и 5 GHz, способен работать в режиме монитора чтобы проводить атаки связанные с перехватом handshake-ов, для дальнейшего дешифрования ключа WPA и получения соединения с точкой. Кроме того программный модуль «Аналитик» способен проводить смену MAC-адреса для получения доступа к точке под видом верифицированного пользователя. Возможность работать в двух диапазонах позволяет так же генерировать поддельную беспроводную точку, на программном уровне возможно подобрать на поддельную точку SSID равный SSID-у доверенной точки для условного противника, при том используя второй диапазон для

подавления канала изначальной точки, что открывает возможность для проведения атак относящихся к социальной инженерии [2, 3].

В данной работе для специального программного воздействия предлагается использовать программный комплекс «Аналитик». В отличие от существующих сканеров сетевой безопасности, программный комплекс имеет следующие преимущества [6]:

– обнаружение скрытых точек доступа и абонентских терминалов беспроводных сетей, подключённых к ним;

– подбор WEP, WPA-PSK ключей аутентификации беспроводных сетей стандарта 802.11;

– определение уязвимостей программного и аппаратного обеспечения сканируемого объекта;

– проведение атак на РЭО условного противника.

Рассмотрим часть разрабатываемых модулей программного комплекса.

Взаимодействие посредством беспроводных сетей в комплексе «Аналитик» разработан модуль сканирования Wi-Fi, который позволяет выполнять поиск и обнаружение скрытых точек доступа и подключённых к ним абонентских терминалов. Модуль выполняет перехват данных, передаваемых по беспроводным сетям стандарта 802.11 и определяет используемый тип шифрования. В процессе работы модуль отображает уровень сигнала беспроводной сети, скорость передаваемых данных и используемый канал.

Для определения ключа шифрования данных, собранных модулем сканирования Wi-Fi, используется модуль подбора ключей аутентификации. В процессе аудита используются уязвимости в протоколах обеспечения безопасности беспроводной передачи данных, а именно WEP и WPA-PSK [6].

Для организации специальных программных воздействий разрабатывается модуль «Атаки», с помощью которого можно провести атаку и подтвердить выявленную уязвимость. В модули реализованы способы атаки типа «Посредник», также реализован анализатор трафика.

Для просмотра, проходящего трафика можно использовать встроенный анализатор трафика в программном комплексе «Аналитик». Анализатор трафика или сниффер – это программа для перехвата и анализа своего или чужого, проходящего трафика через сетевую карту радиоэлектронного объекта выбранного интерфейса [4]. Анализатор в программном комплексе имеет возможность сохранять и загружать сессию в формате pcap, также установить в фильтре количество считываемых пакетов и направление обработки трафика (входящий, исходящий, входящий-исходящий). Для обработки более узкой направленности захвата, можно воспользоваться фильтром выражений, портов и хостов. Данные фильтры можно комбинировать с помощью логических операторов AND, OR и NOT. В таблицу выводится следующая информация о перехваченных пакетах: время перехвата, адрес источника и адрес назначения, протокол и размер пакета.

Разработанный программный комплекс позволяет ускорить процесс анализа уязвимостей в используемом аппаратном и программном обеспечении сетевой информационной системы бортового оборудования воздушных судов,

что оказывает существенное влияние на управление информационной безопасностью.

Список источников

1. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна // Вопросы кибербезопасности, 2018. № 4. С. 920.

2. Уолтон Ш. Создание сетевых приложений в среде Linux. Издательский дом «Вильямс», 2001. 464 с.

3. Бабин С.А. Инструментарий хакера. СПб.: БХВ-Петербург, 2015. 240 с.

4. Бабин С.А. Лаборатория хакера. СПб.: БХВ-Петербург, 2016. 240 с.

5. Лохин В.М., Манько С.В., Романов М.П., Гарцеев И.Б., Колядин К.С. Тенденции развития беспилотных летательных аппаратов мини- и микроклассов // Нано- и микросистемная техника. – 2005. - № 2. – С. 44 – 48.

6. Верещагин Д. Ю., Семисчастнов А. Е. Научная рота в сфере обеспечения информационной безопасности (на примере интеллектуального программного комплекса «Бастион») // Тамбовские правовые чтения имени Ф. Н. Плевако. – Тамбов, 2021. – С. 344 – 350.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Омельченко И.А. – старший оператор научной роты войск радиоэлектронной борьбы.

Горбунов С.Н. – старший оператор научной роты войск радиоэлектронной борьбы.

Гусев А.А. – младший научный сотрудник научной роты войск радиоэлектронной борьбы.

Шатских В.В. – старший научный сотрудник научной роты войск радиоэлектронной борьбы.

Вклад авторов

Омельченко И.А. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Горбунов С.Н. – сбор материала, обработка материала, частичное написание статьи (25%).

Гусев А.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Шатских В.В. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Классификация методов противодействия фишингу

Данила Викторович Поддубный [1]✉, Дмитрий Юрьевич Смыков [2], Дмитрий Андреевич Лысов [3], Алексей Максимович Гулак [4]
[1,2,3,4] Брянский государственный технический университет, Брянск, Россия
[1]danila.poddubnyy@mail.ru ✉, https://orcid.org/0009-0003-8332-7542
[2]uselessbiotrash@gmail.com, https://orcid.org/0009-0001-0719-7665
[3]lysovdmitriia@gmail.com, https://orcid.org/0009-0003-9666-7191
[4] gml13@yandex.ru✉, https://orcid.org/0009-0005-1253-4303

Аннотация. В статье рассмотрены методы противодействия фишинговым атакам. Выделено значение данного явления. Приведена статистика фишинга за 2022 год.

Ключевые слова: информационная безопасность, фишинг, методы противодействия фишингу.

Фи́шинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям [5.5].

В современном мире с развитием технологий повлекло за собой как положительные так и отрицательные стороны. Было создано множество систем защиты от угроз информационной безопасности, но по статистике за 2022 год самой большой угрозой стал человеческий фактор. Поэтому фишинг в современном мире является одной из основных угроз в сфере информации.

Согласно данным сайта Securelist компании «Лаборатория Касперского» в 2022 году:

1. 48,63% писем по всему миру и 52,78% писем в Рунете были спамом.
2. Из России исходило 29,82% всех спамовых писем.
3. Наш почтовый антивирус заблокировал 166 187 118 вредоносных почтовых вложений.
4. Система «Антифишинг» предотвратила 507 851 735 попыток перехода по фишинговым ссылкам.
5. 378 496 попыток перехода по фишинговым ссылкам были связаны с попытками угона Telegram-аккаунтов.

Можно выделить некоторые методы по предотвращению и обеспечению защиты от фишинговых атак.

Обучение персонала

Обучить сотрудников компании это самый важный аспект в защите от фишинга.

Необходимо проводить регулярный инструктаж для сотрудников организации на тему фишинга. Особенно следует уделить внимание почтовым письмам и разъяснить критерии по которым можно отличить письмо от мошенников.

Критерии:

1. Сокращение ссылок.
2. Орфография, опечатки и многочисленно использование знаков вопроса или восклицания.
3. Угрозы.
4. Упоминания срочных сроков в письме.
5. Просьбы предоставить ваши конфиденциальные данные.

Двухфакторная аутентификации

Одним из надёжных средств защиты от фишинга является двухфакторная аутентификация. Она поможет защитить ваши данные в случае если злоумышленник получил пароль от вашей учётной записи. Двухфакторная аутентификация работает по принципу генерирования случайных кодов, которые приходят вам в SMS или на приложение в телефоне. Рекомендуется использовать приложение для двухфакторной аутентификации это более надёжный метод по сравнению с SMS.

Системы резервного копирования

Системы резервного копирования представляют собой комплекс программного и аппаратного обеспечения, который служит для создания копий данных на носителе, который предназначен для восстановления информации в случае её утраты или искажения. Рекомендуется делать регулярную копию данных для обеспечения сохранения информации.

Антивирусные программы

Самым банальным, но одним из самых эффективных средств защиты от фишинга будет является антивирус. Антивирусная программа будет являться хорошим средством блокирующим переход по вредоносным ссылкам или в случае блокировки и уничтожения скачиваемого вредоносного ПО. Хорошим решением в данном случае будет Kaspersky Internet Security

Настройка браузера

Настроить браузер сотрудников это одна из основных задач при защите от фишинга. Необходимо ограничить доступ сотрудникам в интернет пространстве и добавить блокировку перечня веб–сайтов, относящихся к мошенникам.

Спам фильтры

Спам фильтр - это программа предназначенная фильтрации электронных писем. Она определяет интересно ли письмо пользователю, если нет то письмо отправляется в спам или же полностью удаляется.

Сетевые экраны

Сетевые экраны предназначены для ограничения входящего, исходящего и внутреннего трафика сети. Сетевой экран принимает решение пропускать или же заблокировать проходящий пакет данных. Основная функция блокировать вредоносные активности и предотвращать несанкционированные действия в сети.

Одноразовые пароли

Одноразовый пароль – это пароль, действующий для одной аутентификации. Одноразовые пароли хороши тем, что в случае перехвата пароля злоумышленником пароль для аутентификации будет или уже изменён или недействителен. Благодаря этому злоумышленник не сможет попасть в систему даже узнав пароль.

Если вы все-таки стали жертвой интернет мошенников, то рекомендуется выполнять следующие действия. МВД разработало алгоритм действия для граждан, которые пострадали от действий злоумышленников [5.5]:

1. Первое действие после того, как вы недосчитались на своем банковском счете некоторой суммы, – это отключить смартфон и вытащить из него сим-карту.
2. Далее следует как можно скорее связаться с банком и отозвать денежный перевод, а заодно блокировать все возможные действия с расчетным счетом.
3. Написать заявление в двух экземплярах об отзыве платежа, возврате средств и блокировании доступа к системе «Мобильный банк». Предоставить заявление в банк необходимо в течение одного дня с момента атаки интернет-мошенников.
4. Также необходимо получить в банке детализацию с расчетного счета и обратиться в банк, в который ушли деньги по инициативе злоумышленника, с заявлением о приостановке исполнения платежа и возврате средств.
5. И наконец, написать заявление о факте хищения денежных средств, которое необходимо предъявить в полицию. Для оформления дела понадобится документальное подтверждение хищения денежных средств: выписка из банка, детализация расходов и т. д.

Главной защитой от фишинговых атак на данный момент являются ваши знания и внимательность.

Список источников

1. Данько, О. С. Исследование техник фишинга и методов защиты от него / О. С. Данько, Т. А. Медведева // Молодой исследователь Дона. – 2021. – № 3(30). – С. 60-66. – EDN FSXVIO.
2. Енин, В. М. Фишинг как угроза нового поколения / В. М. Енин, И. А. Матющенко // International Journal of Advanced Studies in Computer Engineering. – 2021. – № 2. – С. 31-37. – EDN MMIRXB.
3. Сазонова, Е. С. Фишинг как вид интернет-мошенничества / Е. С. Сазонова, А. В. Головин // Наука молодых - будущее России : сборник научных статей 4-й Международной научной конференции перспективных разработок молодых ученых. В 8-ми томах, Курск, 10–11 декабря 2019 года / Ответственный редактор А.А. Горохов. – Курск: Юго-Западный государственный университет, 2019. – С. 156-158. – EDN UMAYMF.
4. Спам и фишинг в 2021 году. URL: https://securelist.ru/spam-and-phishing-in-2021/104407/ (дата обращения: 20.11.2022).

5. Чернышева А.А., Самойлов С.И. Фишинг как угроза современному информационному обществу // Научный потенциал. – 2021. - № 3 (34). – С. 131 – 136.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Поддубный Д.В. – студент кафедры «Информационной безопасности», направление подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Смыков Д.Ю. – студент кафедры «Информационной безопасности», направление подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Гулак А.М. – студент кафедры «Компьютерные технологии и системы», направление подготовки «10.05.04 – Информационно-аналитические системы безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Поддубный Д.В. – сбор материалов, редактирование текста, частичное написание статьи (25 %).

Смыков Д.Ю. – идея, сбор материалов, обработка материалов, частичное написание статьи (25 %).

Лысов Д.А. – частичное написание статьи, научное редактирование текста (25%).

Гулак А.М. – обработка материалов, частичное написание статьи (25 %).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.5

Использование технологии OCR (optical character recognition) для распознавания текста в программах, написанных на C#

Александр Владимирович Полуэктов[1]✉, Антон Иванович Заревич[2], Филипп Владимирович Макаренко [3]
[1, 2, 3]Воронежский государственный лесотехнический университет имени Г.Ф. Морозова, Воронеж, Россия
[1]palv2006@yandex.ru✉, http://orcid.org/0009-0005-4032-5031
[2]antonzarevich@ngs.ru, https://orcid.org/0009-0000-5354-5598
[3]Phillipp@mail.ru, https://orcid.org/0009-0001-9311-8942

Аннотация. В статье рассматриваются история, теоретическая база построения технологии OCR (optical character recognition). Определяется программный аппарат, который используется при разработке программ с использованием OCR. Выполняется рассмотрение и сравнение библиотек для разработки программ с технологией OCR на C# и определяются методики работы с OCR на этапах разработки программы. Выполняется проектирование программы в среде программирования Visual Studio с использованием пакета Tesseract.

Ключевые слова: технологии OCR, язык программирования C#, пакет Tesseract.

OCR или Optical Character Recognition является технологией, которая позволяет компьютеру распознавать текст на изображениях и сканированных документах. Она широко используется во многих приложениях, таких как автоматическое заполнение форм, распознавание номеров автомобильных номеров и многое другое [2].

OCR разрабатывался с середины 20-го века. Первые устройства для чтения текста были созданы для людей с нарушениями зрения. В 60-е годы функциональность была расширена с помощью компьютерных технологий, что сделало распознавание текста доступным на множестве платформ.

С 1974 года стандарт оцифровки текстов с использованием OCR был принят почтовыми службами мира [4]. Направления использования:

1. Документационное обеспечение
2. Библиотечное дело и архивирование
3. Банковское и страховое дело
4. Почтовые и транспортные услуги

Некоторые из самых популярных библиотек программирования, используемых для разработки OCR-приложений, включают Tesseract, OCRopus, Abbyy и Google Cloud Vision.

Разработка программного обеспечения на языке C# используя OCR-технологию может быть построена с использованием двух направлений: использование локальной библиотеку и использование онлайн сервиса. Рассмотрим пример создания программы на C#, которая позволяет распознавать текст на изображениях [1].

C# предоставляет несколько библиотек для реализации OCR. Некоторые популярные библиотеки:

- Tesseract (https://github.com/charlesw/tesseract) - это одна из самых популярных и точных библиотек OCR. Tesseract создан компанией Google и является открытым программным обеспечением с большим сообществом разработчиков.
- IronOCR (https://ironsoftware.com/csharp/ocr/) - это коммерческая библиотека для OCR на C#. IronOCR предлагает набор разнообразных функций для распознавания текста на изображениях и поддерживает множество языков.

Рассмотрим использование библиотеки Tesseract. Для этого необходимо установить эту библиотеку и написать код на C#, который загружает изображение и передает его в Tesseract для распознавания текста. Ниже приведен пример кода на C#, использующего библиотеку Tesseract [3]:

```
using Tesseract;
public string RecognizeText(string imagePath)
{
    using (var engine = new TesseractEngine(@"./tessdata", "eng", EngineMode.Default))
    {
        using (var img = Pix.LoadFromFile(imagePath))
        {
            using (var page = engine.Process(img))
            {
                var text = page.GetText();
                return text;
}}}
}
```

Приведенный выше код создает новый экземпляр объекта Tesseract с указанным языком и моделью, загружает изображение из файла, обрабатывает его и выводит распознанный текст в консоль. Замените `imagePath` на путь к вашему изображению и `tessDataPath` на путь к каталогу tessdata, который содержит языковые модели Tesseract.

Второй вариант, с использованием онлайн-движки OCR, которые обычно предоставляют API, которые позволяют разработчикам интегрировать эту функцию в свои приложения. Для использования таких API вам нужно регистрироваться и получать уникальный API-ключ, который используется в вашем коде программы [4].

Для работы в C#, используйте следующие библиотеки:

- Google.Cloud.Vision.V1 для Google Cloud Vision OCR

- Microsoft.Azure.CognitiveServices.Vision.ComputerVision для Microsoft Azure Computer Vision OCR
- ABBYY.CloudSdk.V2.Client для Abbyy Cloud OCR SDK

Пример программы на C#, которая использует Google Cloud Vision OCR:

```
using Google.Cloud.Vision.V1;
using System;
class Program
{
   static void Main(string[] args)
   {
// Установите переменную среды GOOGLE_APPLICATION_CREDENTIALS с путем к файлу JSON с ключом API
Environment.SetEnvironmentVariable("GOOGLE_APPLICATION_CREDENTIALS", "path/to/your/apikeyfile.json");
      // Создайте клиента OCR
      var client = ImageAnnotatorClient.Create();
      // Загрузите изображение с текстом
      var image = Image.FromFile("path/to/your/image.jpg");
      // Выполните распознавание текста
      var response = client.DetectText(image);
      // Выведите распознанный текст на экран
      foreach (var annotation in response)
      {
         Console.WriteLine($"Description: {annotation.Description}");
         Console.WriteLine($"Bounding Poly: {annotation.BoundingPoly}");
   }}
}
```

Не забудьте заменить `path/to/your/apikeyfile.json` на путь к файлу с ключом API и `path/to/your/image.jpg` на путь к изображению, которое вы хотите распознать. Обратите внимание, что перед использованием библиотеки Google.Cloud.Vision.V1 необходимо установить.

Аналогичным образом, вы можете использовать и другие OCR-движки, заменяя клиента и библиотеку на соответствующие им.

Выводы

Таким образом, использование локальных библиотек или онлайн-движки OCR позволит внедрить идею распознавания текста в разработку программного обеспечения, а использование выбранной технологии зависит только от потребности заказчика ПО или желания разработчика.

Список источников

1. Classification Features / G. Sidorov, F. Velasquez, E. Stamatatos, A. Gelbukh, L. Chanona-Hernández, Springer LNAI 7630, Mexico, 2012. pp. 1-11.

2. Szarvas, M. Finite-state transducer based modeling of morphosyntax with applications to Hungarian LVCSR / M. Szarvas, S. Furui // Proc. ICASSP’2003, Hong Kong, China, 2003. pp. 368–371.

3. Руководство по использованию Google API. – URL:: https://developers.google.com/web/updates/2013/01/Voice-Driven-Web-Apps-Introduction-to-the-Web-Speech-API (дата обращения: 05.03.2023).

4. Карпов, А.А. Методология оценивания работы систем автоматического распознавания речи/ А.А. Карпов, И.С. Кипяткова, // Известия вузов. Приборостроение, Т. 55, № 11, 2012, С. 38-43.

Статья поступила в редакцию 27.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Полуэктов А.В. - преподаватель базовой кафедры технического и программного обеспечения вычислительных и информационных систем ФГБОУ ВО «ВГЛТУ».

Заревич А.И. - к.т.н., базовой кафедры технического и программного обеспечения вычислительных и информационных систем ФГБОУ ВО «ВГЛТУ».

Макаренко Ф.В. - к.ф.-м.н., базовой кафедры технического и программного обеспечения вычислительных и информационных систем ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Полуэктов А.В. - идея, сбор материала, обработка материала, написание статьи (80%).

Заревич А.И. - частичное написание статьи, научное редактирование текста (20%).

Макаренко Ф.В. – подготовка иллюстрирующих материалов и табличных данных (10%).

Конфликт интересов отсутствует.

Научная статья
УДК 004:056

Разработка рекомендаций для эффективного реагирования на инциденты информационной безопасности

Полина Николаевна Полякова[1], Максим Михайлович Голембиовский[2], Екатерина Владимировна Кондрашова [3]
[1,2,3]Брянский государственный технический университет, Брянск, Россия
[1]polyakova.polina@yandex.ru✉
[2]maksim32region@yandex.ru✉
[3]kondrashova_katerina@bk.ru✉

Аннотация. Меры противодействия инцидентам информационной безопасности с каждым годом становятся более актуальными. При проектировании системы безопасности предприятия зачастую трудно предусмотреть все возможности взлома. Это особенно актуально, если само предприятие и его инфраструктура достаточно велики и не сосредоточены на одной территории.

Ключевые слова: информационная безопасность, инциденты, SIEM-система.

Вопрос противодействия инцидентам информационной безопасности становится все более актуальным с каждым годом. Это происходит в связи с развитием информационных технологий в целом и наращиванием доступности технических средств реализации кибератак, а также обучающих материалов и инструкций как это можно сделать.

При проектировании системы защиты предприятия очень часто бывает затруднительно предусмотреть все возможные варианты нелегитимного проникновения в систему. Особенно, если само по себе предприятие и его инфраструктура достаточно обширны и не локализуются в пределах одной территории.

В сложившихся условиях особую важность приобретает не только процесс общей защиты от реализации инцидентов ИБ, но и процесс реагирования и расследования в случае попытки их реализации.

Одной из самых эффективных технологий отслеживания инцидентов информационной безопасности, не имеющей на данный момент равных аналогов, является SIEM-система.

SIEM-система представляет собой объединение систем управления информационной безопасностью (SIM) и управления событиями безопасности (SEM) в единую систему управления безопасностью. SIEM-системы в качестве самостоятельного решения не предназначены и не способны предотвращать инциденты нарушения информационной безопасности [1].

Преимущество SIEM-системы в том, что она способна непрерывно анализировать все сетевые события применительно ко всем имеющимся объектам сетевой инфраструктуры. В случае если системой обнаружены какие-то нетипичные события, она формирует сообщение об инциденте пользователю, что позволяет своевременно проверить сигнал и предотвратить реализацию инцидента вообще или минимизировать последствия от тех действий, которые злоумышленник успел реализовать.

Одной из наиболее приоритетных среди существующих является SIEM-система Wazuh. Ее преимущество состоит в том, что это бесплатное решение с открытым исходным кодом, которое может быть доработано и развито под нужды любой организации. Стоимость всех представленных на российском рынке систем превышает 15 миллионов рублей. И если для крупномасштабных организаций эта стоимость является средней, то для небольших предприятий она неподъемна. Такими предприятиями и может использоваться SIEM-система Wazuh, которая при минимальных (относительно стоимости других решений) вложениях в доработку, позволит отслеживать сетевые события.

Помимо систем данного типа есть различные программы и утилиты позволяющие специалистам по информационной безопасности в организации собственными силами провести процедуру расследования инцидента и в соответствии с полученными результатами принять адекватные меры по реагированию.

В данный перечень входят сканеры открытых портов, утилиты для программного восстановления данных с различных носителей информации, утилиты для получения данных о подключаемых внешних носителях, утилиты для захвата физической памяти компьютера, с целью ее дальнейшего анализа, утилиты, с помощью которых можно получить информацию о запущенных процессах и службах, управлять ими, запускать или завершать процессы, программы для поиска руткитов.

В табл. 1 представлен перечень конкретных средств каждого класса, рекомендуемых для внедрения на объектах.

Таблица 3

Перечень рекомендованных средств для реагирования на инциденты ИБ

Класс и назначение средства	**Возможные варианты**
SIEM-система – предоставляет исходную информацию о сетевых событиях	Wazuh, Security Onion, Open Search
Сканеры открытых портов – позволяют увидеть через какие каналы злоумышленник мог проникнуть в систему	Nmap, Acunetix, Netstat, Shodan.io
Утилиты для программного восстановления данных с различных носителей информации	R-saver, Hatman Recovery
Утилиты для получения данных о подключаемых внешних носителях	Windows USB Storage Parser, USB dewiev

Утилиты для захвата физической памяти компьютера, с целью ее дальнейшего анализа	MAGNET RAM Capture, The SIFT Workstation
Утилиты, с помощью которых можно получить информацию о запущенных процессах и службах, управлять ими, запускать или завершать процессы	PSTools, Process Monitor, Process Explorer, AutoRuns
Программы для поиска руткитов. (Руткит – вредоносная программа для получения злоумышленниками прав суперпользователя на устройстве без ведома жертвы)	RootkitRevealer, BackLite

Таким образом, внедрив рекомендованные в рамках статьи решения на объекте, организации удастся обеспечить максимально эффективное и оперативное реагирование на инциденты информационной безопасности, что в последствии поможет минимизировать их количество и улучшить общие показатели защищенности обрабатываемой информации.

Список источников

1. Абденов А.Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / Абденов А.Ж., Трушин В.А., Сулайман К.. — Новосибирск : Новосибирский государственный технический университет, 2018. — 122 с. — ISBN 978-5-7782-3603-5. — URL: https://www.iprbookshop.ru/91179.html (дата обращения: 13.03.2023).

Статья поступила в редакцию 10.04.23; принята к публикации 10.05.2023.

Информация об авторах

Полякова П.Н. – студент кафедры «Системы информационной безопасности», направление подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Голембиовский М.М. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Кондрашова Е.В. – студент кафедры «Системы информационной безопасности», направление подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Полякова П.Н. – идея, сбор материала, частичное написание статьи (40%).

Голембиовский М.М. – идея, научное редактирование текста, частичное написание статьи (35%).

Кондрашова Е.В. – идея, сбор материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК: 004.056.53

Требования к сложности паролей и анализ методов парольной защиты

Николь Дмитриевна Потапова[1]✉, Максим Алексеевич Гладышев[2], Никита Сергеевич Ершов[3], Мустафа Абдулкадим Ал-Амееди[4]
[1, 2, 3] МИРЭА - Российский технологический университет, Москва, Россия
[4]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1] potapova.n.d@edu.mirea.ru ✉, https://orcid.org/0009-0004-0395-515X
[2] gladyshev.m.a@edu.mirea.ru, https://orcid.org/0009-0001-4604-7125
[3] ershov@mirea.ru, https://orcid.org/0009-0009-3227-8326
[4] fit_tstu@mail.ru, https://orcid.org/ 0009-0002-1066-6650

Аннотация. Парольная защита является важным аспектам безопасности в сети Интернет. Пароли используются для защиты личной информации, включая логины, электронную почту, социальные сети, онлайн-банкинг и многое другое. Хороший пароль — это первый шаг к безопасности в Интернете, и в этой статье мы рассмотрим, как создать и использовать пароли для максимальной защиты.

Ключевые слова: парольная аутентификация, пароли, информационная безопасность, защита информации.

Парольная аутентификация стала неотъемлемой частью нашей жизни, оставаясь наиболее простой и распространенной. Однако, слишком простые пароли или неправильное использование могут позволить злоумышленникам легко получить доступ к конфиденциальной информации, особенно учитывая риски дешифровки хешей паролей с помощью радужных таблиц, брутфорсинга или переборам по словарям. Для примера из утекшей базы Sony Pictures порядка 82% хешей паролей легко взламываются через радужные таблицы, а по исследованиям Технологического института (штат Джорджия США) на взлом восьмизначного пароля, при использовании группы видеокарт, достаточно всего двух-трех часов. Поэтому подходить к вопросу создания пароля нужно вдумчиво и осознанно, для чего в данной статье предлагаются правила и способы по увеличению стойкости пароля.

Основная часть

Для начала стоит определиться с составом символов, из которых будет строиться пароль. Это обязательно должны быть буквы как верхнего, так и нижнего регистра, цифры и специальные символы, так как чем больше разнотипных символов в себя включает пароль, тем сложнее его предсказать.

Следующим немало важным вопросом является длина пароля. Как показывает статистика в среднем это от шести до десяти символов, в основном восемь. Уже упоминалось, что при должном техническом обеспечении такой пароль взламывается за обозримое время, поэтому рекомендуемая длина пароля

от 12 символов, чем больше, тем лучше, так как тогда время, затрачиваемое на брутфорсинг, увеличивается с экспоненциальным ростом [1].

Зачастую пользователи, пытаясь удовлетворить данным требованиям, прибегают к очевидным подстановкам символов: вместо «о» - ноль, вместо «ч» - четыре, вместо «s» - символ доллара и так далее, все это на сегодняшний день хакерские программы учитывают, поэтому их также следует избегать.

Еще одним плохим примером формирования пароля является использование очевидных комбинаций слов для легкого запоминания, что взламывается по средствам переборов по словарям, или использование в составе пароля информации доступной из социальных сетей или другая раскрытая личная информация: имена, клички питомцев, дни рождения и так далее, всего этого также следует избегать [2].

Но тогда возникает вопрос, как, не прибегая ко всему этому, получить надежный и запоминающийся пароль? Здесь существует два относительно похожих подхода: из мнемонических фраз или необычных сочетаний слов по определенному правилу строится пароль или к сгенерированной цепочке случайных символов формируется мнемоническая фраза.

Для примера из фразы «корова жги алый фагот» можно сформировать пароль «коровА!жгИ%алыЙ?фагоТъ», или для цепочки символов «f2a_+Vm3cV*j» можно сформировать фразу «фрукты два ананаса подчеркнули и добавили VISA музыка 3 цента VISA умножает джинсы».

Такой подход хорош тем, что созданный таким способом пароль очень сложно взломать, угадать или подобрать по словарям, а главное легко запомнить владельцу, так как все сводится к фразе и её ассоциации с паролем.

Кроме того, если такой подход кажется слишком сложным, существует несколько способов улучшить безопасность парольной аутентификации. Например, можно использовать двухфакторную аутентификацию, которая требует дополнительного подтверждения личности пользователя, такого как код, отправленный на телефон. Также можно использовать менеджеры паролей, которые хранят пароли в зашифрованном виде и генерируют новые пароли для каждой учетной записи, тогда необходимо будет запомнить только один сформированный по приведенным рекомендациям пароль.

В заключение следует отметить, что Создание надежного пароля - только первый шаг в защите вашей информации, и относиться к нему нужно с особым вниманием. В заключение хочется привести еще ряд рекомендаций по работе с паролями. Никогда не сохраняйте пароли на листочках или в заметках, это сводит парольную защиту даже с самым сложным паролем к нулю. Не используйте одни и те же пароли на разных ресурсах, при фальсификации пароля в одном месте, автоматически подвергаются угрозе и другие. Чаще обновляйте пароли от самых важных ресурсов, для минимизации риска несанкционированного доступа к вашей информации.

Список источников

1. Шаффер К. Не слишком ли строги пароли ? / К.Шаффер // Открытые системы. СУБД, 2012. С. 42.

2. Фатхи Д.В. Способ повышение надежности пароля пользователя и его исследование / Д.В.Фатхи // Интеллектуальные ресурсы – региональному развитию, 2019. С. 110-117.

Информация об авторах

Потапова Н.Д. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Гладышев М.А. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Ершов Н.С. – преподаватель кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Мустафа Абдулкадим Ал-Амееди - аспирант Института автоматики и информационных технологий «ТГТУ».

Вклад авторов

Потапова Н.Д. - идея, сбор материала, обработка материала (25%).

Гладышев М.А. - сбор материала, обработка материала, написание статьи (40%).

Ершов Н.С. - написание статьи, научное редактирование текста (20%).

Мустафа Абдулкадим Ал-Амееди - частичное написание статьи (15%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.832

Методы преподавания в сфере ИБ с использованием интерактивных способов обучения

Фёдор Михайлович Пыршев [1] ✉, Павел Игоревич Карасев [2], Алмали Ахмед Аднан Латиф[3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]pyrshev.f.m@edu.mirea.ru✉, http://orcid.org/0009-0009-1000-2759
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3] fit_tstu@mail.ru, https://orcid.org/0009-0007-4529-9674

Аннотация. В современном мире подготовка студентов к профессиональной деятельности предполагает вооружение системой необходимых знаний, совокупностей практических умений и навыков, органичной взаимосвязи теории с практикой. В статье рассматривается возможность создания упрощённой виртуальной модели, которая симулирует разные аспекты деятельности ИБ специалиста. Эта модель призвана сформировать у студентов интерес к профессии и определиться с тем, к какой частью ИБ у них имеется больший интерес.

Ключевые слова: образование, информационная безопасность, геймификация, геймификация в образовании, геймдизайн.

Современное образование в сфере информационной безопасности предоставляет разнообразные знания, но эти знания часто не выходят за пределы теоретической, академической сферы, что затрудняет их применение в профессиональной среде. Вследствие этого, студенты сталкиваются с несоответствием своих знаний и рабочих реалий.

Относительно современным методом решения этой проблемы является геймификация.

Геймификация - это применение игровых подходов для неигровых процессов с целью повышения вовлечённости участников в решение прикладных задач. Термин был предложен в 2004 году английским программистом Ником Пиллингом [1]. Геймификация используется для вовлечение учащегося в учебный процесс с помощью всевозможных игровых механик таких как: рейтинги, достижения, испытания, награды и т.д.

Основные приёмы геймификации, которые используются в образовании:

– приемы контроля внимания;

– декомпозиция абстрактных целей на более простые и понятные задачи;

– формирование системы санкций, весомых для участников;

– формирование качественного баланса между сложностью задач и

способностями ученика;

– создание моделей, симулирующих возможные рабочие задачи, с которыми студент должен разобраться

Задачи, решаемые введение геймификации:

– сформировать практические навыки решения различных ситуаций;

– дать студенту понимание того, как необходимо действовать в ситуации нехватки или противоречивости информации;

– повысить мотивацию студента повышать свою квалификацию в изучаемой сфере.

Современные игровые технологии позволяют представить необходимые знания в разнообразных интерактивных формах, что позволяет максимально всесторонне охватить информацию в сфере информационной безопасности. Поэтому необходимо разработать перечень игровых механик, которые смогут вовлечь студента в изучение материала, а также ознакомят его с особенностями разных сфер защиты информации.

Наиболее целесообразно организовать подачу материала согласно историческим этапам формирования представлений об информационной безопасности. Обычно выделяют следующие периоды:

Первый период - начало создания осмысленных и самостоятельных средств и методов защиты информации.

Второй период - появление технических средств обработки информации и передачи сообщений с помощью электрических сигналов и электромагнитных полей.

Третий период - внедрение автоматизированных систем обработки и хранения информации [2].

Также важно выделить основные направления деятельности в сфере защиты информации. Защита информации встречается почти во всех сферах жизнедеятельности и охватывает почти все виды деятельности. Но всё же можно выделить следующие направления:

– Организационно-правовое направление - отслеживание изменения законотворческой деятельности государства, формирование и актуализация документальной базы предприятия, проведение курсов повышения квалификации сотрудников и т.д.

– Программное направление - Разработка и внедрение новшеств в программной области защиты информации, обеспечение технической базы информационной безопасности предприятия и т.д.

– Программно-аппаратное направление - разработка и внедрение новшеств в программно-аппаратной области защиты информации, обеспечение технической базы информационной безопасности предприятия и т.д.

– Криптографическое направление - Разработка и внедрение криптографических технологий в области защиты информации, обеспечение криптографической базы информационной безопасности предприятия и т.д.

Важно отметить, что очень важно следовать правилам хорошего геймдизайна при разработке каких-либо материалов. Хороший геймдизайн — процесс создания целей, которые игрок захочет достигнуть, и правил, которым

игрок будет следовать в процессе принятия значимых решений на пути к достижению этих целей [3]. Важно следовать этому определению, так как, используя геймификацию, мы заходим в игровую область знания. А значит, что для создания качественных продуктов потребуется следовать не только правилам из области информационной безопасности, но и правилам из области геймдизайна.

На базе наработок необходимо разработать интерактивные механики, которые смогут дать студентам понимание основной деятельности по данным направлениям, поможет определиться с тем, какое направление наиболее точно подходит студенту и в каком направлении он хочет развивать свои профессиональные навыки.

Список источников

1. Краткая история геймификации. URL: https://www.gamification-now.ru/blog/kratkaya-istoriya-geymifikacii (дата обращения: 05.03.2023 г.).

2. Развитие средств и методов защиты информации. URL: https://moodle.kstu.ru/mod/page/view.php?id=28907 (дата обращения: 10.02.2023).

3. Введение в геймдизайн: Основные понятия и принципы проектирования игр. URL: https://vc.ru/flood/10495-gamedev-challenges (дата обращения: 10.03.2023).

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Пыршев Ф.М. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Алмали Ахмед Аднан Латиф - аспирант Института автоматики и информационных технологий «ТГТУ».

Вклад авторов

Пыршев Ф.М. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Карасев П.И. - написание статьи, научное редактирование текста (30%).

Алмали Ахмед Аднан Латиф - частичное написание статьи (20%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.832

Роль машинного обучения в обеспечении информационной безопасности персональных данных

Даниил Александрович Родькин [1] ✉, Павел Игоревич Карасев [2], Алмали Ахмед Аднан Латиф[3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]rodkin.d.a@edu.mirea.ru✉, http://orcid.org/0009-0009-4500-2468
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3] fit_tstu@mail.ru, https://orcid.org/0009-0007-4529-9674

Аннотация. В статье рассматривается роль машинного обучения в информационной безопасности и то, как оно может быть использовано для защиты персональных данных.

Ключевые слова: машинное обучение, информационная безопасность, нейронная сеть.

Распространение цифровых устройств и интернета привело к сбору и хранению огромного количества персональных данных. Под персональными данными понимается любая информация, которая может быть использована для идентификации личности, например, имя, адрес, номер телефона, электронная почта и финансовая информация. Сбор и использование персональных данных компаниями, правительствами и другими организациями вызвали обеспокоенность по поводу конфиденциальности и безопасности личной информации. Необходимость защиты персональных данных стала еще более острой в эпоху Интернета, где личная информация может быть легко доступна, распространена и использована не по назначению. Информационная безопасность — это практика защиты информации от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения. Роль машинного обучения в информационной безопасности становится все более важной, поскольку объем и сложность персональных данных продолжают расти [1].

Текущее состояние информационной безопасности:

Несмотря на усилия по улучшению информационной безопасности, утечки данных продолжают происходить с угрожающей скоростью. По данным новостного центра (RBC), в 2022 году в России количество утекших персональных данных составляет более 660 миллионов записей, в результате которых было раскрыто более 300 миллионов записей. RBC сообщил, что основной причиной утечки данных является хакерство, за которым следуют фишинг и случайный контакт. Последствия утечки данных могут быть

серьезными, включая финансовые потери, кражу личных данных, репутационный ущерб и юридическую ответственность.

Роль машинного обучения в защите персональных данных:

Машинное обучение стало мощным инструментом защиты персональных данных. Алгоритмы машинного обучения могут анализировать большие объемы данных, выявлять закономерности и аномалии, а также делать прогнозы на основе этих данных. Использование методов машинного обучения может помочь определить потенциальные риски безопасности и выявить аномальное поведение, которое может свидетельствовать о нарушении данных. Некоторые методы машинного обучения, используемые для защиты персональных данных, включают контролируемое и неконтролируемое обучение, нейронные сети и глубокое обучение. Контролируемое обучение — это тип машинного обучения, который предполагает обучение модели на маркированных данных. Маркированные данные состоят из входных данных и соответствующих выходных меток, которые используются для обучения модели. После обучения модели ее можно использовать для прогнозирования выходных меток для новых входных данных. Контролируемое обучение может использоваться в защите персональных данных для выявления закономерностей и аномалий в данных и обнаружения потенциальных рисков безопасности.

Неподконтрольное обучение — это тип машинного обучения, который предполагает обучение модели на немаркированных данных. Модель учится выявлять закономерности и аномалии в данных без каких-либо входных меток. Неконтролируемое обучение может использоваться в защите персональных данных для выявления потенциальных рисков безопасности и обнаружения аномального поведения, которое может указывать на утечку данных [2].

Нейронные сети — это тип модели машинного обучения, основанный на структуре человеческого мозга. Нейронные сети состоят из слоев взаимосвязанных узлов, которые обрабатывают входные данные и выдают выходные данные. Нейронные сети можно использовать для защиты персональных данных, чтобы выявлять закономерности и аномалии в данных и обнаруживать потенциальные риски безопасности.

Глубокое обучение — это тип нейронной сети, которая включает в себя несколько слоев взаимосвязанных узлов. Глубокое обучение может использоваться в защите персональных данных для выявления закономерностей и аномалий в данных и обнаружения потенциальных рисков безопасности.

В заключение следует отметить, что машинное обучение быстро становится важным инструментом информационной безопасности для защиты персональных данных. Его способность анализировать большие объемы данных, выявлять закономерности и принимать интеллектуальные решения сделала его ценным активом для обнаружения и предотвращения кибератак [3].

Список источников

1. М.Ю. Рытов, Чио Кларенс, Фримэн Дэвид, Машинное обучение и безопасность: защита систем с помощью данных и алгоритмов, 2020 г. - 388 стр.

2. Арутюнов, В. В. Применение методов искусственного интеллекта для обеспечения информационной безопасности: результативность и востребованность итогов исследований российских учёных / В. В. Арутюнов // Научные и технические библиотеки. – 2020. – № 11. – С. 105-116.

3. Искусственный интеллект в ИБ. URL: https://cisoclub.ru/aaiskusstvennyj-intellekt-v-ib/ (дата обращения 10.04.2023)

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Родькин Д.А. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Алмали Ахмед Аднан Латиф - аспирант Института автоматики и информационных технологий «ТГТУ».

Вклад авторов

Родькин Д.А. - идея, сбор материала, обработка материала (40%).
Карасев П.И. - написание статьи, научное редактирование текста (30%).
Алмали Ахмед Аднан Латиф - частичное написание статьи (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.55

Основы криптографии. Нюансы визуального и облачного видов шифрования

Никита Александрович Руденко ✉
Брянский государственный технический университет, Брянск, Россия
rudenkonikita889@gmail.com ✉

Аннотация. В статье рассмотрена терминология в области криптографии. Рассмотрены нюансы визуальной и облачной криптографии.

Ключевые слова: шифрование, открытый текст, дешифровка, криптография, визуальное шифрование, облачное шифрование.

Криптография больше не является сугубо военным инструментом, с которым не следует связываться. Пришло время демистифицировать криптографию и в полной мере использовать преимущества, которые она предоставляет современному обществу. Далее представлена базовая терминология и основные методы криптографии.

Основная терминология

Предположим, что кто-то хочет отправить сообщение получателю и хочет быть уверенным, что никто другой не сможет прочитать это сообщение. Однако существует вероятность того, что кто-то другой откроет письмо или услышит электронное сообщение. В криптографической терминологии сообщение называется **открытым текстом**. Кодирование содержимого сообщения таким образом, чтобы скрыть его содержимое от посторонних, называется **шифрованием**. Зашифрованное сообщение называется **зашифрованным текстом**. Процесс извлечения открытого текста из зашифрованного называется **расшифровкой**. Для шифрования и дешифрования обычно используется **ключ,** а метод кодирования таков, что дешифрование может быть выполнено только при знании правильного ключа.

Криптография - это искусство или наука сохранения сообщений в секрете.

Криптоанализ - это искусство взлома шифров, то есть извлечения открытого текста без знания правильного ключа. Люди, которые занимаются криптографией, являются **криптографами**, а практикующие криптоанализ - **криптоаналитиками**.

Криптография имеет дело со всеми аспектами защищенных сообщений, аутентификации, цифровых подписей, электронных денег и других приложений.

Криптология - это раздел математики, изучающий математические основы криптографических методов.

Основные криптографические алгоритмы

Метод шифрования и дешифрования называется **шифром**. Некоторые криптографические методы основаны на секретности алгоритмов; такие алгоритмы представляют только исторический интерес и не подходят для реальных нужд. Все современные алгоритмы используют ключ для управления шифрованием и дешифрованием; сообщение может быть расшифровано, если ключ совпадает с ключом шифрования. Ключи шифрования и дешифрования, могут отличаться, но для большинства алгоритмов они одинаковы.

Существует два класса алгоритмов, основанных на ключах: **симметричные** (с секретным ключом) и **асимметричные** (с открытым ключом) алгоритмы. Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и дешифрования (или ключ дешифрования легко выводится из ключа шифрования), в то время как асимметричные алгоритмы используют другой ключ для шифрования и дешифрования; ключ дешифрования не может быть получен из ключа шифрования.

Симметричные алгоритмы можно разделить на **потоковые шифры** и **блочные шифры**.

Потоковые шифры могут шифровать один бит открытого текста за раз, в то время как блочные шифры принимают несколько битов (обычно 64 бита в современных шифрах) и шифруют их как единое целое.

Асимметричные шифры (также называемые алгоритмами с открытым ключом или вообще криптографией с открытым ключом) делают ключ шифрования общедоступным (он может быть даже опубликован в газете), позволяя любому зашифровать с помощью ключа, в то время как только соответствующий получатель (который знает ключ дешифрования) может расшифровать сообщение. Ключ шифрования также называется открытым ключом, а ключ дешифрования - закрытым ключом или секретным ключом.

Современные криптографические алгоритмы на самом деле не выполняются людьми. Надежные криптографические алгоритмы предназначены для выполнения компьютерами или специализированными аппаратными устройствами. В большинстве случаев шифрование и дешифрование выполняется с помощью компьютерного программного обеспечения.

Визуальная криптография

Визуальная криптография - это метод безопасной связи, который использует изображения для шифрования секретных сообщений. Он работает путем разделения изображения или текста на несколько общих разделов, так что, когда общие разделы накладываются друг на друга, исходное изображение или текст становятся видимыми.

Как это работает?

1. Исходное изображение или текст разделены на две или более части, каждая из которых выглядит как случайный и бессмысленный шаблон.
2. Затем части печатаются и распространяются среди предполагаемых получателей.
3. Чтобы раскрыть секретное сообщение, общие элементы накладываются друг на друга либо путем укладки, либо путем их точного выравнивания.

4. Наложенные общие ресурсы создают исходное изображение или текст.

Преимущества визуальной криптографии

1. Нет необходимости в защищенном канале для обмена ключом.
2. Проста в реализации и понимании.
3. Устойчивость к компьютерным атакам, поскольку части выглядят бессмысленными.
4. Не требуется специализированного программного или аппаратного обеспечения.
5. Может использоваться в различных областях, таких как системы безопасного голосования, банкноты и схемы секретного обмена.

Недостатки визуальной криптографии

1. Низкая емкость встраивания, что означает, что он может скрывать только ограниченную информацию.
2. Чувствительность к шуму и ухудшению качества, которые могут повлиять на качество восстановленного изображения.
3. Сложность в реализации цветных изображений.
4. Требуется точное выравнивание общих ресурсов для раскрытия исходного сообщения.
5. Ограниченная устойчивость к атакам со стороны людей, имеющих доступ к общим ресурсам.

Облачная криптография

Облачная криптография - это набор методов, используемых для защиты данных, хранящихся и обрабатываемых в средах облачных вычислений. Он обеспечивает конфиденциальность данных, их целостность и неразглашение с помощью систем шифрования и безопасного управления ключами.

Общие методы, используемые в облачной криптографии, включают:

1. Симметричное шифрование: шифрует и дешифрует данные, используя один и тот же ключ.
2. Асимметричное шифрование: использует два разных ключа: открытый ключ для шифрования и закрытый для дешифрования.
3. Хеш-функции: создание дайджеста сообщения, чтобы обеспечить его целостность.
4. Управление ключами: безопасное хранение ключей шифрования и управление ими для обеспечения безопасности зашифрованных данных.

Использование криптографии в облаке имеет важное значение для защиты конфиденциальной информации и обеспечения соответствия таким нормативным актам, как GDPR и HIPAA.

Как это работает?

Облачная криптография основана на шифровании, при котором компьютеры и алгоритмы используются для преобразования текста в зашифрованный текст. Затем этот зашифрованный текст может быть преобразован в открытый текст с помощью ключа шифрования путем декодирования его с помощью ряда битов.

Шифрование данных может осуществляться одним из следующих способов:

1. **Предварительно зашифрованные данные, которые синхронизируются с облаком**

Доступно программное обеспечение для предварительного шифрования, прежде чем информация попадет в облако, что делает невозможным чтение для любого, кто попытается ее взломать.

2. **Сквозное шифрование**

Отправители и получатели отправляют сообщения, в результате чего они единственные, кто может их прочитать.

3. **Шифрование файлов**

Шифрование файлов происходит, когда данные в состоянии покоя зашифрованы таким образом, что если неавторизованное лицо попытается перехватить файл, оно не сможет получить доступ к хранящимся в нем данным.

4. Полное шифрование диска

Когда какие-либо файлы сохраняются на внешнем диске, они будут автоматически зашифрованы. Это ключевой метод защиты жестких дисков на компьютерах.

Вывод

В итоге мы усвоили основы криптографии, а также ознакомились с визуальным и облачным типами криптографии.

Список источников

1. Geeksforgeeks.org 6 февраля 2023 URL: https/www.geeksforgeeks.org/an-overview-of-cloud-cryptography/?ref=rp
2. Geeksforgeeks.org 2 февраля 2023 URL: https/www.geeksforgeeks.org/visual-cryptography-introduction

Статья поступила в редакцию 22.03.2023; принята к публикации 10.05.2023.

Научная статья
УДК 004.424

Проблемы и методы защиты персональных данных в веб-сервисах коммерческой организации

Александр Витальевич Рязанцев [1] ✉, Павел Игоревич Карасев [2], Мустафа Абдулкадим Ал-Амееди[3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]ryazantsev.a.v@edu.mirea.ru✉, http://orcid.org/0009-0005-7517-5491
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3]fit_tstu@mail.ru, https://orcid.org/0009-0002-1066-6650

Аннотация. В статье рассматривается проблема защиты персональных данных в веб-сервисах коммерческих организаций и методы, которые могут быть использованы для решения этой проблемы.

Ключевые слова: информационная безопасность, коммерческие организации.

В современную цифровую эпоху защита персональных данных становится все более важным вопросом, особенно в связи с широким распространением веб-услуг. Коммерческие организации, в частности, несут ответственность за обеспечение сохранности и безопасности личных данных своих клиентов. Это не только этическая, но и юридическая ответственность, поскольку законы о защите данных были приняты для защиты частной жизни людей.

Персональные данные - это любая информация, которая может быть использована для идентификации человека, например, его имя, адрес, номер телефона или адрес электронной почты. Когда люди предоставляют свои личные данные коммерческой организации через ее веб-сайт или веб-сервисы, они ожидают, что их данные будут использоваться только в тех целях, для которых они их предоставили, и что они будут надежно защищены.

Чтобы обеспечить защиту персональных данных, коммерческие организации должны принимать соответствующие меры по их сохранению. Это включает в себя применение технических и организационных мер для предотвращения несанкционированного доступа, обеспечение точности и актуальности данных, а также предоставление лицам доступа к их личным данным и возможности исправления любых неточностей.

Кроме того, коммерческие организации должны обеспечивать прозрачность в отношении того, как они используют персональные данные. Они должны четко объяснить, зачем они собирают данные, как они будут использованы и кому они будут переданы. Они также должны получать согласие людей перед сбором и использованием их персональных данных.

Неспособность защитить персональные данные может иметь серьезные последствия как для частных лиц, так и для коммерческих организаций. Частные лица могут пострадать от кражи личных данных, финансовых потерь или репутационного ущерба, а коммерческие организации могут столкнуться с судебными исками, финансовыми штрафами и ущербом для своей репутации.

Таким образом, защита персональных данных является важным компонентом веб-услуг, предоставляемых коммерческими организациями. Это не только этическая, но и юридическая ответственность, и неспособность защитить персональные данные может иметь серьезные последствия. Поэтому коммерческие организации должны принимать соответствующие меры по защите персональных данных и быть прозрачными в отношении того, как они используются [1].

Проблема защиты персональных данных в веб-сервисах коммерческих организаций возникает по нескольким причинам:

1) Веб-сервисы собирают персональные данные своих пользователей для предоставления им персонализированных услуг, которые часто используются в маркетинговых целях. Эти персональные данные могут включать конфиденциальную информацию, такую как имя, адрес, номер телефона, адрес электронной почты, финансовую и даже медицинскую информацию. Хранение этой информации может создать значительный риск для пользователей, если не обращаться с ней должным образом.

2) Коммерческие организации уязвимы к кибератакам, которые могут привести к утечке данных и их неправомерному использованию. Киберпреступники могут украсть личные данные и использовать их для мошеннических действий, таких как кража личных данных, фишинговые аферы и финансовое мошенничество. Кроме того, коммерческие организации также могут злоупотреблять персональными данными, передавая их сторонним поставщикам услуг без согласия пользователя или используя их в непредусмотренных целях.

Для решения проблемы защиты персональных данных в веб-сервисах коммерческих организаций можно использовать несколько методов:

Во-первых, организациям следует принять надежную политику защиты данных, в которой приоритет отдается конфиденциальности и безопасности данных. Это может включать в себя внедрение надежных методов шифрования данных, ограничение доступа к данным только уполномоченным персоналом, а также регулярное проведение аудита безопасности для выявления уязвимостей и рисков.

Во-вторых, организации должны получать согласие пользователей перед сбором и использованием персональных данных. Этого можно достичь путем предоставления четкой и ясной политики конфиденциальности, которая информирует пользователей о типе собираемых данных, способах их использования и о том, кому они будут переданы. Кроме того, организации должны предоставлять пользователям возможность отказаться от сбора и обработки данных, если они не хотят делиться своими личными данными.

В-третьих, организациям следует внедрить политику уведомления о нарушении данных, которая своевременно информирует пользователей о том, что их личные данные были скомпрометированы. Это может помочь пользователям принять необходимые меры предосторожности, такие как смена паролей, мониторинг финансовых счетов и сообщение о подозрительных действиях [2].

В заключение следует отметить, что защита персональных данных в веб-сервисах коммерческих организаций является критической проблемой, требующей внимания и действий. Организации должны уделять приоритетное внимание конфиденциальности и безопасности данных пользователей, принимая надежные политики защиты данных, получая согласие пользователей и внедряя политики уведомления о нарушении данных. Применяя эти методы, организации могут обеспечить защиту и безопасность персональных данных, а пользователи могут доверять и продолжать уверенно пользоваться их услугами.

Список источников

1. Рытов М.Ю., Аверченков В. И., Гайнулин Т. Р. Защита персональных данных в организации. – Брянск, 2016. - 124 с.

2. Внедрение искусственного интеллекта: как государство поддерживает общество. URL: https://www.rbc.ru/technology_and_media/21/11/2022/6373b9d99a7947fa230d041d (дата обращения 10.04.2023)

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Рязанцев А.В. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Мустафа Абдулкадим Ал-Амееди - аспирант Института автоматики и информационных технологий «ТГТУ».

Вклад авторов

Рязанцев А.В. - идея, сбор материала, обработка материала (40%).

Карасев П.И. - написание статьи, научное редактирование текста (30%).

Мустафа Абдулкадим Ал-Амееди - частичное написание статьи (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.832

Анализ методов проверки безопасности цифровых активов

Ильяс Радикович Сафин [1] ✉, Павел Игоревич Карасев [2], Юрий Юрьевич Громов [3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]mega.korporatsiya@edu.mirea.ru✉, http://orcid.org/0009-0005-6368-7297
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3]gromovtambov@yandex.ru, https://orcid.org/ 0000-0003-3313-2731

Аннотация. В статье рассмотрены признаки возможного нелегального происхождения средств в криптовалюте. Знание принципов легализации цифровых денежных средств, заработанных незаконным путём, позволит финансовым регуляторам и специалистам по информационной безопасности предотвращать и расследовать экономические преступления с применением криптовалюты.

Ключевые слова: криптовалюта, легализация денежных средств, транзакции.

В наши дни всё большую популярность набирают электронные средства платежей. Это сопровождается как преимуществами в виде повышения скорости проведения финансовых транзакций, так и недостатками в лице привязки всех действий к конкретному физическому или юридическому лицу. В 2009-м году анонимным разработчиком или группой анонимных разработчиков была запущена новая цифровая валюта – криптовалюта Bitcoin [1]. Достоинствами нового платёжного средства стали отсутствие верификации личности, единого управления в лице компаний и государственных регуляторов и отказоустойчивость (система работает децентрализованно на сотнях тысяч компьютеров энтузиастов по всему миру).

Цифровая система оказалась настолько хорошей, что злоумышленники не смогли обойти её стороной: они начали использовать инновационные средства платежей для легализации денег, заработанных преступной деятельностью. Для некоторых публицистов такой ход событий играет на руку, ведь высказывания о «нелегальных деньгах» тяжело проверить людям, не сильно разбирающимся в теме цифровых платёжных систем. Отсюда возникает проблема – люди вместо решения задачи в инновационной для них сфере просто отказываются от благ прогресса.

Куда правильнее было бы выработать методику определения юридической «чистоты» средств на электронном кошельке, ведь это позволит компаниям и регуляторам предотвращать попытки легализации незаконно полученных денег,

а специалистам по информационной безопасности – быстрее и эффективнее расследовать инциденты, в которых замешаны криптовалюты.

Легализация денежных средств – это совокупность операций, совершаемых над денежными средствами, полученными незаконным способом, в попытке сделать возможным их законное использование. Такие действия часто называют «отмыванием» денег [2].

Злоумышленники для своей противоправной деятельности используют преимущественно криптовалюты Bitcoin и Ethereum. Блокчейны этих двух криптовалют открыты, а это значит, что любой заинтересованный человек может свободно изучать операции в них.

Некоторые люди, имеющие предпринимательскую инициативу и знакомые с устройством криптовалют, решили заработать на сложившейся ситуации – они разработали свои приложения, позволяющие «запутать» транзакции, чтобы в результате не было явной связи конечных денежных средств с начальными.

Подобные сервисы получают деньги от пользователя, смешивают их со своим «резервом» цифровых монет, состоящим в основном из средств других пользователей, и отправляют немного меньшую сумму на конечный кошелёк. Подобное действие усложняет анализ операций. Цифровые активы как будто «смешиваются» между собой – так подобные приложения стали называть «миксерами» [3] (от английского «to mix» - смешивать) (рис. 1). Каждый сервис может предложить свои дополнительные функции: перемешивание средств между множеством кошельков, задержки транзакций, разбиение конечной суммы на множество мелких с последующей отправкой на разные счета.

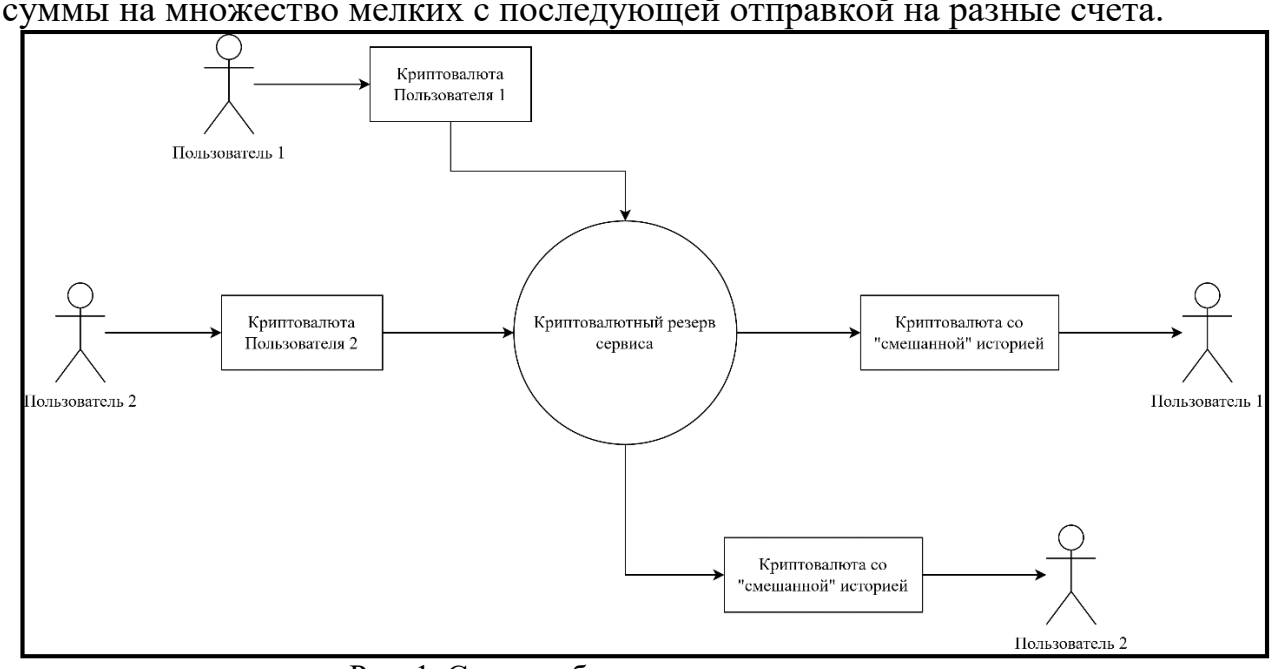

Рис. 1. Схема работы сервисов-«миксеров»

Многие злоумышленники полагают, что такие сервисы позволяют раз и навсегда «очистить» историю цифровых активов. Как бы то ни было, при пользовании услугами «миксеров» существует достаточно простой способ связать начальный и конечный кошельки – нужно проанализировать исходящие транзакции с начального счёта и посмотреть, куда были отправлены средства

далее. Если был использован классический алгоритм «микширования» цифровых денег, то с большой вероятностью удастся обнаружить адрес, на который поступила сумма, немногим меньшая изначальной. В случае же, если при «смешивании» электронных монет использовалось разделение финальной суммы на несколько небольших и последующая их отправка на разные кошельки, то необходимо попытаться выявить комбинации счетов, сумма входящих средств на которые даст число, которое незначительно меньше начального. В анализе транзакций может помочь специализированное программное обеспечение.

Не стоит забывать и про другой индикатор возможной попытки легализации средств – пакетные транзакции, изначально созданные для экономии денег на комиссиях за переводы за счёт объединения нескольких переводов в один. Пакетными транзакциями часто пользуются биржи, осуществляя вывод криптовалюты своим клиентам.

Данная технология, хоть и была создана для удобства пользователей, всё же может показать не самые благие намерения использования криптовалюты. Подозрение должна вызвать пакетная транзакция, в результате которой средства разбиваются на приблизительно равные суммы и, проходя через несколько адресов, вновь соединяются на едином счёте. Такие операции могут проводиться с целью затруднить анализ переводов в блокчейне.

Конечно, вышеперечисленные индикаторы не доказывают попытки легализовать денежные средства. Тем не менее, они могут указывать на возможную неблагонадёжность владельца счёта.

Вывод: при проверке криптовалютного счёта на легальность происхождения средств необходимо обратить внимание на пакетные транзакции, а также проанализировать, объединились ли в последующем средства, отправленные с изучаемого кошелька, на каком-то одном счёте.

Список источников

1. Биткойн. URL: https://ru.wikipedia.org/wiki/Биткойн (дата обращения: 01.03.2023).

2. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 №115-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 01.03.2023).

3. Биткойн-миксер. URL: https://ru.wikipedia.org/wiki/Биткойн-миксер (дата обращения: 03.03.2023).

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Сафин И.Р. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Громов Ю.Ю. – д.т.н. профессор, Институт автоматики и информационных технологий «ТГТУ».

Вклад авторов

Сафин И.Р. - идея, сбор материала, обработка материала (40%).
Карасев П.И. - написание статьи, обработка материала (20%).
Громов Ю.Ю. - научное редактирование текста (40%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.53

Анализ решений для безопасной передачи данных между Android-приложениями на одном устройстве

Владислав Витальевич Свиридов[1] ✉, Павел Игоревич Карасев [2], Мустафа Абдулкадим Ал-Амееди[3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1] sviridov.v.v1@edu.mirea.ru✉, http://orcid.org/ 0009-0001-4172-3841
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3] fit_tstu@mail.ru, https://orcid.org/ 0009-0002-1066-6650

Аннотация. Статья описывает методы безопасного обмена данными между Android-приложениями на одном устройстве. Разделение приложений на отдельных пользователей со своими идентификаторами и группами обеспечивает безопасность их данных, но возникают ситуации, когда необходимо передавать конфиденциальные данные между приложениями. В статье рассматриваются плюсы и минусы различных способов передачи данных.

Ключевые слова: Android, информационная безопасность, безопасность приложений, конфиденциальные данные, обмен конфиденциальными данными.

Операционная система Android разработана на основе ядра Linux, при этом каждое приложение она рассматривает как отдельного пользователя со своим идентификатором пользователя и группы, такое разделение достаточно безопасно, оно гарантирует, что одно приложение не сможет получить доступ к директории другого, что позволяет хранить многие конфиденциальные данные на устройстве пользователя в директории приложения.

Однако возможна ситуация, когда необходимо передать какие-то конфиденциальные данные между двумя приложениями на одном устройстве, в частности когда необходимо чтобы если пользователь авторизовался в одном из приложений, то авторизация автоматически происходила во всех приложениях компании на устройстве. Рассмотрим плюсы и минусы различных способов передачи этих данных. Глобально их все можно разделить на те, которые выполняются на серверной части приложения и на клиентской [1].

Главной проблемой передачи этих данных через сервер является то, что возникает необходимость однозначной идентификации устройства, существует несколько способов это сделать.

Серийный номер: уникален для каждого устройства, в лучшем случае он должен оставаться постоянным, однако существуют способы его изменения. Кроме того, для получения серийного номера устройства необходимо явное разрешение от пользователя, полученное обоими приложениями.

IMEI (International Mobile Equipment Identity): обладает теми же плюсами и минусами, что и серийный номер.

Android_ID: для устройств с версией ниже Android 8.0 – уникальный идентификатор устройства, который присваивается устройству при первом запуске, однако в последующих версиях он уникален для каждой комбинации приложения, устройства, пользователя.

MAC – адрес: уникальный идентификатор сетевого интерфейса, который обычно назначается производителем устройства. Однако Android версий выше 10 использует случайный MAC-адрес для каждого подключения к беспроводной сети.

Таким образом заметна тенденция к запрету идентификации устройств приложениями, возможны методы создания цифрового отпечатка устройства, но они не обладают достаточной точностью, чтобы гарантировать, что разные устройства не получат уникальное значение идентификатора.

Рассмотрим способы передачи конфиденциальных данных, которые происходят непосредственно на устройстве пользователя [2].

Content Provider: стандартный способ межпроцессорной связи и безопасной передачи данных между приложениями, для передачи конфиденциальных данных необходимо объявить уровень доступа signature, который обозначает, что для доступа одного приложения к данным другого они должны быть подписаны одинаковой электронно-цифровой подписью или уровень dangerous, если необходимо передать данные приложению другого разработчика, тогда приложение явно запросит у пользователя разрешение на доступ к информации [3].

Service: предназначен для выполнения каких-то действий в фоне и для предоставления части функционала приложения другому приложению. Для доступа к сервису используется механизм разрешений так же, как и для Content Provider.

Broadcast: механизм отправки и получения широковещательных сообщений. Любое приложение может подписаться на сообщение и тогда при его отправке система направит его приложению. Обычно используется для получения приложением различных системных событий (загрузка системы, подключение зарядного устройства и т.д.), но может использоваться и для межпроцессорного взаимодействия. Тоже поддерживает механизм разрешений, кроме того при отправке возможно указать пакет, тогда система отправит сообщение только приложениям соответствующим этому пакету. Стоит так же учитывать, что трансляцию может отправить любое приложение и эта трансляция может быть потенциально вредоносной, однако существуют методы указать какие трансляции будут приниматься.

Shared Memory: низкоуровневый инструмент, который позволяет создать сервис, который выделяет область памяти, а затем передать этот сервис клиенту через файловый дескриптор.

Схожесть между механизмами контроля доступа между Content Provider, Service, Broadcast обусловлена использованием ими механизма Intents для передачи данных между приложениями.

Таким образом существует 4 основных способа безопасной передачи данных между приложениями на одном устройстве под управлением ОС Android, они используют достаточно схожий механизм безопасности и выбор одного из них может зависеть от архитектуры приложения.

Список источников

1. Broadcasts. URL: https://developer.android.com/guide/components/broadcasts (дата обращения: 10.03.2023).
2. Service URL: https://developer.android.com/reference/android/app/Service (дата обращения: 10.03.2023).
3. Официальная документация Android URL https://developer.android.com (дата обращения: 10.03.2023).

Статья поступила в редакцию 22.03.2023; принята к публикации 10.05.2023.

Информация об авторах

Свиридов В.В. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.03.01 – Информационная безопасность» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Мустафа Абдулкадим Ал-Амееди - аспирант Института автоматики и информационных технологий «ТГТУ».

Вклад авторов

Свиридов В.В.- идея, сбор материала, обработка материала (40%).

Карасев П.И. - написание статьи, научное редактирование текста (30%).

Мустафа Абдулкадим Ал-Амееди - частичное написание статьи (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.55

О применении российских алгоритмов шифрования при создании виртуальных частных сетей

Диана Алексеевна Свиридова[1]✉, Николь Дмитриевна Потапова[2]✉, Хайдар Абдулваххаб Х. Шамсулдин[3]✉
[1, 2] МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1] sviridova.d.a@edu.mirea.ru✉, https://orcid.org/0009-0001-4216-1465
[2] potapova.n.d@edu.mirea.ru✉, https://orcid.org/0009-0004-0395-515X
[3] fit_tstu@mail.ru✉, https://orcid.org/0009-0006-4255-5874

Аннотация. Статья посвящена виртуальным частным сетям, а в частности возможности и потенциальной необходимости применения российских стандартов при создании виртуальных частных сетей. Возможность рассматривается на примере протокола безопасности сетевого уровня WireGuard с применением аналогов алгоритмов, рекомендованных к применению Техническим комитетом по стандартизации ТК 026 "Криптографическая защита информации". Приведено краткое сравнение алгоритмов AES и ГОСТ 34.12-2015 «Кузнечик».

Ключевые слова: VPN соединения, VPN протоколы, AES, Кузнечик, Магма, ГОСТ, WireGuard, ТК 026, ФСБ РФ.

В настоящее время VPN (Virtual Private Network) используются не только для повышения анонимности в Интернете, но и компаниями, которые организуют работу собственных корпоративных сетей с применением данной технологии. Именно они подвергаются наибольшей опасности как со стороны конкурентов, так и зарубежных недоброжелателей, целью которых становятся данные. В последующем украденные данные, вне зависимости от того, были ли данные украдены у обычного пользователя VPN или компании, используются против жертвы. Попавшие в руки злоумышленников данные могут не только уменьшить потенциальную прибыль пострадавшей стороны, так и сказаться на репутации.

Виртуальные частные сети в коммерческих предприятиях позволяют удалённо объединять АРМ в полноценную сеть, что позволяет располагать офисы компании в разных местах или части сотрудников работать удалённо. Увеличение количество компаний, а также расширение существующих повышает спрос на использование VPN в качестве каналов связи, так как не все готовы разворачивать собственную VPN сеть. Из-за чего увеличивается количество недобросовестных сервисов, предлагающих подобного рода услуги.

Недобросовестный провайдер VPN может хранить не только сведения об устройствах, подключенных к его сети, но и журналы посещаемых ресурсов и иные данные, в зависимости от использования защищенного или незащищенного протокола. Поэтому все передаваемые данные внутри защищенной VPN могут попасть напрямую к злоумышленнику. И если человек, использующий виртуальные частные сети в качестве анонимайзеров, для своего спокойствия может почитать пользовательское соглашение сервиса, где провайдер обязан с юридической стороны обозначить все функции сервиса и сбор сведений о пользователях, то компаниям этого недостаточно. В таком случае гораздо более надёжным способом передачи данных становится собственноручно настроенный корпоративный VPN.

Защитить трафик проходящий по VPN туннелю позволяют алгоритмы шифрования. В зависимости от выбора которых зависит степень защиты сети. На данный момент наиболее распространенными алгоритмами шифрования являются MMPE, RSA, 3DES и AES. Среди них AES версии 3 считается наиболее новым и безопасным.

В Российской Федерации в 2007 году был создан «ТК 26» - технический комитет, занимающийся объектами стандартизации среди методов шифрования. С 2018 года данный комитет разрабатывает и выпускает разнообразные рекомендации и проекты по стандартизации применения национальных криптографических стандартов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015. В том числе комитет совместно с Федеральной службой безопасности Российской Федерации (ФСБ РФ) начали настоятельно рекомендовать переводить рунет на сертификаты, основанные на национальных стандартах шифрования, но сказать на какие именно не представляется возможным.

Шифры AES и ГОСТ 34.12-2015 «Кузнечик» являются алгоритмами блочного шифрования. Блочное шифрование основывается на том, что выбранное сообщение разделяется на “блоки” определенной длины, что позволяет на одном ключе зашифровать сообщение с большей длиной. В большинстве случаев размер блока сообщения составляет от 64 до 256 бит. В алгоритме AES могут быть использованы ключи длиной 128, 192 и 256 бит. При варианте ключа длиной 256 бит в алгоритме AES используются блоки длиной 128 бит и производятся 14 раундов шифрования. В алгоритме Кузнечик при длине ключа 256 бит, блоках сообщений длиной 128 бит используются 9 раундов шифрования. Количество раундов шифрования значительно снижено из-за того, что эти алгоритмы имеют совершенно разные квадратные матрицы. Некоторое время назад Доцент и Заведующий кафедрой Национального исследовательского университета А. Б. Лось сделал выводы о том, что алгоритм AES обладает разреженной матрицей по большей части, состоящей из нулей, что значительно увеличивает раунды шифрование. В свою очередь алгоритм Кузнечик обладает плотной матрицей, состоящей из ненулевых значений. Из-за чего алгоритм Кузнечик является более быстродействующим и требует меньше памяти для обработки.

Для передачи данных в частных виртуальных сетях используются протоколы, которые являются набором правил и процессов, описывающих подключение, обмен данными внутри сети. От протокола зависят скорость работы (передачи), платформы (операционные системы) и безопасность. Наиболее распространенными протоколами для передачи данных по сетям VPN являются OpenVPN, IPSec, WireGuard, SSTP, PPTP, IKEv2, L2TP. Только у части из приведённых протоколов есть сведения об архитектуре в открытом доступе.

В 2015 году появился VPN протокол под названием WireGuard, который имеет открытый исходный код. Изначально он предназначался для платформ под управлением ОС Windows, однако к 2020 году разработчики адаптировали его в том числе и для ОС Linux, iOS и macOS. В своём обычном виде протокол применяет целый набор криптоалгоритмов для разных целей, среди которых: Curve25519, ChaCha20, SipHash, BLAKE2 и Poly1305, HMAC.

В конце 2020 года группа исследователей и научных сотрудников из BI.ZONE и «Криптонит» опубликовали результаты своей работы над отечественной версией протокола WireGuard, основанной на российских криптографических алгоритмах. В табл. 1 приведен список замен исходного набора алгоритмов на российские.

Таблица 1

Установленные замены алгоритмов

Тип алгоритма	Исходный алгоритм	Замена алгоритму
Алгоритм согласования ключа (DH)	ChaCha20 и Poly1305	ГОСТ Р 34.10-2012 VKO или DH
Эллиптическая кривая	Curve25519	ГОСТ Р 34.10-2012 GC256A
Хэш-функция	BLAKE2s	ГОСТ Р 34.11-2012
HMAC	SipHash	ГОСТ Р 34.11-2012
Кривая (KDF)	HKDF	ГОСТ Р 34.11-2012 KDFTREE или HKDF
AEAD	ChaCha20	ГОСТ Р 34.12–2015 Кузнечик в режиме MGM

Перед началом разработки в 2019 году специалисты из BI.ZONE направляли в ТК26 предложение по изучению и работе по стандартизации протоколов, среди которых был WireGuard. Комитет в свою очередь не выразил заинтересованности, поэтому компания начала работу самостоятельно.

К концу 2020 года ТК26 утвердил рекомендации по стандартизации протокола безопасности сетевого уровня, в котором в роли протокола выступает IPlir, являющийся аналогом протокола IPsec, разработанным компанией ИнфоТеКС ранее.

Для защиты информации в виртуальных частных сетях стоит использовать надежные протоколы сетевого уровня, применяющие доверенные

криптографические алгоритмы с высоким уровнем криптостойкости, вычисленным математически. Шифрование данных, передаваемых по сетям VPN, начинается с зашифрованного канала связи - туннеля. Что позволяет при использовании публичных сетей сократить риски перехвата данных. Передаваемые по туннелю данные также подвергаются шифрованию, разбиваясь на блоки установленной длины согласно используемому алгоритму. Что позволяет добиться максимально возможного уровня защиты передаваемой информации.

Использование российских алгоритмов шифрования при создании виртуальных частных сетей может положительно сказаться на защищенность данных, передаваемых пользователями внутри этой сети. Разработка новых протоколов сетевого уровня, основанных на российской криптографии, позволит в дальнейшем чаще использовать доверенные средства внутри организаций, государственных органах и частным лицам.

Список источников

1. Браун Стивен Виртуальные частные сети / Браун Стивен — Москва : Лори, 2001 — 504 с.

2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Юрайт, 2023. — 473 с.

3. Приказ №1325-ст «Об утверждении рекомендаций по стандартизации Российской Федерации» – М.: Росстандарт, 2020.

4. ГОСТ 34.12–2015 Информационная технология. Криптографическая защита информации. Блочные шифры : национальный стандарт Российской Федерации : дата введения 2015-12-16 / Федеральное агентство по техническому регулированию и метрологии – М.: Стандартинформ, 2015.

5. Bogdanov A., Khovratovich D., Rechberger C. Biclique cryptanalysis of the full AES. In: ASIACRYPT 2011. Springer, 2011, 344–375. URL: https://doi.org/10.1007/978-3-642-25385-0_19

6. Altawy R., Youssef A.M. A meet in the middle attack on reduced round Kuznyechik. IEICE Trans. Fundam. Electron., 2015, vol. E98.A, no. 10, pp. 2194–2198. URL: https://doi.org/10.1587/transfun.E98.A.2194

7. BI.ZONE. Проект протокола Ru-WireGuard // GitHub. — URL: https://github.com/bi-zone/ruwireguardspec (дата обращения: 10.04.2023).

8. Donenfeld J. A. Протокол WireGuard / Jason A. Donenfeld // WireGuard. — URL: https://www.wireguard.com/ (дата обращения: 05.04.2023).

Статья поступила в редакцию 22.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Свиридова Д.А. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Потапова Н.Д. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Шамсулдин Хайдар Абдулваххаб Х. - аспирант Института Автоматики и информационных технологий «ТГТУ».

Вклад авторов

Свиридова Д.А. - написание статьи, помощь со сбором материала, научное редактирование текста (40%).

Потапова Н.Д.- идея, сбор материала, обработка материала (30%).

Шамсулдин Хайдар Абдулваххаб Х. - частичное написание статьи (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.832

Исследование решений на основе клавиатурного почерка для аутентификации пользователя

Олег Владимирович Свист [1], Алмали Ахмед Аднан Латиф[2], Константин Владимирович Стародубов [3]
[1, 3]МИРЭА - Российский технологический университет, Москва, Россия
[2]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]svist.o.v@edu.mirea.ru✉, http://orcid.org/0009-0006-4897-368X
[2] fit_tstu@mail.ru, https://orcid.org/0009-0007-4529-9674
[3] starodubov@mirea.ru, https://orcid.org/0009-0007-4529-9674

Аннотация. В статье проводится анализ различных методов аутентификации пользователя по клавиатурному почерку, таких как статистический анализ, машинное обучение и нейронные сети. Описываются преимущества и недостатки каждого метода, а также рассматриваются возможности их применения в различных сферах, например, в банковском секторе или в системах безопасности. Авторы статьи обращают внимание на то, что выбор метода аутентификации должен зависеть от конкретной задачи и требований к безопасности системы.

Ключевые слова: почерк, аутентификация, пользователь, обучение, анализ, выбор.

Аутентификация/идентификация пользователя компьютерной системы по клавиатурному почерку позволяет повысить защищенность системы, усложнить возможность отказа от авторства и повысить удобство пользователя за счет возможного использования упрощенного пароля. Пользователю достаточно запомнить любую парольную фразу, например, длина пароля может состоять от 4 до 8 знаков. Если учесть особенности ввода отдельно взятого пользователя, угроза компрометации пароля злоумышленником перестаёт иметь смысл, так как параметры ввода могут сильно отличаться.

Задача аутентификации по клавиатурному почерку, сводится к задаче распознавания клавиатурного почерка конкретного пользователя с помощью двух основных групп методов [1]:

– Геометрические, использующие разные меры близости (мера Хэмминга, Евклидова мера и др.);

– Методы на основе применения искусственных нейронных сетей.

Данные имеют следующие недостатки:

- относительно невысокую точность классификации вследствие высокой аппроксимации областей решения.

- Долгое обучение, вероятность попасть в паралич обучения.

- Сложность переноса результатов обучения на более широкий круг пользователей, клавиатурный почерк которых не использовался при обучении.

- Потребность в сборе обширного массива данных для проведения обучения.

- Увеличение размера пароля для увеличения точности определения пользователя. Уникальные характеристики клавиатурного почерка могут быть обнаружены как при наборе свободного текста, так и по набору ключевой фразы.

Следует отметить, что реализация таких методов позволяет не только идентифицировать пользователей, но и определить их функциональное состояние [2].

Такой подход позволяет:

- Контролировать физическое самочувствие пользователей.

- Обеспечить обычный и надежный способ идентификации.

- Упростить запоминание пользователями сложных паролей, поскольку в качестве пароля может быть использован произвольный текст.

К плюсам использования клавиатурного почерка для аутентификации можно отнести следующее:

- Простая реализация и внедрение в систему аутентификации. Реализация включает в себя только программную часть, так как ввод текста выполняется со стандартного устройства ввода (чаще всего клавиатуры), следовательно не требуется вложений в приобретение дополнительного оборудования для получения биометрических данных пользователя. Это наиболее бюджетный способ, для реализации аутентификации по биометрическим данным пользователя.

- Не требует от пользователя никаких дополнительных действий, кроме привычных. Пользователь в любом случае для входа использует пароль, который можно использовать как парольную фразу, по которой будет проходить процесс аутентификации по клавиатурному почерку.

- Возможность проводить аутентификацию скрытно - пользователь даже может быть не в курсе, что включена дополнительная проверка при входе, а значит не сможет об этом сообщить злоумышленнику.

Главная минус использования клавиатурного почерка – это сильная зависимость от психологического и физического состояния. Например, если у человека плохое самочувствие, он может не пройти аутентификацию, так как параметры ввода символов могут сильно измениться. Также необходимо учитывать зависимость ввода текста от пользовательского опыта и технических характеристик клавиатуры [3].

Различают два типа моделей распознавания: по заранее определенному фрагменту текста и по фрагменту текста произвольного содержания. В обоих случаях для определения эталонов клавиатурного почерка оператору необходимо несколько раз ввести один или несколько фрагментов одного и того же текста. В случае необходимости анализа клавиатурного почерка на базе определенного текстового фрагмента, основу эталонов, как правило, составляют показатели времени удержания клавиши и времени между удержанием клавиш, касающихся последовательного порядка нажатия клавиш [4].

Лучшим вариантом для аутентификации по клавиатурному почерку будет использование сверточных нейронных сетей. Следует отметить, что характеристики разных типов сверточных нейронных сетей отличаются достаточно сильно, поскольку адаптированы под разные условия применения. Основываясь на результатах, определено, что при разработке нейросетевой системы распознавания целесообразно использовать нейронную сеть типа SqueezeNet.

В заключении, можно сделать вывод. Затруднения разработки средств распознавания личности по клавиатурному почерку заключаются в необходимости анализа зашумленных многомерных данных, которые соотносятся с параметрами клавиатурного почерка. Зашумленность данных объясняется прежде всего зависимостью значений указанных параметров от функционального и психоэмоционального состояния пользователя. Перспективным путем усовершенствования средств распознавания лица по клавиатурному почерку является внедрение в них модуля анализа параметров динамики клавиатурного почерка на основе сверточной нейронной сети типа SqueezeNet.

Список источников

1. Killourhy, K. S., & Maxion, R. A. (2019). Comparing anomaly-detection algorithms for keystroke dynamics. IEEE Transactions on Information Forensics and Security, 4(2), 191-200.

2. Monrose, F., & Rubin, A. (2020). Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, 16(4), 351-359.

3. Yang, J., Li, X., & Yang, J. (2019). Keystroke dynamics-based user authentication using deep belief networks. Neurocomputing, 137, 204 – 213.

4. Bhattacharya, P., & Chatterjee, S. (2018). Keystroke dynamics: A review of recent advances and future directions. Journal of Biomedical Informatics, 46(2), 365-379.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Свист О.В. - студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Алмали Ахмед Аднан Латиф - аспирант «ТГТУ».

Стародубов К.В. - к.т.н., преподаватель кафедры КБ-2 «Прикладные информационные технологии» РТУ «МИРЭА».

Вклад авторов

Свист О.В.- идея, сбор материала, обработка материала (60%).

Алмали Ахмед Аднан Латиф - частичное написание статьи (20%).

Стародубов К.В. – научное редактирование материала (20%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.8

Анализ системы контроля управления доступом в общеобразовательных учреждениях

Кирилл Андреевич Седаков[1]✉, Михаил Юрьевич Рытов[2]
[1, 2]Брянский государственный технический университет, г. Брянск, Россия
[1]sekira98@mail.ru✉, https://orcid.org/0009-0002-9284-4624
[2] ozikts@yandex.ru

Аннотация. Рассмотрены особенности системы контроля управления доступом в общеобразовательных учреждениях.

Ключевые слова: система контроля управления доступа, категорирование нарушителей целостности конфиденциальной информации.

Система контроля управления физическим доступом является одним из основных способов снизить возникновение угроз не только для конфиденциальной информации любой организации, но и для безопасности сотрудников в целом. Актуальность данной проблемы состоит в том, что в нынешних условиях безопасность людей, а особенно детей, является главной задачей общеобразовательных учреждений.

В ходе анализа данной проблемы было установлено, что система контроля управления доступа во многих общеобразовательных учреждениях практически не реализована. Образовательные учреждения являются наиболее уязвимыми для злоумышленников. В этом контексте информационная безопасность имеет важное значение в образовательных учреждениях для предотвращения атак со стороны террористов на учителей и учащихся. Риски безопасности могут быть устранены путем выявления уровня осведомленности учителей об информационной безопасности [1].

В школе, как и в любой другой организации, есть конфиденциальная информация. К ней относятся: персональные данные сотрудников и учеников, приказы, инструкции, налоговая отчетность.

Для обеспечения информационной безопасности в общеобразовательных учреждениях прежде всего необходимо определить какого типа нарушители могут нести угрозы конфиденциальности. Хотя данные учреждения наиболее зависимы и нуждаются в них.

Абсолютно во всех учреждениях общеобразовательного формата имеется охрана, которая и выполняет весь контроль за ограничением доступа на территорию школы. Сама территория ограждена забором с двумя-тремя входами и выходами.

Исходя из анализа, образуется ряд особенностей, которые существуют в большинстве общеобразовательных учреждений, а именно:

1. Персонал охраны состоит из 2-3 людей, которые заменяют друг друга посменно.
2. Сотрудники охраны относятся к специализируемой организации.
3. Наличие ограждения школьной территории.
4. Отсутствие технического оборудования, которое блокирует вход в здание школы злоумышленнику.

Делая вывод из вышеперечисленного, напрашивается вопрос: «Как улучшить данную ситуацию?»

В первую очередь должен быть квалифицированный персонал охраны, который относится к специализированным организациям.

Но несмотря на это, всегда есть вероятность нарушения режима контроля. Поэтому необходимо установить турникеты с системой доступа ограниченных лиц [2].

Любая информационная система, внедряемая на объекте, должна быть утверждена Министерством просвещения. Поэтому необходимо выделить главные требования к системе контроля управления физическим доступом со стороны школы и определить полноту их реализации в устанавливаемой системе.

Физический контроль доступа достигается за счет ограничения возможности несанкционированного прохода на территорию объекта. К самому распространенному способу ограничения относится установка турникетов и ограждений при входе – для школ это вестибюль или фойе первого этажа здания. Для соответствия системы контроля управления физическим доступом требованиям МЧС необходимо предусмотреть грамотное формирование зоны прохода, т.е. размещение ограждений и турникетов с соблюдением условий беспрепятственной эвакуации людей во время пожара.

Средняя стоимость предлагаемых на рынке аппаратно-программных комплексов системы контроля управления физическим доступом для школ с численностью от 1000 человек, включающих 1 турникет с пульта управления, составляет в среднем 70 000–170 000 руб. При этом, цена решения может варьироваться в зависимости от качества и трудностей установки. Для внедрения системы контроля управления физическим доступом в школе могут использоваться разные источники финансирования: различного уровня бюджет; деньги родителей; деньги компании-установщика.

В ходе анализа данной темы было обнаружено, что более экономный и эффективный вариант системы контроля управления физическим доступом является пропускная система, особенно в школах с большой численностью учеников. Необходимо создать пропуска, подтвержденные официальной печатью учреждения и подписью директора. Они должны отличаться и по продолжительности времени действия: постоянные для работников школы и учеников, временные для различных комиссий, приглашенных родителей и т.д.

Особенность данных учреждений состоит в том, что они имеют централизованное управление, а значит любое изменение должно касаться каждой школы. Исходя из этого следует, что данный метод идентификации сложно реализовать финансово и технически даже в пределах одного города.

В заключение можно сказать, что для обеспечения должного контроля физическим доступа в общеобразовательных учреждениях необходимо выработать нужную систему контроля, обеспечить техническими средствами и квалифицированными специалистами.

Список источников

1. Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов. —Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014 — 256 с. —ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/33430.html;

2. Аверченков, В. И. Аудит информационной безопасности: учебное пособие для вузов / В. И. Аверченков. — Брянск: Брянский государственный технический университет, 2012 — 268 с. — ISBN 978-89838-487-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/6991.html.

Статья поступила в редакцию 19.04.2023; принята к публикации 10.05.2023.

Научная статья
УДК 004.056.53

Анализ подходов к надежному удалению информации на твердотельных накопителях

Олег Сергеевич Седачев[1]✉, Дмитрий Андреевич Лысов[2], Алексей Петрович Горлов [3]
[1,2,3] Брянский государственный технический университет, Брянск, Россия
[1]sedachev57@mail.ru✉, https://orcid.org/0009-0004-7688-249X
[2]lysovdmitriia@gmail.com, https://orcid.org/0009-0003-9666-7191
[3]apgorlov@gmail.com, https://orcid.org/0009-0003-3100-3466

Аннотация. В статье указывается необходимость и актуальность надежного удаления данных с накопителей. Приводится сравнение накопителей на жестких магнитных дисках и твердотельных накопителей. Описывается принцип хранения данных на твердотельных накопителях. Рассматриваются специализированные технологии, используемые твердотельными накопителями для организации хранения и удаления информации.

Ключевые слова: информационная безопасность, удаление данных, надежное удаление, стирание информации, накопители данных, твердотельный накопитель.

Необходимость надежного удаления информации может возникнуть как при работе организации в штатном режиме, например, по истечению срока хранения, так и при нештатных ситуациях, например во избежание её утечки.

На сегодняшний день ввиду развившейся технологии производства, и, как следствие удешевления, все большую популярность обретают твердотельные накопители (Solid State Drive, SSD). Их бесспорными преимуществами перед классическими накопителями на жестких магнитных дисках (жесткими дисками) являются скорость чтения и записи данных, компактность, отсутствие шума при работе и стойкость к вибрациям и ударной нагрузке. Недостатками же являются более высокая стоимость, чем у жестких дисков и ограниченный объем записи данных.

При классическом удалении данных средствами операционной системы информация не стирается с накопителя, а лишь помечается как удаленная. При этом сохраняется возможность её восстановления, зачастую без повреждений.

Особенности, характерные для методов надежного удаления информации на жестких дисках, обусловлены их физическим принципом действия. После стирания данных на поверхности магнитных пластин все еще остается остаточная намагниченность, позволяющая восстановить информацию.

Методы удаления информации на твердотельных накопителях значительно отличаются от методов, которые используются при работе с жесткими дисками. Тем не менее, следует упомянуть, что данные, хранящиеся

на SSD, можно уничтожить вместе с самим накопителем, также, как и в случае с жестким диском. Основными методами в таком случае являются механическое, термическое, химическое уничтожение.

Для определения оптимальных и наиболее эффективных методов надежного удаления информации на твердотельном накопителе, необходимо проанализировать принцип хранения данных на носителях такого типа.

Наименьшей логической единицей данных на SSD является т.н. ячейка, представляющая собой транзистор с плавающим затвором, способным сохранять заряженное состояние при отсутствии питания. Таким образом ячейка способна либо иметь заряд, при этом являясь двоичным битом 1, либо не иметь его – двоичный бит 0. Такой тип ячейки, способный хранить лишь 1 бит, называется Single Level Cell (SLC). На сегодняшний день существуют технологии изготовления ячеек, которые могут хранить 2, 3 и даже 4 бита – Multi Level Cell (MLC), Triple Level Cell (TLC) и Quad Level Cell (QLC) соответственно. С увеличением плотности хранения информации в ячейке, снижается ресурс самих ячеек и возможно снижение скорости работы флэш-памяти. Ячейки могут физически располагаться как в один слой (Planar NAND или 2D NAND), так и в несколько (3D NAND или V-NAND). Второй способ на сегодняшний день гораздо более распространен ввиду возможности значительного увеличения объема памяти микросхем без существенного увеличения их физических размеров и возможности уменьшения количества чипов памяти на одном накопителе. Совокупность ячеек образует собой страницу объемом от 2 до 16 кбит, совокупность которых в свою очередь образует блок. Блок памяти может содержать от 128 до 256 страниц, таким образом его объем составляет от 256 кбит до 4 Мбит [4].

Для адресации флэш-памяти используется алгоритм, называемый слой флэш-трансляции (Flash Translation Layer, FTL). Его назначение заключается в том, чтобы преобразовать логические адреса накопителя в физические адреса флэш-памяти. Каждому адресу логического блока ставится в соответствие определенная область физической памяти и таким образом формируется таблица номеров логических единиц (Logical Unit Number Table, LUN table). Не существует единого стандартизированного FTL, и производители реализуют различные подходы к адресации в зависимости от типа и назначения накопителя. Тем не менее, есть 2 основных подхода к реализации FTL – блочная и страничная адресация. В первом случае размер логического блока соответствует размеру физического, а в LUN table записывается адрес физического блока и соответствующий ему адрес логического блока. Такой подход обладает недостатком в виде большого размера блока и в случае, когда необходимо перезаписать небольшой объем данных, придется перезаписать весь блок. Также за счет этого снижается скорость перезаписи данных. Тем не менее, блочная адресация обладает преимуществом в виде малого размера LUN table и находит свое применение в накопителях, имеющих небольшой объем оперативной памяти. В случае страничной адресации аналогичные записи в LUN table создаются не для блоков, а для страниц. Как следствие, растет размер LUN table, которая требует большего объема оперативной памяти. Однако, такая адресация

позволяет повысить скорость перезаписи данных. На сегодняшний день применяются гибридные алгоритмы, которые сочетают блочную и страничную адресацию [3].

Задача надежного удаления данных на твердотельных накопителях затрудняется тем, что данные в ходе работы записываются на него неравномерно. В современных твердотельных накопителях используется технология, называемая TRIM. Она позволяет поддерживать высокий уровень производительности SSD путем периодического стирания неиспользуемых блоков данных. Реализация этой процедуры возможна только при её поддержке со стороны операционной системы. Это происходит следующим образом: система передает накопителю информацию о том, что какую-то область данных необходимо очистить, контроллер помечает эту область как область удаляемых данных и производит запись в свободные ячейки без задержки на удаление этих данных. Затем контроллер во время бездействия или малой нагрузки в фоновом режиме начинает процесс очистки ранее отмеченной области. Таким образом, даже при отсутствии взаимодействия пользователя с накопителем, процедура TRIM будет выполняться. Однако, до того, как ячейки очищаются, данные на них сохраняются, и злоумышленник может попытаться воспользоваться этим. Существует 3 алгоритма работы контроллеров накопителей, от которых зависит результат вышеописанного действия. Первый из них – Non-deterministic TRIM. В случае использования контроллером данного алгоритма, он может выдать как данные из этих ячеек, так и случайную последовательность бит, причем результат может быть разным в разных попытках. Вторым алгоритмом является Deterministic TRIM (DRAT). В случае его использования контроллер будет давать одинаковое значение (вероятнее всего нули) для всех ячеек. Следующий алгоритм – Deterministic Read Zero after TRIM (DZAT), гарантированно дающий нули для всех ячеек после TRIM. На сегодняшний день наиболее распространены контроллеры, использующие второй из вышеописанных алгоритмов, а использующие первый крайне редки [2]. Наиболее простым, но ненадежным способом удаления информации с твердотельного накопителя является его быстрое форматирование. В этом случае дисковое пространство на SSD помечается как свободное для записи, но данные, ранее хранившиеся на нем, не удаляются. Запись новых данных идет просто поверх старых т.к. операционной системе было сообщено, что накопитель или раздел чист и готов для записи. После такого форматирования значительную часть ранее хранившейся информации возможно восстановить, что делает быстрое форматирование абсолютно ненадежным.

Также для твердотельных накопителей существует способ надежного удаления – Secure Erase. Он был признан Национальным Институтом Стандартов и Технологий США (NIST) как эффективный и безопасный способ удовлетворения юридических требований к санации данных. Secure Erase производит очистку накопителя на аппаратном уровне путем сбрасывания всех ячеек в состояние двоичного 0. Этот метод позволяет не только провести гарантированное удаление информации на SSD, но и сделать это с минимально возможным для него вредом. Очистка Secure Erase может быть проведена как

программными средствами, в том числе выпущенными фирмами-производителями накопителей, так и до загрузки операционной системы в UEFI, если такой функционал предусмотрен производителем материнской платы [1].

На сегодняшний день всё большую популярность обретают NVM Express (NVMe) SSD, подключаемые напрямую к материнской плате в слот m.2 и использующие высокоскоростную шину PCI Express (PCIe). Благодаря этому они имеют более высокую скорость чтения и записи данных, чем у SSD формата 2,5 дюйма, ограниченного скоростью интерфейса SATA 3. Накопители такого типа не поддерживают команды, характерные для SATA дисков, однако поддержка Secure Erase у них также имеется.

Описанная выше процедура Secure Erase является лучшим способом удаления информации с твердотельного накопителя с сохранением его работоспособности т.к. гарантированно реализует очистку всех ячеек памяти на аппаратном уровне, после чего восстановление информации невозможно.

Список источников

1. Видишь данные? Нет. Вот и я не вижу, а они есть. Уничтожаем данные на SSD-накопителях, да ещё и скорость восстанавливаем. Блог компании Kingston Technology. URL: https://habr.com/ru/companies/kingston_technology/articles/448624/

2. Заметаем следы или как безвозвратно удалить данные. Блог компании Xelent. URL: https://www.xelent.ru/blog/zametaem-sledy-ili-kak-bezvozvratno-udalit-dannye/

3. Твердотельные накопители. Внутреннее устройство и принципы их построения. Блог компании НПП «Цифровые решения». URL: https://habr.com/ru/companies/dsol/articles/504380/

4. SSD: устройство, компоненты и принципы работы. DTF. URL: https://dtf.ru/hard/46510-ssd-ustroystvo-komponenty-i-principy-raboty

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Седачев О.С. – студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горлов А.П. – к.т.н. доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Седачев О.С. – идея, сбор материала, обработка материала, частичное написание статьи (40%).

Лысов Д.А. – написание статьи, научное редактирование текста (30%).

Горлов А.П. – написание статьи, научное редактирование текста (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.53

Анализ видов объектов информатизации, которые подвергаются современным кибератакам

Олег Сергеевич Седачев[1]✉, Михаил Юрьевич Рытов[2]
[1, 2]Брянский государственный технический университет, Брянск, Россия
[1]sedachev57@mail.ru✉, https://orcid.org/0009-0004-7688-249X
[2]rmy@tu-bryansk.ru, https://ocrid.org/(orcid number)

Аннотация. В статье указывается необходимость и актуальность исследования мотивов нарушителей безопасности информации. Приводится статистика атак на российские информационные системы за 2022 год. Рассматриваются цели и последствия этих атак. Проводится анализ и прогнозирование атак на информационные системы рассматриваемых сферах. Приводятся причины активизации злоумышленников в сфере информационной безопасности. Рассматривается мотивация нарушителей безопасности информации.

Ключевые слова: информационная безопасность, нарушитель безопасности информации, мотивация нарушителя.

Нарушение безопасности информации может быть осуществлено лицами различной квалификации и в различных целях. Анализ потенциальных и реальных нарушителей информационной безопасности, их навыков и мотивации позволяет построить более эффективную систему защиты объекта информатизации.

Согласно методическому документу ФСТЭК России «Методика оценки угроз безопасности информации», утвержденному 5 февраля 2021 г., основными способами реализации угроз информационной безопасности могут являться различные уязвимости, вредоносное программное обеспечение, недекларированные возможности системного и прикладного ПО и программно-аппаратных средств и комплексов, различные программные или программно-аппаратные закладки, скрытые каналы передачи данных, физический доступ к конфиденциальной информации, нарушение безопасности при поставках программных, программно-аппаратных средств и/или услуг по установке, настройке, испытаниям, пусконаладочным работам, а также ошибки, совершаемые при создании информационных систем и сетей.

Также в вышеуказанном документе приводятся основные виды нарушителей безопасности информации, к которым относятся специальные службы иностранных государств, террористические и экстремистские группировки, криминальные структуры, отдельные физические лица (хакеры), конкурирующие организации, разработчики программных и программно-аппаратных средств, лица, обеспечивающие поставку программных,

программно-аппаратных средств и обеспечивающих систем, поставщики услуг связи и вычислительных услуг, лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ, лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и т.д.), авторизованные пользователи систем и сетей, системные администраторы и администраторы безопасности, уволенные работники [3].

Согласно статистике, собранной компанией Positive Technologies, число инцидентов информационной безопасности в России в 2022 году возросло на 20,8% по сравнению с 2021. В 67% случаев успешно проведенные атаки имели целенаправленный характер. В 2022 году произошло большое количество утечек данных, которые сами по себе являясь нарушением информационной безопасности, могут повлечь за собой совершение новых атак с использованием скомпрометированной информации. Число успешных атак, направленных на веб-ресурсы организаций, увеличилось на 56%. Наибольшее их количество пришлось на СМИ, сферу транспорта и госучреждения [1].

При атаках на российские государственные учреждения в каждом втором случае использовалось вредоносное программное обеспечение, из которых наибольшую часть составили шифровальщики (56% среди атак с применением вредоносного ПО) и вредоносные программы для удаленного управления (29%). Также при атаках на российские государственные учреждения активно использовались методы социальной инженерии, с помощью которой злоумышленники производили заражение компьютеров вредоносным ПО и похищали конфиденциальную информацию. Случаи успешного проведения таких атак часто становились причиной утечки значительного объема персональных данных граждан России. В дальнейшем число случаев, когда атаке подвергаются информационные системы государственных учреждений, будет только расти. Активно развивающаяся в России цифровизация услуг для населения безусловно станет стимулом для злоумышленников, которые смогут не только похитить персональные данные, но и повлиять на жизнь отдельного гражданина и общества в целом.

Также атакам подвергаются медицинские учреждения. В таких случаях действия злоумышленников направлены на компрометацию персональных данных пациентов, а также на вызов сбоев в работе остановку нормального функционирования медучреждения. В будущем, вероятно, продолжатся атаки как с целью похищения конфиденциальной информации, так и с целью ограничения оказания учреждениями медицинских услуг.

Кроме этого, значительному числу атак подвергаются промышленные предприятия. Их целью являются вызов сбоев в работе, нарушения технологических процессов, которые могут повлечь за собой возникновение локальных аварий и остановка деятельности предприятия. Также злоумышленники похищают конфиденциальную информацию, в частности сведения, относящихся к коммерческой тайне. Атакам подвергаются не только металлургические, машиностроительные и прочие подобные им предприятия, но и предприятия агропромышленной отрасли. Примерами могут послужить

«Мираторг», который был атакован шифровальщиком BitLocker, временно остановленный завод «Тавр», и агрохолдинг «Селятино», в котором злоумышленники получили несанкционированный доступ к системам, отвечающим за температурный режим хранения замороженной продукции, была предпринята попытка испортить продукцию. Крайне высока вероятность того, что целью атаки продолжит быть не получение финансовой выгоды, а нарушение деятельности предприятий, остановка производственных процессов и вызов аварийных ситуаций.

Также атакам подвергаются организации, относящиеся к финансовой сфере. Однако, число таких атак в 2022 году уменьшилось на 7% в сравнении с 2021 г. В 47% случаев использовались методы социальной инженерии, при помощи которых похищалась конфиденциальная информация. Кроме этого, последствием таких атак часто становится остановка бизнес-процессов и в меньшей мере финансовые потери. В настоящее время существует тенденция на снижение числа атак производимых в отношении финансовых учреждений, которая вызвана улучшением системы защиты информации и собственной отслеживаемой и контролируемой на всех этапах разработкой программного обеспечения. Злоумышленники более склонны атаковать клиентов финансовых организаций и получать от них персональные данные и финансовые средства. Тем не менее, в связи с тем, что банки создают и развивают свои экосистемы, включающие в себя системы умный дом, торговые площадки, сервисы потребления медиаконтента и т.д., высока вероятность того, что будущие атаки будут направлены именно на них.

Научные и образовательные учреждения также нередко являются целью злоумышленников. Как правило, похищается конфиденциальная информация, включающая в себя по большей части персональные данные. Кроме того, злоумышленники довольно часто используют шифровальщики для получения выкупа за расшифровку данных. В будущем вероятно увеличение числа подобных атак как с целью похищения персональных данных, так и для получения доступа к новейшим научным разработкам в различных сферах. Также следует ожидать увеличения числа атак на набирающие все большую популярность сервисы онлайн обучения [2].

Причиной повышения активности злоумышленников во многом послужил уход и, как следствие, нехватка квалифицированных кадров в сфере информационной безопасности, а также уход с российского рынка многих иностранных компаний, поставляющих средства обеспечения информационной безопасности, в связи с политической обстановкой [2]. Кроме этого, причиной увеличения числа атак на российские информационные системы являются уязвимости, обнаруживаемые в программном обеспечении с открытым исходным кодом, которое используется вместо продуктов ушедших с российского рынка компаний. Также имеет место пренебрежение работниками установленными правилами при обращении с конфиденциальной информацией. Зачастую сотрудники используют для хранения и передачи такой информации облачные хранилища, социальные сети и мессенджеры. Кроме этого,

существенной проблемой является слабая развитость и малая популярность отечественного программного обеспечения и микроэлектроники.

Также в связи со сложившейся политической ситуацией возросло число инициативных групп, состоящих из высококвалифицированных, мотивированных и, вероятно, спонсируемых недружественными России государствами лиц. Именно они ставят своей целью атаки, направленные на государственные учреждения, СМИ, транспорт и другие важные для функционирования государства сферы и отрасли [1]. Доподлинно неизвестно, являются эти люди политически, идеологически или финансово замотивированными. Существует немалая вероятность того, что они совершают атаки, сочетая все эти виды мотивации.

В будущем число атак на российские информационные системы будет расти, также будет расти и число используемых при этом средств и методов. Для предотвращения этого необходимо развитие и поддержка отечественных средств защиты информации, программного обеспечения и микроэлектроники. Также необходимо увеличить число квалифицированных мотивированных специалистов в данной области. Кроме этого, нужно усилить контроль за соблюдением установленных правил сохранения конфиденциальности информации на всех уровнях.

Список источников

1. Актуальные киберугрозы: итоги 2022 года // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/

2. Кибербезопасность 2022-2023. Тренды и прогнозы // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/

3. Методический документ. Методика оценки угроз безопасности информации: утвержден ФСТЭК России 5 февраля 2021 г.

Статья поступила в редакцию 06.07.2023; принята к публикации 10.05.2023.

Информация об авторах

Седачев О.С. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Рытов М.Ю. - к.т.н., доцент, заведующий кафедрой «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Научная статья
УДК 004.9

Цифровые сигнальные процессоры и микроконтроллеры для систем управления и средств связи

Татьяна Владимировна Скворцова [1]✉, Ольга Владимировна Вихрова [2], Игорь Владимирович Скоркин [3], Владислав Алексеевич Острецов [4]
[1,2,3,4,5] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия
[1]soultan06@bk.ru✉, https://orcid.org/0000-0003-7508-1215
[2] klen120263@mail.ru, https://orcid.org/0000-0003-3406-0226
[3] skor@mail.ru, https://orcid.org/0000-0003-3508-1375
[4] Ostretsov123@gmail.com, https://orcid.org/0000-0003-3528-0988

Аннотация. В статье рассматривается разработка цифровых сигнальных процессоров и микроконтроллеров. Приводятся их характеристики и средства отладки.

Ключевые слова: САПР, микросхема, разработка, проектирование.

В конце 70-х годов та же фирма Intel выпустила первый микроконтроллер (МК) – однокристальную микро-ЭВМ семейства MCS48, содержащую на одном кристалле помимо микропроцессорного блока обработки информации (ядра) ОЗУ, программное ПЗУ, тактовый генератор, таймер-счетчик и порты ввода/вывода. Микроконтроллеры различаются в первую очередь по разрядности обрабатываемых данных. Выпускаются 4-, 8-, 16,- и 32-разрядные МК. Есть основания ожидать появления в ближайшем будущем для ряда применений и 64-разрядных МК. Архитектура некоторых МК обеспечивает обработку данных переменной разрядности, например, существуют 4/8-разрядные или 8/16-разрядные МК, система команд которых включает и часть команд для работы с 8- или 16-разрядными данными. Например, компанией Philips Semiconductor создан 16-разрядный МК с индексом 51XA, совместимый по исходному коду с популярными 8-разрядными МК семейства MCS51 [6].

Стремление использовать микро-ЭВМ для цифровой обработки сигналов привело к созданию специализированных изделий – цифровых процессоров обработки сигналов (ЦПОС), оптимизированных для решения задач с большим количеством математических вычислений, в первую очередь типа "MAC" – операции умножения с накоплением результата. Даже самые производительные из обычных МК плохо справляются с подобными задачами. Первой подобное изделие выпустила японская фирма NEC, за ней последовали Texas Instruments, AT&T, Motorola, Analog Devices и ряд других. Подобные специализированные микросхемы и получили название "цифровые сигнальные процессоры" или цифровые процессоры обработки сигналов. По объемам продаж уже в 90-е годы они стали сопоставимыми с обычными микро-ЭВМ [6].

В зависимости от формата данных ЦПОС подразделяются на два класса: ЦПОС с плавающей запятой; ЦПОС с фиксированной запятой.

В настоящее время значительную часть рынка продаж изделий ЦПОС занимают 16 разрядные системы с форматом данных "фиксированная запятая". В связи с этим усилия ведущих зарубежных фирм направлены на разработку и 16 разрядных ядер ЦПОС и систем различной конфигурации на их основе.

К числу таких фирм относятся: Texas Instruments, USA., занимает около 45% мирового рынка ЦПОС. На базе своего низкопотребляющего ядра C20xLP разработала семейство C20x недорогих сигнальных процессоров, предназначенных для массового применения, в том числе для замены микроконтроллеров (8 типов микросхем производительностью 20 MIPS и 40 MIPS) [6].

Семейство C24x – высокоинтегрированные ЦПОС, оптимизированные для цифровых систем управления связным оборудованием, электродвигателями и т. п. (12 типов ИМС производительностью 20 MIPS и 40 MIPS). Вновь разработанный TMS320C2700 также интегрирует функции ЦПОС и микроконтроллера на одном кристалле и обеспечивает производительность до 100 MIPS [6].

Mentor Graphics Corp., разработавшая совместимые с аналогичными изделиями фирмы Texas Instruments ядра M320C25 и M320C50 производительностью 20 MIPS и 40 MIPS и степенью интеграции 25К вентилей и 40К вентилей соответственно.

Несмотря на достигнутые высокие показатели производительность/стоимость сигнальных процессоров с фиксированной запятой, решение определенного класса задач, таких, например, как обработка информации в радарах, распознавание образов и многих других специальных применениях требует применения 32 разрядных ЦПОС с форматом "плавающая запятая". Для данных микросхем разработано аппаратно-програмное обеспечение, включающее в себя аппаратный отладчик в режиме реального времени и программный эмулятор, накоплена библиотека программ для решения типовых задач и имеются специалисты для разработки управляющих программ.

Для разработки систем на основе выпускаемых НИИЭТ изделий для серии 1830 и 1874 разработаны программно-аппаратные средства отладки [1, 2, 3, 4, 5]. Аппаратную отладку программ для ИМС 1867ВМ2 можно проводить на процессорной плате TMDS 3260026, выполненной на ЦОС TMS320C26. ИМС TMS320C26 программно и аппаратно совместима с ИМС TMS320C25, за исключением обьема внутренних ОЗУ и ПЗУ, эти отличия легко отслеживаются программистом. В комплект поставки входит Ассемблер, Линкер и Отладчик.

Список источников

1. Зольников В.К. Схемотехнические методы обеспечения стойкости ЭКБ к воздействию тяжёлых заряженных частиц / Зольников В.К., Макаренко Ф.В., Журавлева И.В., Попова Е.А., Гриднев Ю.В., Литвинова Ю.А. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 35-42.

2. Победа С.А. Создание поведенческой модели LDMOS транзистора на основе искусственной MLP нейросети и ее описание на языке VERILOG-A / Победа С.А., Черных М.И., Макаренко Ф.В., Зольников К.В. // Моделирование систем и процессов. 2021. Т. 14. № 2. С. 28-34.

3. Козюков А.Е. Методы обеспечения стойкости электронной компонентной базы к одиночным событиям путем резервирования / Козюков А.Е., Зольников В.К., Евдокимова С.А., Квасов О.Н., Яковлев К.А., Платонов А.Д. // Моделирование систем и процессов. 2021. Т. 14. № 1. С. 10-16.

4. Полуэктов А.В.Моделирование колебательных процессов в пакете MVSTUDIUM / Полуэктов А.В., Зольников К.В., Анциферова В.И. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 139-148.

5. Зольников В.К. Проектирование интерфейсов сбоеустойчивых микросхем / Зольников В.К., Мозговой Н.В., Гречаный С.В., Селютин И.Н., Струков И.И. // Моделирование систем и процессов. 2020. Т. 13. № 1. С. 17-24.

6. Крюков В.П. Проектирование базовых элементов комплементарных БИС двойного назначения : диссертация ... кандидата технических наук : 05.13.12. – Воронеж, 2002.

Статья поступила в редакцию 24.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Скворцова Т.В. - к.т.н., доцент кафедры «Вычислительной техники и информационных систем» ФГБОУ ВО «ВГЛТУ».

Вихрова О.В. - преподаватель СПО кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Скоркин И.В. - аспирант ФГБОУ ВО «ВГЛТУ».

Острецов В.А. - преподаватель СПО кафедра «Информационных технологий» ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Скворцова Т.В. - идея, сбор материала, обработка материала, частичное написание статьи (25%), научное редактирование текста.

Вихрова О.В. - частичное написание статьи (25%).

Скоркин И.В. - частичное написание статьи (25%).

Острецов В.А. - частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.832

Анализ методов аутентификации и авторизации и их применение для защиты ПК от несанкционированного доступа

Даниил Андреевич Скотаренко [1] ✉, Павел Игоревич Карасев [2], Хайдар Абдулваххаб Х. Шамсулдин [3]
[1, 2]МИРЭА - Российский технологический университет, Москва, Россия
[3]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1] skotarenko.d.a2@edu.mirea.ru✉, http://orcid.org/0009-0006-5945-4092
[2]karasev@mirea.ru, https://orcid.org/0009-0009-3628-6980
[3] fit_tstu@mail.ru, https://orcid.org/0009-0006-4255-5874

Аннотация. В статье мы анализируем различные доступные методы аутентификации и авторизации и обсуждаем их применение для защиты ПК от несанкционированного доступа.

Ключевые слова: методы авторизации, информационная безопасность, защита ПК от несанкционированного доступа.

Аутентификация и авторизация - два основных механизма безопасности, используемых для защиты персональных компьютеров от несанкционированного доступа. Аутентификация включает в себя проверку личности пользователя или устройства, в то время как авторизация определяет, имеет ли пользователь или устройство права доступа к определенному ресурсу или информации. Использование надежных методов аутентификации и авторизации имеет решающее значение для защиты ПК от несанкционированного доступа, который может привести к потере конфиденциальной информации, финансовым потерям и другим нарушениям безопасности.

Программные методы аутентификации включают в себя ввод логина и пароля, использование биометрических данных (например, сканирование отпечатков пальцев), а также использование токенов доступа. Логин и пароль — это наиболее распространенный способ аутентификации. Биометрическая аутентификация становится все более популярной и может быть реализована через сканер отпечатков пальцев или камеру, распознающую лицо. Токены доступа, такие как карточки доступа или USB-ключи, могут использоваться для дополнительной защиты.

Аппаратные методы аутентификации включают в себя использование устройств, таких как смарт-карты, токены безопасности и датчики отпечатков пальцев, встроенных в компьютер или подключаемых к нему. Эти устройства обычно являются надежными и обеспечивают дополнительный уровень безопасности.

Комбинация программных и аппаратных методов аутентификации может обеспечить надежную защиту ПК. Важно выбрать наиболее подходящий метод для конкретной ситуации, учитывая уровень риска и удобство использования. Все методы аутентификации имеют свои преимущества и недостатки, и правильный выбор метода может значительно повлиять на безопасность ПК [4].

Методы авторизации включают списки контроля доступа (Access Control List), контроль доступа на основе ролей (Role-Based access control) и контроль доступа на основе атрибутов (Attribute-based access control). Списки контроля доступа (Access Control Lists, ACL) — это метод, который позволяет управлять доступом к ресурсам на основе списка пользователей и групп пользователей, имеющих права доступа. Каждый ресурс имеет свой собственный список доступа, который определяет, кто имеет право на чтение, запись или выполнение на этом ресурсе.

Контроль доступа на основе ролей (Role-Based Access Control, RBAC) — это метод, который определяет доступ к ресурсам на основе ролей пользователей в системе. Каждая роль имеет свои права доступа, и пользователи назначаются в роли в зависимости от их функций или полномочий в организации. Например, роль "администратор" может иметь права на изменение настроек системы, в то время как роль "пользователь" может иметь только права на чтение.

Контроль доступа на основе атрибутов (Attribute-Based Access Control, ABAC) — это метод, который определяет доступ к ресурсам на основе атрибутов пользователя и ресурса. Например, атрибуты могут включать уровень секретности информации, дату создания ресурса и т.д. Пользователи получают доступ на основе соответствия атрибутов пользователя и ресурса правилам доступа.

Одним из примеров ABAC является многоуровневый контроль доступа (Multilevel Security, MLS), который используется в системах, где необходимо обеспечить доступ к информации на разных уровнях секретности. Пользователям разрешено доступ только к информации на уровне секретности, не выше их уровня авторизации [5].

Применение методов аутентификации и авторизации для защиты ПК от несанкционированного доступа зависит от конкретного случая использования. Например, в корпоративной среде RBAC может использоваться для ограничения доступа к конфиденциальной информации только уполномоченным сотрудникам. В здравоохранении биометрическая аутентификация может использоваться для обеспечения доступа к записям пациентов только уполномоченного медицинского персонала.

В заключение следует отметить, что использование надежных методов аутентификации и авторизации имеет решающее значение для защиты ПК от несанкционированного доступа. Пароли, биометрические данные, смарт-карты и маркеры — все это действенные методы аутентификации, а ACL, RBAC и ABAC - эффективные методы авторизации. Применение этих методов зависит от конкретного случая использования, но их использование необходимо для поддержания безопасности персональных компьютеров и предотвращения нарушений безопасности.

Список источников

4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - С.-П., 2004. - 384 с.
5. Олифер В.Г, Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание – Санкт-Петербург, 2023. - 799-933.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Скотаренко Д.А.- студент кафедры КБ-1 «Защита информации», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» РТУ «МИРЭА».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Шамсулдин Хайдар Абдулваххаб Х. - аспирант Института автоматики и информационных технологий «ТГТУ».

Вклад авторов

Скотаренко Д.А. - идея, сбор материала, обработка материала (40%).
Карасев П.И. - написание статьи, научное редактирование текста (30%).
Шамсулдин Хайдар Абдулваххаб Х. - частичное написание статьи (30%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.051

Практические рекомендации по достижению оптимальных результатов для построения моделей глубокого обучения

Константин Владимирович Стародубов[1]✉, Юрий Юрьевич Громов[2]✉, Павел Игоревич Карасев[3]✉
[1, 3]МИРЭА - Российский технологический университет, Москва, Россия
[2]ФГБОУ ВО «ТГТУ» - Тамбовский государственный технический университет, Тамбов, Россия
[1]starodubov@mirea.ru✉, https://orcid.org/0009-0006-9088-2216
[2]gromovtambov@yandex.ru✉, https://orcid.org/0000-0003-3313-2731
[3]karasev@mirea.ru✉, https://orcid.org/0009-0009-3628-6980

Аннотация. В статье рассматривается проблема отсутствия детальных практических рекомендаций и описаний процессов, приводящих к достижению хороших результатов в глубоком обучении. Автор отмечает, что для этого требуется большое количество времени и построения гипотез, а также отмечает разрыв между результатами экспертов и менее квалифицированными практиками, использующими схожие методы. Рассматриваются гипотезы относительно выбора структуры и параметров искусственных нейронных сетей, а также предлагаются рекомендации по выбору начальной конфигурации модели. Основное внимание уделено выбору архитектуры модели и ее гиперпараметров. Авторы рекомендуют использовать зарекомендовавшие себя архитектуры, которые можно повторно использовать, и в случае необходимости создавать пользовательскую модель. Они также рекомендуют находить научные статьи, максимально приближенные к решаемой проблеме, и использовать их модель в качестве отправной точки для начальной конфигурации.

Ключевые слова: нейронные сети, оптимальные значения, глубокое обучение.

В настоящее время для того, чтобы заставить глубокие нейронные сети хорошо работать на практике, требуется затрата большого количества затрат по времени и построение гипотез. Кроме того, реальные рецепты, которые люди используют для получения хороших результатов с помощью глубокого обучения, редко документируются. В статьях не описывается процесс, который привел к их конечным результатам, чтобы представить более чистую историю, а у инженеров по машинному обучению, работающих над коммерческими проблемами, редко есть время сделать шаг назад и обобщить свой процесс. Учебники, как правило, избегают практических рекомендаций и отдают приоритет фундаментальным принципам, даже если их авторы обладают необходимым опытом прикладной работы, чтобы давать полезные советы. В научных материалах на настоящий момент отсутствуют какой-либо попытки

объяснить, как добиться хороших результатов с помощью глубокого обучения. Существует огромная пропасть между результатами, достигнутыми экспертами по глубокому обучению, и менее квалифицированные практики, использующие внешне схожие методы. В то же время эти самые эксперты с готовностью признают, что некоторое из того, что они делают, может быть неоправданным. По мере развития глубокого обучения и его все большего влияния на мир обществу требуется больше ресурсов, охватывающих полезные советы, включая все практические детали, которые могут быть столь важны для получения хороших результатов [1].

В ходе анализа материалов и документов были сформулированы следующие гипотезы, относящиеся к выбору структуры и параметров искусственной нейронной сети.

При запуске нового проекта попробуйте повторно использовать модель, которая уже работает.

• Выберите хорошо зарекомендовавшую себя модель, часто используемую архитектуру модели, чтобы сначала приступить к работе. Всегда есть возможность позже создать пользовательскую модель.

• Архитектуры моделей обычно имеют различные гиперпараметры, которые определяют размер модели и другие детали (например, количество слоев, ширину слоя, тип функции активации).

• Таким образом, выбор архитектуры действительно означает выбор семейства различных моделей (по одной для каждой настройки гиперпараметров модели).

• По возможности найти научную статью, в которой рассматривается что-то, максимально приближенное к рассматриваемой проблеме, и воспроизведите эту модель в качестве отправной точки.

Для выбора начальной конфигурации необходимо воспользоваться следующими гипотезами:

• Перед началом настройки гиперпараметра определить отправную точку. Это включает в себя указание конфигурации модели (например, количества слоев), гиперпараметров оптимизатора (например, скорости обучения) и количество шагов обучения.

• Для определения этой начальной конфигурации потребуется несколько настроенных вручную обучающих запусков и метод проб и ошибок.

• Основной принцип заключается в том, чтобы найти простую, относительно быструю, с относительно низким потреблением ресурсов конфигурацию, которая обеспечивает "разумный" результат.

• «Простота» означает, что по возможности следует избегать сложных конфигураций. Даже если сложные конфигурации окажутся полезными в будущем, добавление их в первоначальную конфигурацию чревато потерей времени на настройку бесполезных функций и/ или ненужными усложнениями.

• Начинать следует с постоянной скорости обучения, прежде чем добавлять причудливые графики затухания.

• Выбор начальной конфигурации, которая является быстрой и потребляет минимальные ресурсы, сделает настройку гиперпараметров намного более эффективной.

• Начинайте с модели меньшего размера.

• "Разумная" производительность зависит от проблемы, но, как минимум, означает, что обученная модель работает намного лучше, чем случайный случай в наборе проверки (хотя это может быть достаточно плохо, чтобы не стоило развертывать).

Выбор количества тренировочных шагов предполагает балансировку следующего напряжения:

• С одной стороны, обучение большему количеству шагов может повысить производительность и упростить настройку гиперпараметров [2].

• С другой стороны, тренировка на меньшее количество шагов означает, что каждый тренировочный прогон работает быстрее и использует меньше ресурсов, повышая эффективность настройки за счет сокращения времени между циклами и позволяя проводить больше экспериментов параллельно. Более того, если изначально выбран неоправданно большой бюджет шагов, может быть трудно изменить его в дальнейшем, например, после того, как график скорости обучения будет настроен на это количество шагов.

В заключении можно отметить, что глубокое обучение является мощным инструментом для решения сложных задач, но для достижения хороших результатов требуется не только теоретический базис, но и практический опыт. Использование уже существующих моделей и архитектур может значительно сэкономить время и улучшить результаты. Кроме того, важно начать с определения отправной точки для выбора гиперпараметров. В целом, более практическое и конкретное обучение может помочь в заполнении пропасти между экспертами и менее квалифицированными практиками в области глубокого обучения и повысить эффективность его применения в различных областях.

Список источников

1. Deep Learning Tuning Playbook URL: https://github.com/google-research/tuning_playbook/blob/main/README.md (дата обращения: 20.04.23).

2. Measuring the Effects of Data Parallelism on Neural Network Training URL: https://arxiv.org/abs/1811.03600 (дата обращения: 20.04.23).

Статья поступила в редакцию 21.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Стародубов К.В. - к.т.н., доцент кафедры КБ-2 РТУ МИРЭА.

Громов Ю.Ю. – д.т.н. профессор, Институт автоматики и информационных технологий «ТГТУ».

Карасев П.И. - к.т.н., доцент кафедры КБ-1 «Защита информации» РТУ «МИРЭА».

Вклад авторов

Стародубов К.В. - идея, сбор материала, обработка материала, частичное написание статьи (60%).

Громов Ю.Ю. – помощь в анализе информации, научное редактирование текста (20%).

Карасев П.И. – рекомендации по оформлению статьи, научное редактирование текста (20%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.051

Разработка сценариев создания правил корреляции SIEM на основе модели угроз и профиля нарушителя информационной безопасности

Константин Владимирович Стародубов[1]✉, Виктор Андреевич Зайцев[2], Виктор Владимирович Суменков[3] , Владислав Валерьевич Павлов[4]
[1,2,3,4]РТУ МИРЭА, Москва, Россия
[1]✉starodubov@mirea.ru✉, https://orcid.org/
[2]vit130800@yandex.ru, https://orcid.org/0009-0002-6311-9925
[3]sumenkov.vitya2909@yandex.ru, https://orcid.org/0009-0007-2061-1115
[4]georhecitrulline@mail.ru, https://orcid.org/0009-0005-8386-2232

Аннотация. В статье описывается разработка сценариев создания правил корреляции для систем безопасности информации, используя модель угроз и профиль нарушителя. Она включает основные принципы работы с системой безопасности информации, описание модели угроз и профиля нарушителя, сценарии использования правил корреляции SIEM в различных ситуациях, таких как обнаружение внутренних и внешних атак, а также атак, основанных на социальной инженерии. Результаты экспериментов, проведенных авторами, подтверждают эффективность использования разработанных на основе модели угроз и профиля нарушителя сценариев создания правил корреляции SIEM для обеспечения безопасности информации.

Ключевые слова: SIEM, информационная безопасность, модель, угроза, правила корреляции, модель нарушителя.

В настоящее время все большую популярность приобретают SIEM-системы, которые позволяют решать множество задач, связанных с обеспечением безопасности информации. Они позволяют собирать и нормализовать данные из различных источников, классифицировать и коррелировать события, создавать инциденты и предоставлять инструменты для их расследования. Благодаря возможности хранения информации о событиях и инцидентах на длительный период времени и быстрого доступа к ней, SIEM-системы становятся незаменимым инструментом для обеспечения безопасности информации. Также SIEM входит в число обязательных систем ИБ по нескольким стандартам требования регуляторов: ФЗ-187, приказ ФСТЭК 21, 31, ГОСТ Р ИСО/МЭК 27002-2021, ГОСТ Р 57580.1. На основании ФЗ-187 все SIEM-системы обязаны быть подключены к ГосСОПКА.

Цель данной статьи заключается в разработке сценариев создания правил корреляции SIEM на основе модели угроз и профиля нарушителя информационной безопасности. В статье будет рассмотрена модель угроз и профиль нарушителя, который представляет наибольшую угрозу для системы информационной безопасности, а также методы создания правил корреляции на

их основе. Результатом работы станут готовые сценарии создания правил корреляции, которые можно будет использовать для обеспечения безопасности информации.

Модель угроз и нарушителя информационной безопасности позволяет идентифицировать потенциальные угрозы для системы и оценить возможности и мотивы нарушителя. Это позволяет определить, какие типы атак могут быть направлены на систему, какие уязвимости следует защитить и на основе полученных данных создать требуемые правила корреляции.

Правила корреляции SIEM позволяют обнаруживать и предупреждать об атаках и инцидентах информационной безопасности, используя различные источники данных, например, журналы событий, системные и сетевые журналы, данные о пользователе и т.д. Правила корреляции SIEM могут использоваться для автоматического обнаружения и реагирования на различные виды атак, основываясь на специфических правилах, например, повторяющиеся неудачные попытки входа в систему, необычные запросы или трафик на сети и т.д.

Таким образом, правила корреляции SIEM и модель угроз и нарушителя информационной безопасности могут использоваться совместно для обнаружения и предотвращения различных видов атак и инцидентов информационной безопасности. Модель угроз и нарушителя может быть использована для определения, какие виды атак наиболее вероятны, а правила корреляции SIEM могут быть настроены для обнаружения этих атак и предотвращения их.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

- внешние нарушители – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;
- внутренние нарушители – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Для достижения целей данной статьи мы остановились на администраторе ИБ, так как данный вид нарушителя представляет наибольшую угрозу для системы информационной безопасности.

Администратор безопасности - внутренний нарушитель с базовыми возможностями, может иметь разный уровень прав доступа к информационным ресурсам и компонентам систем и сетей.

Нарушитель может использовать различные методы и инструменты для получения доступа к конфиденциальной информации и нанесения вреда компьютерным системам и сетям. Поэтому, разработка эффективных мер безопасности и защиты информации является критически важной задачей для любой организации.

Приведенные выше угрозы применимы для любой IT-компании и позволяют выбрать следующие сценарии по созданию правил корреляции:

1. Раннее предупреждение о сканировании, распространении сетевых червей и т.д. Триггер: Предупреждение о 15 или более событиях

отбрасывания/отклонения/запрета брандмауэра с одного IP-адреса в течение одной минуты. Источники событий: Брандмауэры, маршрутизаторы и коммутаторы

Результат: Предотвращение распространения сетевых червей в корпоративной сети.

2. Оповещение при обнаружении вируса, шпионского или другого вредоносного ПО на хосте. Триггер: Оповещение при обнаружении на одном узле идентифицируемой части вредоносного ПО Источники событий: Антивирус, HIPS, детекторы поведенческих аномалий сети/системы.

Результат: Предотвращение распространения вируса, шпионского или другого вредоносного ПО.

3. Оповещать, когда контролируемый источник журнала не отправил событие в течение 1 часа (время зависит от устройства).Триггер: Устройство сбора журнала должно периодически создавать событие, чтобы показать, сколько событий было получено, и что это число больше 0. Источники событий: Устройство сбора журналов.

Результат: Своевременное получение событий.

В результате работы были разработаны готовые сценарии создания правил корреляции SIEM на основе модели угроз и профиля нарушителя информационной безопасности, на их основе были представлены методы создания правил корреляции. Полученные сценарии можно использовать для обеспечения безопасности информации. Данная статья поможет повысить уровень безопасности информации и снизить риски ее утечки или кражи.

Список источников

1. «The Common Attack Pattern Enumeration and Classification (CAPEC)». Механизмы атаки. URL: https://capec.mitre.org/data/definitions/1000.html (дата обращения: 10.04.23)

2. Федеральная служба по техническому и экспортному контролю. Методологический документ. Методика оценки угроз безопасности информации от 5.02.21. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения: 10.04.23).

3. Федеральная служба по техническому и экспортному контролю. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/ (дата обращения: 11.04.23).

4. Дмитрий Кузнецов. ГосСОПКА: что такое, зачем нужна и как устроена. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/gossopka-what-is-it-how-it-works (дата обращения: 17.04.23).

5. Громов Ю.Ю., Стародубов К.В., Карасев П.И., Зайцев В.А., Суменков В.В. История, тенденции развития и роль SIEM-систем. URL: https://elibrary.ru/item.asp?id=50143217 (дата обращения: 17.04.23).

Статья поступила в редакцию 21.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Стародубов К.В. - к.т.н., доцент кафедры КБ-2 «Прикладные информационные технологии» РТУ МИРЭА.

Зайцев В.А. – студент кафедры КБ-2 «Прикладные информационные технологии», РТУ «МИРЭА».

Суменков В.В. – студент кафедры КБ-2 «Прикладные информационные технологии», РТУ «МИРЭА».

Павлов В.В. – магистр кафедры КБ-4 «Интеллектуальные системы информационной безопасности», РТУ «МИРЭА».

Вклад авторов

Стародубов К.В. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Зайцев В.А. – помощь в анализе информации, научное редактирование текста (20%).

Суменков В.В. – рекомендации по оформлению статьи, научное редактирование текста (20%).

Павлов В.В. – редактирование текста, написание выводов по работе (10%).

Конфликт интересов отсутствует.

Обзорная статья
УДК 004:056

Угрозы и атаки в области кибербезопасности

Дарья Алексеевна Терехова ✉
Брянский государственный технический университет, Брянск, Россия
darateretehova5@gmail.com✉, http://orcid.org/0000-0002-0027-3442

Аннотация. Угрозы и атаки в настоящее время являются главной проблемой в области кибербезопасности. Злоумышленники постоянно ищут способ заполучить необходимые им сведения, используя самые разные методы, при этом создавая новые и совершенствуя старые. Чтобы себя обезопасить, необходимо знать об источниках, угрозах и атаках в области кибербезопасности как можно больше.

***Ключевые слова*:** кибербезопасность, угроза, атака, вредоносное программное обеспечение, источник.

В современном мире, где большое количество информации хранится в электронном виде и передается по сетям, кибербезопасность становится все более важной. Каждый день компьютерные системы подвергаются угрозам и атакам, которые могут привести к утечке конфиденциальной информации, нарушению работы системы или даже краже денежных средств.

Распространенные источники киберугроз:

1. Внешние носители информации.
2. Хакеры.
3. Враждебные государства.
4. Террористические организации.
5. Вредоносные инсайдеры (сотрудники, которые имеют законный доступ к активам компании и злоупотребляют своими привилегиями для кражи информации или повреждения компьютерных систем в целях экономической или личной выгоды).

Кибербезопасность (безопасность информационных технологий) — это действия по защите компьютерных систем, сетей, устройств и данных от кибератак, киберпреступлений и несанкционированного доступа. Она включает в себя меры по обеспечению конфиденциальности, целостности и доступности данных, а также защиту от вредоносных программ, фишинга и других видов киберугроз.

Угроза кибербезопасности — это преднамеренная попытка получить доступ к каким-либо сведениям. Злоумышленники постоянно совершенствуют свои методы атак (кибератак), чтобы обойти инструменты обнаружения и использовать новые уязвимости, но также они используют некоторые известные методы, к которым можно быть готовым. На данный момент существует несколько типов угроз кибербезопасности:

1. Вредоносные программы (вирусы, трояны, черви и т.д.). Данный тип является наиболее распространенным из известных угроз. Вредоносное программное обеспечение (ВПО) может быть установлено на компьютер без согласия пользователя. Оно может использоваться для сбора конфиденциальной информации, перехвата паролей или даже удаленного управления компьютером. Часто ВПО распространяется через электронную почту, социальные сети или вредоносные сайты.

2. Социальная инженерия — это процесс манипулирования людьми, чтобы они совершили определенные действия, которые могут привести к утечке конфиденциальной информации или нарушению безопасности. Это может быть использовано для получения доступа к паролям, личным данным или другой конфиденциальной информации.

3. Фишинг (мошенничество с использованием электронной почты, социальных сетей и т.д.). Целью фишинговой атаки является получение конфиденциальной информации, такой как логины, пароли или данные банковских карт. Данный тип угроз заключается в отправке электронных писем или сообщений, которые выглядят как официальные запросы от банков, интернет-магазинов или других организаций.

4. Программа-шантажист (вредоносная программа шифрует файлы, блокируя доступ к ним). Злоумышленники часто извлекают данные во время атаки программы-шантажиста и угрожают опубликовать их, если не получат выкуп. В обмен на ключ для расшифровки жертвы должны заплатить выкуп, как правило, в криптовалюте. Не все ключи расшифровки работают, поэтому оплата не гарантирует, что файлы будут восстановлены.

5. Кибершпионаж (получение конфиденциальной информации государственными или корпоративными шпионами).

6. Внутренние угрозы. При внутренней угрозе люди, уже имеющие доступ к некоторым системам, становятся причиной нарушения безопасности или финансовых потерь. Иногда это происходит непреднамеренно. Однако некоторые внутренние угрозы являются намеренными.

7. Целенаправленная устойчивая угроза. При угрозах этого типа злоумышленники получают доступ к системам, но остаются незамеченными в течение длительного периода времени. Преступники исследуют системы целевой компании и похищают данные, не вызывая никаких защитных контрмер [6].

Что касается атак кибербезопасности. К ним в основном относятся:

1. Атака отказа в обслуживании (DDoS)
2. Межсетевые атаки (MITM)
3. Атаки на слабые пароли и учетные записи
4. Взлом через уязвимости в ПО
5. Физический доступ к устройствам и системам
6. Атаки от ВПО (вирусы, черви, трояны и т.п.)

Для защиты от киберугроз необходимо использовать комплексный подход, который включает в себя использование антивирусного программного обеспечения, регулярное обновление программного обеспечения, установку

сильных паролей и двухфакторной аутентификации, а также следование правилам, которые поддерживаются правоохранительными органами.

В целом, кибербезопасность является важной проблемой, которая требует внимания и действий со стороны каждого пользователя компьютера и организации. Угрозы и атаки в области кибербезопасности могут привести к серьезным последствиям, поэтому необходимо принимать все меры для защиты своей информации и систем.

Список источников

1. Сорокин, З. Идем в атаку / З. Сорокин. - М.: ДОСААФ, 2016. - 200 с.
2. Шафрин Ю.А. 1500 основных понятий, терминов и практических советов для пользователей персональным компьютером. – М.: Дрофа, 2001. - 272 с.
3. Фостер, Дж.С. Защита от взлома: сокеты, эксплойты, shell-код: выявление уязвимостей операционных систем и прикладных программ к атакам хакеров / Дж.С. Фостер. - М.: ДМК, 2009. - 784 с.
4. Чирилло, Д. Обнаружение хакерских атак / Д. Чирилло. - М.: СПб: Питер, 2010. - 864 с.
5. Фридланд А.Я. Информатика и компьютерные технологии: Основные термины: Толков. Слов.: Более 1000 базовых понятий и терминов. – 3-е изд. испр. и доп./ А.Я. Фридланд, Л.С. Ханамирова, И.А. Фридланд. – М.: ООО «Издательство Астрель», 2003. - 272 с.
6. https://www.microsoft.com/ru-ru/security/business/security-101/what-is-cybersecurity

Статья поступила в редакцию 22.03.2023; принята к публикации 10.05.2023.

Научная статья
УДК 004:056

Анализ защиты протокола стандарта WPS

Никита Сергеевич Хрущев[1]✉, Альберт Русланович Зайдуллин[2], Роман Михайлович Башкиров[3], Юрий Юрьевич Громов[4], Абд Али Хуссейн Наджми Абд Али[5]
[1,2,3]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[4,5]Тамбовский государственный технический университет, Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0004-5814-2893
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0005-2857-9290
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0001-4442-5217
[4]gromov@is.tstu.ru, https://orcid.org/0000-0003-3313-2731
[5] fit_tstu@mail.ru

Аннотация. В статье представлен обзор спецификации стандарта WPS, предназначенного для настройки беспроводных Wi-Fi сетей. Рассматриваются атаки на протокол регистрации WPS. Приводятся рекомендации по защите беспроводных сетей от рассмотренных атак.

Ключевые слова: анализ защиты, стандарт WPS, протокол.

Wi-Fi – технология построения беспроводных локальных сетей на базе семейства стандартов IEEE 802.11. Сегодня технологию Wi-Fi поддерживают практически все современные электронные устройства, включая персональные компьютеры, игровые консоли, смартфоны, цифровые камеры, планшетные компьютеры, аудиоплееры и современные принтеры. Wi Fi используется не только в домашних сетях, но и в сетях предприятий и госучреждений.

Так как отсутствие физического соединения делает беспроводные сети более уязвимыми чем проводные Ethernet сети, то разработчиками технологи Wi-Fi был предложен ряд мер для защиты передаваемых данных [4].

Несмотря на то, что стандарт WPS был презентован как безопасный и простой способ настройки беспроводных сетей, при его разработке, а также во многих реализациях был допущен ряд существенных недостатков, позволяющих злоумышленнику получить несанкционированный доступ даже к хорошо защищённой беспроводной сети [1].

В данной работе будет проведён обзор стандарта WPS, рассмотрен протокол регистрации нового устройства в беспроводной сети с использованием WPS, а также будет представлен разбор известных атак на данный протокол.

Спецификация стандарта WPS предусматривает два способа развертывания и настройки защищенной беспроводной сети [4]:

– первый способ «Out-of-Band» – позволяет произвести настройку

параметров беспроводной сети Wi-Fi по стандартам Ethernet/UPnP (также стандарт WPS предусматривает возможность использования NFC);

– второй способ «In-Band» – позволяет произвести настройку параметров беспроводной сети Wi-Fi по стандартам IEEE 802.11/EAP.

Остановимся на рассмотрении второго способа, так как именно он представляет наибольший интерес со стороны злоумышленника, так как при использовании данного способа существует набор уязвимостей, используя которые можно получить несанкционированный доступ к беспроводной сети [4].

Второй способ настройки параметров беспроводной сети включает в себя три варианта добавления нового устройства к беспроводной сети [4]:

– вариант с использованием специальной кнопки «Push Button Connect»;

– вариант с использованием внутреннего регистратора (регистрация нового устройства инициируется точкой доступа);

– вариант с использованием внешнего регистратора (регистрация нового устройства инициируется подключаемым устройством).

Остановимся на процедуре проверки WPS PIN, состоящий из 8 цифр, при этом последняя цифра – контрольная сумма, вычисляемая на основе предыдущих цифр. Наличие контрольной суммы необходимо для того, чтобы известить пользователя о том, что PIN введен некорректен до использования в протоколе.

1. После включения точка доступа рассылает пакеты «Beacon», в которых содержится информация о наличии поддержки технологии WPS.

2. Подключаемое устройство, получив информацию о поддержке точкой доступа технологии WPS, отправляет точке доступа свои идентификационные данные в запросе на установление защищенного соединения «Probe request». В ответе «Probe-response» точка доступа отправляет свои идентификационные данные.

3. У пользователя запрашивается PIN, необходимый для установки защищенного соединения.

4. Между подключаемым устройством устанавливается соединение по протоколу 802.1X и выполняется расширяемый протокол аутентификации EAP.

5. Точка доступа и подключаемое устройство обмениваются сообщениями M1-M8. Назначение и содержание данных сообщений будет представлено ниже.

6. Точка доступа и подключаемое устройство обмениваются сообщениями «EAP-Done», «EAP-ACK», «EAP-Fail», означающими завершение сессии протокола регистрации.

7. Клиентское устройство пере-подключается к точке доступа, используя для авторизации данные и настройки, полученные в ходе выполнения протокола регистрации [4].

Перед началом протокола регистрации WPS PIN конвертируется в два 128 битных числа следующим образом:

– PSK1 – первые 128 бит от $HMAC_{AuthKey}$ (первые 4 цифры WPS PIN);

– PSK2 – первые 128 бит от $HMAC_{AuthKey}$ (вторые 4 цифры WPS PIN).

Полученные значения PSK1 и PSK2 используются в R-Hash1 и R-Hash2 для доказательства того, что подключаемому устройству известен корректный WPS PIN точки доступа.

Далее подключаемое устройство генерирует две 128 битные случайные последовательности R-S1, R-S2 которые также используются при вычислении в R Hash1 и R-Hash2. После получения R-Hash1 и R-Hash2, а также шифрованного значения $ENC_{keyWrapKey}$(R-S1), в сообщении M4, точка доступа расшифровывает значение R-S1 и вычисляет R-Hash1'.

Далее точка доступа сравнивает вычисленное значение R-Hash1' и значение R Hash1, полученное от подключаемого устройства.

Если значения совпадают, то это означает, что первые четыре символа WPS PIN были введены верно.

Аналогично осуществляется проверка последних четырех символов WPS PIN после отправки подключаемым устройством сообщения M6.

Если обе части PIN были введены корректно, то точка доступа отправляет сообщение M7 в котором содержатся настройки беспроводной сети, в том числе имя беспроводной сети и её пароль

В случае, если процесс WPS аутентификации не выполняется на каком-либо шаге, то точка доступа отправляет сообщение EAP-NACK, после чего соединение с подключаемым устройством разрывается.

Атака на WPS использует уязвимость, допущенную при разработке стандарта, которая позволяет атакующему разделить WPS PIN на две части, и раздельно получать информацию о корректности этих частей PIN из ответов точки доступа [2].

Данная атака позволяет сократить количество вариантов ключа с 10^8 до $10^4 + 10^4$. Но это еще не все, так как последняя цифра PIN – контрольная сумма, то количество вариантов второй части сокращается до 10^3. Тем самым общее количество вариантов PIN сокращается до $10^3 + 10^4$.

Еще одна атака на протокол WPS была предложена специалистом по компьютерной безопасности Домиником Бонгардом. Данная атака использует уязвимости, допущенные в реализациях протокола регистрации рядом производителей сетевого оборудования. Для осуществления атаки не требуется постоянного подключения злоумышленника к точке доступа [4].

Уязвимость, позволяющая осуществить данную атаку, заключается в генерации случайных чисел (E-S1 и E-S2) на многих точках доступа.

Так, если атакующий сможет узнать значения E-S1 и E-S2 после получения от точки доступа сообщения M3, то он сможет беспрепятственно подобрать WPS PIN путем перебора 11 000 возможных вариантов.

Так, если обмен сообщениями M1 и M3 происходит в одну и ту же секунду, то E-S1 = E-S2 = N1. Если в течение нескольких секунд, то задача подбора WPS PIN сводится к определению начального состояния генератора псевдослучайных последовательностей на основе значения N1.

Использование технологии WPS является небезопасным, это обусловлено уязвимостями, допущенными как при разработке стандарта, так и уязвимостями, допущенными производителями сетевого оборудования при реализации спецификации WPS в своих устройствах.

Самый верный способ защиты – отключение WPS в настройках точки доступа до того, как будет выпушена новая версия стандарта WPS, устраняющая

существующие на данный момент уязвимости [4].

Список источников

1. Wi-Fi Protected Setup Specification Version 1.0h. URL: cfile28.uf.tistory.com/attach/16132E3C50FCFFCB3EC74E.

2. Stefan Viehböck. Brute forcing Wi-Fi Protected Setup. 2011. URL: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

3. Dominique Boungard. Offline bruteforce attack on Wi-Fi Protected Setup. 2014. URL: http://www.slideshare.net/0xcite/offline-bruteforce -attack-on-wifi-protected-setup.

4. Губсков Ю.А., Болдырев А.В., Верещагин Д.Ю., Киселёв М.Д., Манюхин В.А. Анализ уязвимостей стандарта wps и пути их устранения // Информация и безопасность. – 2017. –№ 1. - Т. 20. – С. 81 – 88.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Хрущев Н.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Зайдуллин А.Р. – оператор научной роты войск радиоэлектронной борьбы.

Башкиров Р.М. – младший научный сотрудник научной роты войск радиоэлектронной борьбы.

Громов Ю.Ю. – директор Института автоматики и информационных технологий.

Вклад авторов

Хрущев Н.С. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Зайдуллин А.Р. – сбор материала, обработка материала, частичное написание статьи (25%).

Башкиров Р.М. – сбор материала, обработка материала, частичное написание статьи (25%).

Громов Ю.Ю. – сбор материала, обработка материала, частичное написание статьи (25%).

Абд Али Хуссейн Наджми Абд Али – сбор материала.

Конфликт интересов отсутствует.

Научная статья
УДК 623:74

Анализ информационной безопасности беспилотных авиационных систем с использованием интеллектуального программного комплекса «Аналитик»

Никита Сергеевич Хрущев[1]✉, Илья Александрович Омельченко[2], Иван Сергеевич Гришин[3], Виктор Васильевич Шатских[4]
[1,2,3,4]Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1]nauchnajarota@yandex.ru✉, https://orcid.org/0009-0004-5814-2893
[2]nauchnajarota@yandex.ru, https://orcid.org/0009-0002-5941-9589
[3]nauchnajarota@yandex.ru, https://orcid.org/0009-0000-6355-4551
[4]nauchnajarota@yandex.ru, https://orcid.org/0009-0009-7547-9419

Аннотация. В статье рассматривается способ оценки сетевых комплексов бортовых радиоэлектронных объектов воздушных судов, с помощью разрабатываемого научной ротой войск радиоэлектронной борьбы специальным интеллектуальным программным комплексом «Аналитик».

Ключевые слова: программный комплекс, уязвимости, сканер сетевой безопасности, атаки.

С развитием информационных и вычислительных сетей увеличилось появление уязвимостей, предоставляющих возможность как случайного, так и преднамеренного вмешательства в информационные системы. Беспилотные летательные аппараты (БПЛА) могут оказаться объектом информационного противоборства при осуществлении информационного воздействия, результатом которого будет модификация его свойств как информационной системы [1]. Злоумышленники, получившие доступ к работе бортовой системы БПЛА, могут получить доступ к содержащейся в ней информации и исказить ее достоверность [2].

На основе анализа информационных потоков, циркулирующих в БПЛА, наибольший интерес представляют следующие информационные блоки [5]:

– ключевая информация;

– команды управления БПЛА и аппаратуры;

– данные позиционирования БПЛА в пространстве;

– специальная информация (данные разведки, команды управления в рамках боевой информационной системы);

– телеметрическая информация.

Уязвимость информационной системы (ИС) – свойство ИС, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

К потенциальным уязвимостям БПЛА можно отнести [5]:

– необходимость постоянного обмена информацией с наземными пунктами управления;

– использование внешней системы позиционирования БПЛА в пространстве;

– открытые потоки телеметрической информации;

– отсутствие или ограниченное использование средств криптографической защиты информации (СКЗИ);

– высокая вероятность компрометации ключевой информации и СКЗИ.

Сетевые сканеры направлены на решение следующих задач: идентификация и анализ уязвимостей, инвентаризация ресурсов (таких как операционная система, программное обеспечение и устройства сети) и формирование отчетов, которые содержат описание уязвимостей и варианты их устранения [3, 4].

Большинство современных сканеров безопасности сети работает по нижеперечисленным принципам:

– сбор информации о сети, идентификация всех активных устройств и сервисов, запущенных на них;

– обнаружение потенциальных уязвимостей;

– подтверждение выбранных уязвимостей, для чего используются специфические методы и моделируются атаки;

– формирование отчетов;

– автоматическое устранение уязвимостей.

В данной работе для поиска уязвимостей устройств предлагается использовать специальный интеллектуальный программный комплекс «Аналитик». В отличие от существующих сканеров сетевой безопасности, программный комплекс имеет следующие преимущества [6]:

– высокая скорость проверки доступности и сканирование портов;

– противодействие обнаружению процесса сканирования;

– автоматизированный процесс сбора и анализа результатов сканирования;

– определение местоположения РЭО по результатам сканирования;

– определение уязвимостей программного и аппаратного обеспечения сканируемого объекта.

Комплекс «Аналитик» имеет модульную архитектуру, которая разделена на несколько групп: модули анализа проводных и беспроводных сетей устройств (взаимодействие с сетью), модули обнаружения и эксплуатации уязвимостей программного обеспечения и модули взаимодействия с базами данных.

Рассмотрим часть разрабатываемых модулей программного комплекса. Модуль сканирования сети осуществляет процесс скрытого поиска радиоэлектронных объектов. Параметры настройки сканирования позволяют выбрать диапазон сканируемых IP-адресов, метод осуществления процесса сканирования. В результате был просканирован участок сети, где производился опрос объектов через 80 порт, с помощью метода TCP SYN (рис. 1).

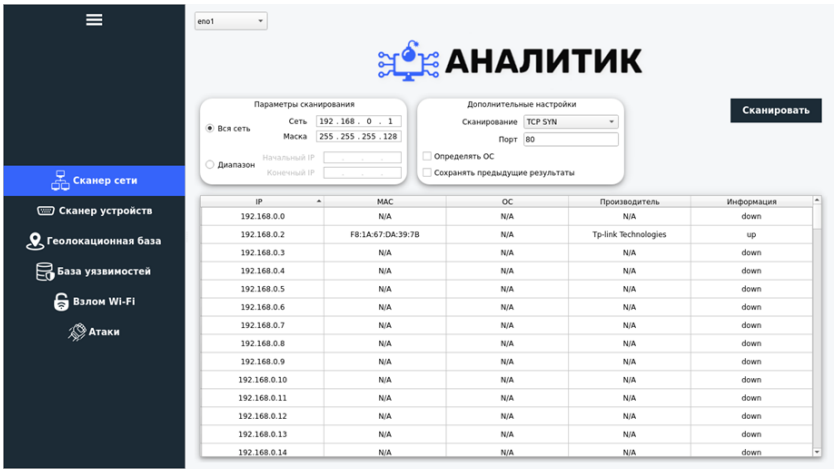

Рис. 1. Результат работы модуля «Сканер сети»

Модуль сканирования портов предназначен для скрытного выявления работы сервисов и служб, запущенных на сканируемом устройстве. Параметры настройки сканирования позволяют выбрать метод сканирования, диапазоны сканируемых портов и адресов радиоэлектронных объектов в сети, а также протокол передачи данных. Было произведено сканирование выявленного объекта сети, с помощью метода SYN SCAN протоколов TCP и UDP в диапазоне от 0 до 2500 порта и в результате чего были обнаружены запущенные сервисы и службы (рис. 2) [6].

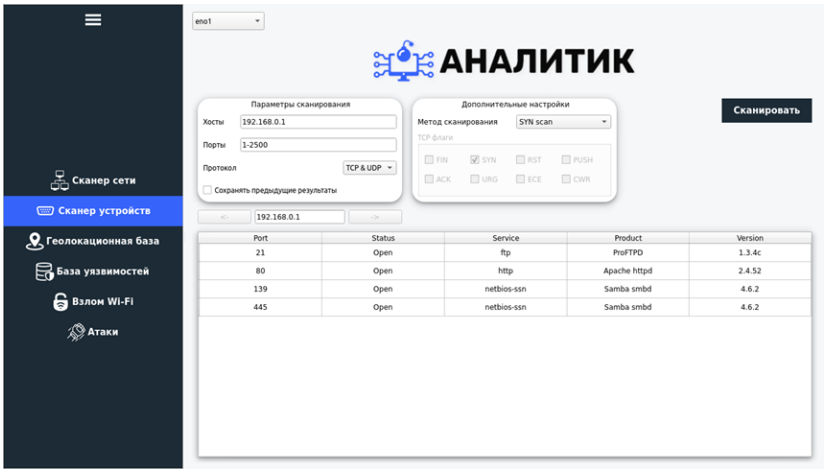

Рис. 2. Результат работы модуля «Сканер устройств»

Результаты работы показанных модулей используются для организации специальных программных воздействий, хранящихся в базе уязвимостей. База уязвимостей содержит описание уязвимости на английском языке, список подверженного этой уязвимости программного обеспечения, условия использования и вредоносный код эксплуатации. Также имеется геолокационная база данных, с помощью которой можно определить географическое местоположение введенного IP-адреса и она также автоматически формирует и отображает перечень стран, регионов, городов и соответствующих им диапазонов IP-адресов [6].

Таким образом, программный комплекс позволяет ускорить процесс

анализа уязвимостей в используемом аппаратном и программном обеспечении сетевой информационной системы бортового оборудования БПЛА, что оказывает существенное влияние на управление информационной безопасностью.

Список источников

1. Манойло А.В. Государственная информационная политика в особых условиях: монография. М.: Изд. МИФИ, 2003. 306 с.

2. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна // Вопросы кибербезопасности. 2018. № 4. С. 9–20.

3. Weidman G. Penetration testing: a hands-on introduction to hacking // No Starch Press. 2014. 531 с.

4. Бабин С.А. Лаборатория хакера. СПб.: БХВ-Петербург, 2016. 240 с.

5. Винокуров А.В. Анализ уязвимостей комплексов с беспилотными летательными аппаратами и классификация угроз безопасности циркулирующей в них информации // I-METHODS. – 2016. - № 1. – Т. 8. – С. 5 – 9.

6. Верещагин Д. Ю., Семисчастнов А. Е. Научная рота в сфере обеспечения информационной безопасности (на примере интеллектуального программного комплекса «Бастион») // Тамбовские правовые чтения имени Ф. Н. Плевако. – Тамбов, 2021. – С. 344 – 350.

Статья поступила в редакцию 20.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Хрущев Н.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Омельченко И.А. – старший оператор научной роты войск радиоэлектронной борьбы.

Гришин И.С. – старший оператор научной роты войск радиоэлектронной борьбы.

Шатских В.В. – старший научный сотрудник научной роты войск радиоэлектронной борьбы.

Вклад авторов

Хрущев Н.С. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Омельченко И.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Гришин И.С. – сбор материала, обработка материала, частичное написание статьи (25%).

Шатских В.В. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Особенности категорирования объекта КИИ в сфере оборонной промышленности и порядок оценки защищенности объектов данной отрасли от кибератак

Егор Евгеньевич Чинилин [1]✉, Алина Михайловна Шапенская[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] chinilin-32@yandex.ru✉
[2] alinashapenskaya2002@gmail.com

Аннотация. Оборонная промышленность является одной из важных сфер КИИ. Защита предприятий этого профиля критически важна, поскольку обеспечение непрерывного функционирования данных объектов – стратегическая задача.

Ключевые слова: критическая информационная инфраструктура, информационная безопасность, оборонная промышленность.

Критическая информационная инфраструктура (КИИ) – программное обеспечение, системы управления и средства связи, которыми пользуются банки, госструктуры, предприятия топливно-энергетического комплекса и другие организации, повреждение сетей которых может привести к серьёзным последствиям для граждан и экономики [1].

Первым этапом при разработке системы защиты КИИ является категорирование объекта в соответствии с Постановлением Правительства РФ № 127 [2].

В зависимости от той или иной категории, к объекту в дальнейшем будут предъявлены требования (по Приказу № 239 ФСТЭК) с целью обеспечения его необходимыми средствами и мерами защиты.

Одной из сфер КИИ является оборонная промышленность. Данная сфера имеет особую важность в связи со сложившейся общемировой обстановкой. Оборонительные отрасли относятся к отраслям, производство или распределение которых остается постоянным независимо от экономических колебаний, преобладающих в экономике страны, из-за оборонительного характера таких продуктов. При этом спрос на них не снижается даже в условиях рецессии.

Комплексная защита предприятий данного профиля критически важна, поскольку обеспечение непрерывного функционирования данных объектов – стратегическая задача.

Целесообразно разработать четкий алгоритм категорирования объекта КИИ в сфере оборонной промышленности, учитывающий особенности и специфику данной сферы и показать на примере принцип работы с ним.

Пример ситуации: Ракетный центр обеспечивает 40% производственных

объемов ракетной продукции страны. На предприятии имеется проектно-конструкторская система, которая контролирует процесс сборки ракетной продукции в соответствии с проектом. В случае атаки на данную систему, объемы производства минимум на 50% от числа производимых заводом ракетных изделий и минимум на 20% от общего объема ракетной продукции страны.

Алгоритм для категорирования в данной сфере выглядит следующим образом:

1. Определение системы, которая может повлиять на производство ракетной продукции.

2. Определение возможной цели и мотива злоумышленника (снижение оборонной мощности государства, дискредитирование организации и т.д.).

3. Определение значимости функций системы в масштабе производительной способности объекта.

4. Определение уровня снижения объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции):

- более 0, но менее или равно 10 (будет определена 3 категория значимости);

- более 10, но менее или равно 15 (будет определена 2 категория значимости);

- более 15 (будет определена 1 категория значимости).

5. Определение категории значимости объекта КИИ.

Таким образом, учитывая условия примера, можем сделать вывод, что для субъекта КИИ – ракетный центр, который использует проектно-конструкторскую АС (она же объект КИИ), ответы в рамках работы с алгоритмом будут иметь вид:

1. Проектно-конструкторская АС.

2. Цель: дискредитирование организации.

3. Система контролирует процесс сборки ракетной продукции в соответствии с проектом.

4. В случае атаки на данную систему, объемы производства минимум на 50% от числа производимых заводом ракетных изделий и минимум на 20% от общего объема ракетной продукции страны.

5. На основании данных, предоставленных в описании, можно сделать вывод о том, что для данной АС целесообразно определить 1 категорию значимости.

Для объективности оценки защищённости КИИ после процедуры категорирования объекта рекомендуется произвести оценку по двум параметрам – уровень соответствия объекта требованиям, предъявляемым законодательством к объектам КИИ (U_s) и готовность субъекта к обнаружению возможной атаки на объект (T_g).

Итоговая оценка защищенности объекта КИИ (Z_o) определяется по формуле:

$$Z_o = \{U_s; T_g\}.$$

Вывод об итоговой оценки защищенности объекта КИИ производится по

таблице 1.

Таблица 1

Итоговая оценка защищенности объекта КИИ (Z_o)

Уровень соответствия объекта требованиям, предъявляемым законодательством к объектам КИИ (U_s)	Готовность субъекта к обнаружению возможной атаки на объект (T_g)		
	Высокая	Средняя	Низкая
Высокий	Высокая	Средняя	Низкая
Средний	Высокая	Средняя	Низкая
Низкий	Средняя	Низкая	Низкая

При этом приоритетным в определении итоговой оценки защищенности является показатель готовности субъекта к обнаружению возможной атаки на объект, поскольку даже в случае отсутствия полного соответствия требованиям законодательства гораздо важнее способность вовремя обнаружить попытку атаки и принять соответствующие меры.

Таким образом, представленный алгоритм позволит быстро и наиболее точно провести процедуру категорирования объекта данной сферы и на основании определенной категории значимости оценить защищённость КИИ, что в свою очередь позволит построить эффективную систему защиты от кибератак.

Список источников

1. Основы тестирования КИИ на проникновение : учебное пособие / А.И. Елисеев [и др.]. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2019. — 84 с. — ISBN 978-5-8265-2090-1. — URL: https://www.iprbookshop.ru/99777.html (дата обращения: 13.03.2023).

2. Постановление Правительства РФ № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», 8 февраля 2018 г.

Статья поступила в редакцию 10.04.23; принята к публикации 10.05.2023.

Информация об авторах

Чинилин Е.Е. - аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Шапенская А.М. - студент кафедры «Системы информационной безопасности», направления подготовки «10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Чинилин Е.Е. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Шапенская А.М. – написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.9

Оценка работоспособности микросхем защиты информации

Александр Сергеевич Ягодкин [1]✉, Дмитрий Эдуардович Косинов [2], Александр Сергеевич Фролов [3], Александр Иванович Озеров [4]
[1,2,3,4] Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, Воронеж, Россия
[1] aas8026@rambler.ru✉, https://orcid.org/0000-0002-4409-1247
[2] dk26.01.1999@yandex.ru, https://orcid.org/0000-0003-4409-0342
[3] frolov_vgltu@mail.ru, https://orcid.org/0000-0003-2207-1371
[4] zero@rambler.ru, https://orcid.org/0000-0002-4095-3428

Аннотация. В статье рассматривается расчетно-экспериментальный метод оценки показателей стойкости и надежности и методика, с помощью которой оценивается стойкость и надежность ИС.

Ключевые слова: расчетно-экспериментальный метод, микросхема, радиация.

При эксплуатации ИС в полях космического излучения, для которых характерна малая мощность воздействия, наряду с процессами деградации электропараметров от облучения, присутствуют процессы естественного старения. Эти процессы имеют комплексный характер, и, кроме того, на них оказывают влияние температура среды и режим работы ИС [1]. Оценка стойкости и надежности изделий путем прямого эксперимента занимает значительное время (которое может составить несколько лет). Следовательно, ставится задача определения стойкости и надежности расчетными или расчетно-экспериментальными методами [1, 2, 3, 4, 5]. В данной работе представлен расчетно-экспериментальный метод оценки показателей стойкости и надежности и методика, с помощью которой оценивается стойкость и надежность ИС.

Сущность метода заключается в проведении испытаний на высокой мощности и пересчете ее к низкой мощности с учетом температуры среды и режима работы ИС. Прогнозирование производится по изменению средних значений и среднеквадратичных отклонений параметров — критериев годности (ПКГ). Изменение ПКГ складывается из изменения от облучения при нормальной температуре (второй член уравнения), учета повышенной температуры среды (третий член уравнения), изменения вследствие старения при различной температуре (четвертый член уравнения). Учет взаимного влияния процессов старения и облучения осуществляется пятым членом уравнения. При активном режиме работы ИС все члены уравнения отличны от нуля. При пассивном режиме работы 4 и 5 члены обращаются в нуль [6].

Другими словами, для каждой ИС определяются параметры аппроксимации модели, характеризующие поведение электропараметра во всем диапазоне доз или

времени испытаний. Таким образом, получается случайный набор значений параметров аппроксимации (вектор параметров), привязанных к конкретной ИС. Каждая из компонент вектора параметров от образца к образцу носит случайных характер, поэтому будет описываться статистическими средним и стандартным отклонением, которые необходимы для расчета показателей стойкости и надежности [6].

Для разработки данного метода были проведены как теоретические (анализ литературных данных), так и экспериментальные исследования. Экспериментальные исследования проводились на ИС серии 530 с тестовыми, а также на ИС серий 134, 106, 1838, 1804. Кроме того, для определения деградации электропараметров от естественного старения использованы результаты, полученные на НПО "Электроника" в течение более чем 20 лет работы, более чем по 50 типономиналам биполярных ИС различного конструктивно-технологического исполнения [6].

В результате проведенных исследований было установлено, что вследствие воздействия гамма-излучения малой мощности в полупроводниковой структуре наблюдается:

а) уменьшение подвижности и эффективной концентрации свободных носителей заряда;

б) уменьшение времени жизни неосновных носителей заряда;

в) накопление объемных и поверхностных зарядов;

г) образование новых центров рекомбинации и т.п.

Данные изменения приводят к: а) увеличению тока базы, а, следовательно, и уменьшению коэффициентов усиления; б) увеличению токов утечки; в) уменьшению напряжения пробоя. Для прогнозирования деградации электропараметров ИС вследствие старения целесообразно использовать аппроксимационную зависимость Аррениуса изменения параметра от времени.

На основе представленной модели разработана методика для расчета показателей стойкости и надежности ИС, эксплуатируемых в активном и пассивном режимах в полях гамма—излучения малой мощности при нормальной и повышенной температуре окружающей среды [6].

Анализ зависимостей показывает, что среднее время наработки до отказа уменьшается при облучении. Причем, это уменьшение будет тем больше, чем больше мощность излучения, когда среднее время доработки на отказ будет определяться только облучением.

Список источников

1. Чубур К.А. Разработка математических моделей физических процессов в разнородной многослойной структуре при радиационном воздействии / Чубур К.А., Струков И.И., Евдокимова С.А., Белокуров В.П., Платонов А.Д., Черкасов О.Н., Зольников К.В. // Моделирование систем и процессов. 2022. Т. 15. № 1. С. 125-133.

2. Беспалов В. А. Обзор методов измерения механической прочности тонких плёнок / Беспалов В. А., Товарнов Д. А., Дюжев Н. А., Махиборода М. А.,

Гусев Е. Э., Зольников К. В. // Моделирование систем и процессов. 2022. Т. 15. № 3. С. 110-128.

3. Зольников В.К. Экспериментальные исследования радиационного воздействия на микросхемы FRAM / Зольников В.К., Гамзатов Н.Г., Анциферова В.И., Полуэктов А.В., Фиронов В.А. // Моделирование систем и процессов. 2022. Т. 15. № 3. С. 16-24.

4. Козюков А.Е. Методы обеспечения стойкости электронной компонентной базы к одиночным событиям путем резервирования / Козюков А.Е., Зольников В.К., Евдокимова С.А., Квасов О.Н., Яковлев К.А., Платонов А.Д. // Моделирование систем и процессов. 2021. Т. 14. № 1. С. 10-16.

5. Зольников В.К. Схемотехнические методы обеспечения стойкости ЭКБ к воздействию тяжёлых заряженных частиц / Зольников В.К., Макаренко Ф.В., Журавлева И.В., Попова Е.А., Гриднев Ю.В., Литвинова Ю.А. // Моделирование систем и процессов. 2021. Т. 14. № 4. С. 35-42.

6. Зольников В.К. Исследование и разработка методов моделирования характеристик ИМС в условиях воздействия радиации. – Воронеж, 1998.

Статья поступила в редакцию 27.04.2023; принята к публикации 10.05.2023.

Информация об авторах

Ягодкин А.С. - к. ф.-м. н. и.о. зав. кафедрой «Информационные технологии» ФГБОУ ВО «ВГЛТУ»

Фролов А.С. – преподаватель СПО кафедры «Информационные технологии» ФГБОУ ВО «ВГЛТУ»

Вклад авторов

Ягодкин А.С. - идея, сбор материала, обработка материала, частичное написание статьи (25%), научное редактирование текста.

Косинов Д.Э. - написание статьи (25%).

Фролов А.С.- написание статьи (25%).

Озеров А.И. - написание статьи (25%).

Конфликт интересов отсутствует.