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

Сборник материалов XVI межрегиональной научно-практической конференции

Брянск
БГТУ
2024

Министерство науки и высшего образования Российской Федерации
Брянский государственный технический университет

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

XVI межрегиональная научно-практическая конференция
(Брянск, 29 апреля 2024 г.)

Сборник материалов и докладов

Под общей редакцией О. М. Голембиовской

Текстовое электронное издание

Брянск
БГТУ
2024

ISBN 978-5-907570-87-0

УДК 004.056
ББК 32.97
И76

Утверждено редакционно-издательским советом БГТУ

И76 **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, 2024. – 320 с. – Режим доступа: https://www.tu-bryansk.ru/mainpage/nauka/konferentsii/sborniki-trudov-konferentsiy-provodimykh-bgtu, свободный. – Загл. с экрана.

Сборник подготовлен по материалам XVI межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных. Проблемы и пути их решения», прошедшей в г. Брянске 29 апреля 2024 года в ФГБОУ ВО «Брянский государственный технический университет».

Издание предназначено для студентов и 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.

УДК 4.056
ББК 32.97

ISBN 978-5-907570-87-0

Научное издание

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

Сборник материалов и докладов
XVI межрегиональной научно-практической конференции

Брянск, 29 апреля 2024 г.

Под общей редакцией О. М. Голембиовской

Текстовое электронное издание

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

Подписано к использованию 28.06.2024.
Объем издания – 6,08 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;
- Шкаберин В. А. – проректор по учебной работе и цифровизации, заместитель председателя 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.

ОГЛАВЛЕНИЕ

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Основные критерии разработки модели угроз безопасности в медицинских информационных системах

Павел Александрович Аверин[1]✉, Кирилл Андреевич Седаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] stopnotwont@gmail.com✉, https://orcid.org/0009-0003-5074-7217
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624

Аннотация. Определены особенности разработки модели угроз безопасности персональных данных при их обработке в медицинских информационных системах. Рассмотрены существующие угрозы конфиденциальности и целостности данных, а также даны рекомендации по повышению уровня защиты персональных данных в медицинских информационных системах.

Ключевые слова: медицинские информационные системы, персональные данные, безопасность данных, защита информации.

Для цитирования: Аверин П. А, Седаков К. А. Основные критерии разработки модели угроз безопасности в медицинских информационных системах // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 9–12.

В эпоху цифровизации, когда информационные технологии играют ключевую роль в различных сферах жизни, вопросы защиты персональных данных становятся все более актуальными, особенно в медицинской сфере. Медицинские информационные системы (МИС) собирают и обрабатывают огромные объемы чувствительных персональных данных пациентов, включая медицинскую историю, результаты обследований, личные данные и т. д. В этом контексте модель угроз становится важным инструментом для обеспечения безопасности информационных систем, включая МИС.

Для обеспечения безопасности медицинских информационных систем необходимо учитывать разнообразие угроз, с которыми они сталкиваются. Это могут быть как традиционные угрозы, такие как вирусы, вредоносное ПО и хакерские атаки, так и специфические для медицинской сферы угрозы, например, медицинский мошенничество или неправомерный доступ к медицинской информации со стороны врачей или медицинского персонала. Модель угроз безопасности должна учитывать разнообразие потенциальных угроз и предусматривать соответствующие меры защиты.

Важно помнить, что разработка модели угроз безопасности информации в медицинских информационных системах — это непрерывный процесс. Угрозы постоянно эволюционируют, и модель безопасности должна постоянно обнов-

ляться и совершенствоваться, чтобы эффективно защищать данные пациентов. Регулярные аудиты безопасности, мониторинг защищенности системы и обучение персонала в области информационной безопасности являются неотъемлемой частью этого процесса.

В случае с медицинскими информационными системами, модель угроз позволяет выявить потенциальные уязвимости и риски, связанные с обработкой и хранением чувствительных персональных данных пациентов, что помогает разработать и реализовать эффективные меры по защите конфиденциальности и целостности этой информации.

Модель угроз — это структурированное представление всей информации, влияющей на безопасность информационной системы, которое включает в себя расчет рисков воплощения угрозы в жизнь, а также оценку предполагаемых последствий [1].

Одной из основных особенностей разработки модели угроз безопасности информации в МИС является необходимость учета строгих требований к конфиденциальности и защите персональных медицинских данных. Врачи и медицинский персонал имеют доступ к чувствительным медицинским данным пациентов, включая диагнозы, истории болезней, результаты лабораторных исследований и т. д. Поэтому любое нарушение безопасности данных может привести к серьезным последствиям для пациентов и медицинских учреждений. Модель угроз безопасности должна определять угрозу, а также должна определять меру для максимальной минимизации угроз [3].

Следует также учитывать разнообразие угроз, с которыми сталкиваются медицинские информационные системы. Это могут быть как традиционные угрозы, такие как вирусы, вредоносное ПО и хакерские атаки, так и специфические для медицинской сферы угрозы, например, медицинский мошенничество или неправомерный доступ к медицинской информации со стороны врачей или медицинского персонала. Модель угроз безопасности должна учитывать разнообразие потенциальных угроз и предусматривать соответствующие меры защиты.

В России, как и во многих других странах, существует законодательная база, регулирующая обработку персональных данных. Федеральный закон №152 «О персональных данных» определяет основные принципы сбора, обработки и хранения персональных данных, а также устанавливает требования к защите таких данных от несанкционированного доступа, утечек и иных угроз.

Рассмотрим наиболее популярные угрозы безопасности информации, с которыми сталкиваются медицинские информационные системы.

Одна из наиболее серьезных угроз безопасности, это неавторизованный доступ к данным. Хакеры могут пытаться получить доступ к медицинским информационным системам (МИС), чтобы украсть или изменить персональные данные пациентов. Для борьбы с этим типом угрозы важно использовать сильные методы аутентификации и авторизации, шифрование данных и контроль доступа.

Помимо этого, медицинские информационные системы подвержены риску заражения вредоносным программным обеспечением, которое может заблокировать доступ к данным, украсть информацию или повредить систему.

Также может привести к утечке информации несанкционированный физический доступ к серверам или компьютерам, на которых хранятся медицинские данные. Для предотвращения этого угрозы необходимо строго контролировать доступ к помещениям, где размещены серверы, и применять соответствующие технические меры безопасности, такие как камеры наблюдения и системы контроля доступа.

В заключении можно сказать, что обеспечение безопасности персональных данных в медицинских информационных системах является критически важной задачей в условиях современной цифровизации медицинской сферы. Модель угроз безопасности представляет собой эффективный инструмент для идентификации, анализа и управления рисками, связанными с обработкой чувствительной медицинской информации о пациентах. Реализация соответствующих мер по защите данных, включая усиление систем аутентификации, шифрование данных, контроль доступа и обучение персонала, поможет минимизировать угрозы безопасности и обеспечить конфиденциальность, целостность и доступность персональных медицинских данных. Это в свою очередь способствует повышению уровня доверия со стороны пациентов к медицинским организациям и обеспечивает сохранность их личной информации в условиях быстрого развития цифровых технологий.

Список источников

1. Модель угроз безопасности персональных данных: что такое и как составлять – Текст: электронный [сайт]. – URL: https://selectel.ru/blog/personal-data-security-threat-model/ (дата обращения: 01.04.2024).

2. Текст: электронный [сайт]. – URL: https://alfario.ru/doc/ispdn_documents/basic_model_of_security_threats_of_personal_data.pdf - (дата обращения: 01.04.2024).

3. Текст: электронный [сайт]. – URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-meditsinskih-organizatsiyah.

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Аверин П. А. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П. А. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Termux как инструмент к проведению пентестов

Артур Игоревич Банников[1]✉, Александр Владимирович Зайцев[2], Олег Сергеевич Якушов[3]
[1] Брянский государственный технический университет, Брянск, Россия
[2, 3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1] Artur-korch@inbox.ru✉, https://orcid.org/0000-0003-2120-0709
[2, 3] nauchnajarota@yandex.ru, https://orcid.org/0009-0007-5540-2719

Аннотация. В настоящее время информационные технологии занимают важное место в жизни общества. Они проникают повсюду — от повседневной жизни до корпоративной сети. С ростом технологий также растет угроза информационной безопасности. Уязвимости сетевых систем могут привести к серьезным последствиям, поэтому безопасность становится все более важным аспектом в IT-сфере.

Одним из инструментов для тестирования уязвимостей является пентестинг. Пентестинг (или тестирование на проникновение) — это способ проверки безопасности информационной системы путем моделирования атаки злоумышленника с целью выявления уязвимостей и их устранения.

Ключевые слова: пентест, Termux, тестирование на проникновение.

Для цитирования: Банников А. И., Зайцев А. В., Якушов О. С. Termux как инструмент к проведению пентестов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 13–16.

Termux — это эмулятор терминала и среда Linux. При установке приложения получаем работоспособный Linux терминал на своем мобильном устройстве под операционной системой Android. Большим достоинством является работы эмулятора в виртуальном окружении, то есть многое можно делать без полных прав доступа (root'a), благодаря чему навредить файловой системе Android практически нельзя.

Основной софт для проведения пентеста после установки python, python2, git, nmap, hydra выглядит следующим образом:

Nmap — свободная утилита, предназначенная для разнообразного сканирования IP сетей. Nmap мощный поисковик отрытых портов, без которого в мир пентеста не обойтись.

Wireshark — инструмент, с помощью которого можно обнаружить уязвимости внутри сети.

Основные функции:

1. Захват пакетов.
2. Анализ пакетов.
3. Фильтрация протоколов.
4. Сканирование всей сети.

Nikto — инструмент для поиска различных конфигураций, файлов, небезопасных программы на веб-серверах.

В Termux можно также установить пакеты инструментов для социальной инженерии.

Основной набор атак:

1) целевые фишинговые атаки;
2) атаки на веб-сайты;
3) генератор зараженных носителей;
4) массовая рассылка;
5) атака на основе Arduino;
6) атаки с использованием QRCode;
7) векторы атак Powershell.

Приведённые выше, а также многие другие инструменты дают большие возможности Termux, которые есть и в среде Linux при проведении пентестов.

Недостакти в Termux присутствуют. Они обусловлены, Bionic-системной Си-библиотекой для Android. В Bionic не реализованы многие функции стандартной libc. По этой причине, например, нельзя сгенерировать нужный региональный стандарт и связанные с ним переменные окружения с помощью locale-gen, в результате чего в Termux нельзя видеть кодировку отличную от Юникода.

Также сообщество Termux не такое большое, как например, другие сообщества операционных систем и поддержки пакетов уровня крупных дистрибутивов здесь пока нет.

Для многих пользователей чтение инструкций, правил настройки, команд — это существенный минус.

Из главных достоинств можно выделить это доступность, возможность использования начиная с Android 6 и довольно большой выбор инструментов.

Проведение пентестов с помощью Termux дает возможность специалистам по информационной безопасности и исследователям тестировать безопасность сетей и веб-приложений непосредственно с мобильного устройства.

Процесс установки Termux достаточно прост и подобен установке любого другого приложения из магазина приложений в системе Android. На мобильном устройстве нужно открыть Google Play Маркет, ввести в строке поиска Termux и установить приложение на устройство. После этого пользователь может начать использовать Termux для выполнения команд и установки пакетов.

После установки приложения, открывается командная строка, где пользователь может выполнять различные команды, осуществлять доступ к фунда-

ментальным Unix-утилитам и устанавливать пакеты с помощью пакетного менеджера. Просто введите apt update для обновления списка пакетов, а затем — apt upgrade для обновления установленных пакетов.

Примеры использования основных команд:

- `pkg install` — команда для установки пакетов в Termux;
- `ls` — команда для просмотра содержимого текущего каталога;
- `cd` — команда для перехода в другой каталог;
- `git clone` — команда для клонирования репозитория с GitHub;
- `python` — команда для запуска интерпретатора Python;
- `curl` — команда для загрузки файлов из Интернета;
- `apt` — пакетный менеджер для управления установленными пакетами.

Пример скрипта на языке Python для проведения пентеста (например, сканер уязвимостей):

```python
import socket
def scan_port(host, port):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(1)
    try:
        s.connect((host, port))
        print(f"Port {port} is open")
    except:
        pass
    s.close()
# Пример использования: сканирование портов на сервере
host = '192.168.1.1'
for port in range(1, 1025):
    scan_port(host, port)
```

Пример инструкции для проведения тестирования на проникновение:

1. Запустите Termux на вашем устройстве.

2. Установите необходимые инструменты для пентеста, например nmap, metasploit или burp suite, с помощью команды `pkg install`.

3. Подключитесь к целевой сети или устройству.

4. Используйте установленные инструменты для сканирования уязвимостей, поиска уязвимых мест и тестирования на проникновение в соответствии с этическими стандартами.

Таким образом, использование Termux для проведения пентестов позволяет специалистам по информационной безопасности и исследователям проводить тестирование на проникновение непосредственно с мобильного устройства. Однако при использовании любых инструментов для тестирования на проникновение необходимо соблюдать законы и этические стандарты, а также иметь разрешение от владельцев системы на проведение тестов.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Банников А. И. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Зайцев А. В. – д. т. н., профессор, преподаватель цикла боевой подготовки (специалистов радиоэлектронной борьбы с наземными системами управления войсками и оружием), Войсковая часть 61460.

Якушов О. С. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Банников А. И. – идея, сбор материала, частичное написание статьи (80 %).

Зайцев А. В. – сбор материала, частичное написание статьи (10 %).

Якушов О. С. – обработка материала, частичное написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Важность устранения уязвимостей системы для обеспечения кибербезопасности

Дарья Дмитриевна Бутузова[1]✉, Оксана Михайловна Голембиовская[2], Валентина Ивановна Анциферова[3]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[1] enikeevadara9@gmail.com✉, http://orcid.org/0009-0000-1789-7297
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133
[3] wkz@rambler.ru

Аннотация. В статье рассмотрены последствия, к которым могут привести уязвимости системы; указаны основные этапы устранения уязвимостей, подробно описаны четыре уязвимости, которые могут привести к несанкционированному доступу; сделаны выводы о важности устранения уязвимостей.

Ключевые слова: уязвимость, злоумышленник, эксплуатация уязвимостей, кража данных, обновление системы.

Для цитирования: Бутузова Д. Д., Голембиовская О. М., Анциферова В. И. Важность устранения уязвимостей системы для обеспечения кибербезопасности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 17–19.

В современную эпоху, когда предприятия и частные лица всё больше полагаются на технологии, обеспечение кибербезопасности стало критически важным. Злоумышленники используют уязвимости, которые представляют собой слабые области в аппаратном и программном обеспечении, чтобы получить нелегальный доступ к скрытым данным или информационным системам. Важной задачей специалистов в этой области является своевременное устранение уязвимостей для избежания серьёзных инцидентов.

Не устранённые уязвимости могут иметь катастрофические последствия для организаций и частных лиц. Нарушители используют их для доступа к конфиденциальным данным, перехвата удалённого управления системой, а также для нарушения работы предприятия [1].

Регулярный мониторинг уязвимостей поможет уменьшить рост кибератак, защитить данные, повысить доверие клиентов и обеспечить непрерывность бизнес-процессов.

Существует определённая последовательность устранения уязвимостей. Первым этапом является выявление уязвимостей. Для этого нужно провести анализ информационной структуры компании, в ходе которого собираются данные об активах. Активы — объекты компании, которые участвуют в создании дохода [2]. Ими являются: сетевое оборудование, рабочие станции.

После сканирования системы и нахождения уязвимостей можно перейти к следующему этапу — определению уровня их опасности и срочности исправления. Рассмотрим самые распространённые уязвимости, через которые возможно воздействие.

Уязвимость BDU:2023-05857 содержится в модуле landing системы управления содержимым сайтов (CMS) 1С-Битрикс. Эксплуатация уязвимости позволяет нарушителю удалённо выполнить команды ОС на уязвимом узле, получить контроль над ресурсами, проникнуть в сеть. Пользователям рекомендуется обновить программный продукт до версии landing 23.850.0 и выше.

Уязвимость CVE-2022-27228 служит для повышения привилегий в компоненте ядра Linux, который обрабатывает системные вызовы. Уязвимость возникает из-за ошибки в проверке прав доступа при обработке определенных типов запросов. Эксплуатация уязвимости может привести к повышению привилегий на целевой системе, выполнению произвольного кода, кражи данных, записи произвольных файлов в систему посредством отправки специально сформированных сетевых пакетов [3]. Пользователям рекомендуется обновить ядро Linux до версии 5.19.12 или более поздней.

Уязвимость CVE-2023-22522 служит для удаленного выполнения кода в Microsoft Windows Print Spooler Service. Уязвимость возникает из-за ошибки в обработке определённых типов файлов, отправленных на печать. Уязвимость для внедрения шаблона позволяет аутентифицированному злоумышленнику в Confluence выполнять произвольный код на целевой системе. Пользователям рекомендуется установить обновление безопасности Microsoft для CVE-2023-22522.

Уязвимость CVE-2023-3519 используется для повышения привилегий в графическом компоненте Windows под названием Windows Graphics Device Interface (GDI). Уязвимость возникает из-за ошибки в обработке определенных типов объектов GDI. Эксплуатация этой уязвимости может привести к повышению привилегий на целевой системе. Citrix NetScaler ADC и NetScaler Gateway тоже уязвимы к ошибке при внедрении кода, которая позволяет удаленно выполнять код без проверки подлинности и без необходимости каких-либо привилегий или взаимодействия с пользователем. Пользователям рекомендуется установить обновление безопасности Microsoft для CVE-2023-3519.

После установки обновлений проводится тестирование системы для поиска новых уязвимостей, затем продолжается мониторинг системы для своевременного обнаружения уязвимостей [4].

Устранение уязвимостей системы является очень важным шагом для обеспечения надежной кибербезопасности. Не устранённые уязвимости могут подвергнуть организации и частных лиц серьезному риску кибератак. Нужно

своевременно находить и устранять уязвимости для защиты конфиденциальных данных, обеспечения непрерывности бизнеса, соответствия нормативным требованиям и повышения доверия клиентов, деловых партнеров. Организации и частные лица должны уделять первостепенное внимание устранению уязвимостей системы, чтобы защитить себя от постоянно совершенствующихся киберугроз.

Список источников

1. Шмерлинг С. За час до атаки. Повести. М.: Средне-Уральское книжное издательство, 2013. 224 с.
2. Стандарт ISO/IEC 27001:2022.
3. Чирилло, Д. Обнаружение хакерских атак. М.: СПб.: Питер, 2017. 864 с.
4. Рытов М. Ю., Мусиенко Н. О., Губсков Ю. А., Минин Ю. В. Аудит и мониторинг состояния объектов информатизации в процессе проектирования комплексных систем защиты информации значимых объектов критической информационной инфраструктуры. Приборы и системы. Управление, контроль, диагностика. 2022. № 10. С. 10–18.

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Бутузова Д. Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Анциферова В. И. – к. т. н., доцент кафедры информационных технологий ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Бутузова Д. Д. – написание статьи, сбор материала, обработка материала (60 %).

Голембиовская О. М. – идея, научное редактирование текста (20 %).

Анциферова В. И. – сбор материала, обработка материала (20 %).

Конфликт интересов отсутствует.

Научная статья
УДК 004

Исследование программ для проведения пентеста собственными силами

Дарья Дмитриевна Бутузова[1]✉, Оксана Михайловна Голембиовская[2], Ирина Юрьевна Артамонова[3]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[1] enikeevadara9@gmail.com✉, http://orcid.org/0009-0000-1789-7297
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133
[3] lap109@mail.ru

Аннотация. В статье представлено исследование вопроса обеспечения безопасности информации на предприятии с помощью пентеста. Данная методика поможет в проведении пентеста собственными силами, в выяснении уязвимостей компании, которые и могут стать главным инструментом для хищения информации злоумышленником.

Ключевые слова: информационная безопасность, пентест, уязвимости, злоумышленник, сканирование, утечка данных.

Для цитирования: Бутузова Д. Д., Голембиовская О. М., Артамонова И. Ю. Исследование программ для проведения пентеста собственными силами // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 20–23.

В современном обществе предприятия осваивают новые технологии, меняют старое оборудование на более совершенное, ищут действенные способы увеличения прибыли, которые и помогают укрепиться в бизнесе. Информация имеет первостепенную роль, ведь её можно продавать, передавать и обрабатывать. Но любую важную информацию следует защищать, поэтому в наше время большое значение придают защите информации.

По статистике за 2023 год доля целевых атак составила 78 % от общего количества [1]. Организации выделили главные последствия успешных кибератак: ими стали утечки конфиденциальной информации (67 %) и нарушение основной деятельности (44 %). Существенный вред был нанесён массовыми атаками через эксплуатации уязвимостей и крупными утечками персональных данных. Из статистики видно, что идеальную защиту специалист по информационной безопасности не может обеспечить, но он может повышать свои навыки, искать новые пути обнаружения уязвимостей системы, которых становится больше и больше с каждым днём.

Например, существует методика принятия на работу человека, который знает построение хакерской деятельности, и это поможет узнать, как будет думать злоумышленник в случае атаки. Ведь зная его мышление, мы сможем заранее закрыть бреши системы и защитить их надёжным способом. Но есть и другая методика, более совершенная.

Пентест — это проверка защищённости компьютерной системы, при которой создаётся реальная атака злоумышленника [2].

Сегодня у хакеров есть множество автоматизированных инструментов тестирования, позволяющих проводить атаки гораздо проще и эффективнее. Действенный способ убедиться, что ваша сеть действительно защищена – это протестировать ее. Пользователь должен быть уверен, что операционная система на его компьютере обновлена, а приложения работают без ошибок, которыми можно воспользоваться при взломе.

В начале пентеста следует собрать информацию: узнать версию программного обеспечения, доменные имена, IP-адреса, исследовать программы, которые могут быть взломаны злоумышленником. Затем начинается этап поиска и анализа уязвимостей, на котором пентестер ищет прорехи безопасности, через которые может попытаться проникнуть злоумышленник. Основными инструментами на данном этапе являются сканеры уязвимостей. Они помогают специалистам информационной безопасности выявить уязвимости и исправить их во избежания инцидентов.

Рассмотрим сканер уязвимостей Nessus. Он позволяет выявить уязвимости с помощью глубокого анализа безопасности, найти неверные конфигурации, выявить отсутствие паролей для учётных записей, найти слабые места в приложениях, рабочих станциях, серверах, определить состояние портов на целевом хосте. Обеспечивает высокоскоростное обнаружение и выявляет конфиденциальные данные.

В качестве второго сканера уязвимостей можно рассмотреть OpenVAS [3]. Он позволяет производить сканирование узлов сети на наличие уязвимостей и управлять уязвимостями. Его несомненным плюсом является мощный внутренний язык программирования для осуществления различных типов тестирования на уязвимость.

После выявления уязвимостей нам понадобятся инструменты для их эксплуатации. Этот этап помогает проверить, насколько сложно воспользоваться найденными уязвимостями и взломать систему.

Начнём с инструмента, который предназначен для автоматизации атак и использования известных уязвимостей, Metasploit. Этот фрэймворк с открытым исходным кодом пользователь может настроить и использовать на многих операционных системах. Основные возможности позволяют пользователям запускать сценарии на хосте, генерировать или использовать существующий набор вредоносного кода для обхода антивирусного обеспечения, перехватывать управление монитором устройства, захватывать сеансы и скачивать файлы.

Второе приложение для эксплуатации уязвимостей — Hydra. Оно позволяет перебрать пароли в режиме реального времени от онлайн-сервисов, веб-приложений, протоколов. Пользователь может легко добавить свои модули, так и использовать существующие. Также это приложение помогает узнать, насколько легко можно получить несанкционированный доступ к системе с удаленного устройства.

Следующий этап заключается в поддержание доступа человеком, который проводит пентест. Главная задача — это оценить, как долго система не замечает, что её взломали и происходит атака. Устанавливаются инструменты для поддержания доступа к системе во время тестирования.

Можно воспользоваться расширенной многофункциональной нагрузкой Meterpreter (payload), которая используется в Metasploit Framework. Она может быть динамически расширена во время выполнения и повышает привилегии до системных.

Предпоследний этап заключается в анализе данных, которые смог получить пентестер. Сюда входит оценивание ущерба от успешной атаки, определение мест ИТ инфраструктуры, которые в первую очередь нуждаются в защите.

На последнем этапе пентестер создаёт отчёт, в котором подробно описаны уязвимости, возможные способы их устранения. Даётся общая оценка безопасности системы.

Можно сделать вывод, что пентест выявляет реальные проблемы в организации, помогает построить стратегию их устранения, поэтому организациям рекомендуется периодично выполнять пентест во избежания серьёзных инцидентов.

Список источников

1. Актуальные киберугрозы: II квартал 2023 года. Режим доступа: ptsecurity.com. (Дата обращения: 05.03.2024).

2. Стандарт ISO/IEC 27001: 2022.

3. Стивенс, У. UNIX: разработка сетевых приложений. М.: СПб.: Питер, 2009. – 396 с.

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Бутузова Д. Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Артамонова И. Ю. – преподаватель кафедры иностранных языков ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Бутузова Д. Д. – написание статьи, сбор материала, обработка материала (60 %).

Голембиовская О. М. – идея, научное редактирование текста (20 %).

Артамонова И. Ю. – сбор материала, обработка материала (20 %).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Обзор программ по выявлению уязвимостей системы

Дарья Дмитриевна Бутузова[1]✉, Оксана Михайловна Голембиовская[2], Артём Сергеевич Грошев[3]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[1] enikeevadara9@gmail.com✉, http://orcid.org/0009-0000-1789-7297
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133
[3] ArtGrosh@mail.ru

Аннотация. В статье указаны программы для выявления уязвимостей в системе. Рассматриваются различные инструменты, которые помогают провести поиск эксплойтов, просканировать открытые порты и программное обеспечение, провести эксплуатацию уязвимостей, чтобы выявить слабые места в системе.

Ключевые слова: уязвимость, злоумышленник, сканирование уязвимостей, управление уязвимостями.

Для цитирования: Бутузова Д. Д., Голембиовская О. М., Грошев А. С. Обзор программ по выявлению уязвимостей системы // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 24–26.

В сфере информационной безопасности одним из ключевых аспектов является регулярное сканирование и обнаружение уязвимостей в системе. Для этого существуют программные средства, которые позволяют автоматизировать процесс выявления уязвимостей, упрощая работу администраторов и повышая общий уровень безопасности.

Пенетрационные тесты (пентесты) — это имитация атак злоумышленника на систему с целью оценки её безопасности [1]. Нужно учесть, что данные методы оценки безопасности системы нельзя проводить без подготовки, которая заключается в изучении системы, определение инструментов, необходимых для проведения атак, а также создание копии системы для восстановления работы после тестирования.

Первичное сканирование на возможность определения открытых портов можно провести с помощью «Nmap». Программа может сканировать целевую сеть, определять активные узлы, анализировать операционные системы, открытые порты. Программа позволяет определить топологию сети, выявить связь

между устройствами. Пользователь может настроить параметры сканирования с помощью опций командной строки.

При сканировании на наличие открытых портов можно также использовать программу «MaxPatrol 8». Программа предоставляет инструменты для постоянного мониторинга безопасности информационных систем. Осуществляет сканирование систем на уязвимости и помогает в их классификации. В «MaxPatrol 8» можно создать отчёт о состоянии безопасности систем, выявленных уязвимостях и рекомендациях по их устранению.

Сканирование программного обеспечения, расположенного на периметре, производится с помощью программы «Nessus». Программа позволяет просканировать систему на уязвимости, может выполняться на сетевых устройствах, серверах, рабочих станциях. В «Nessus» можно создать отчёт об обнаруженных уязвимостях, рекомендациях по устранению.

Для сканирования программного обеспечения также подойдёт «Acunetix». Программа автоматически сканирует веб-сайты и веб-приложения на наличие уязвимостей. «Acunetix» удобна в использовании и может быть интегрирована с другими инструментами безопасности и системами управления проектами [2].

Поиск эксплойтов для обнаруженного программного обеспечения можно провести с помощью «Metasploit». Фреймворк позволяет использовать эксплойты для проверок уязвимостей в сетевых протоколах и приложениях. Эксплойт — это код, который позволяет проверить наличие уязвимостей и использовать их для получения доступа к системе без разрешения владельца.

Для эксплуатации уязвимостей или подбора пароля можно использовать утилиту «Hydra». Она используется для атак на серверы с использованием словарей паролей. Её основная функция — атака на различные протоколы сети: FTP, HTTP, SMB, SSH, SQL и др.

В установке обратного соединения поможет сетевой примитив «Gsocket». Он позволяет создавать, использовать и закрывать сокеты для сетевой коммуникации. Сокет — это виртуальная конструкция, которая позволяет компьютерам обмениваться данными.

Повышения привилегий для доступа в систему можно добиться с помощью трояна «WinPeas». Он выступает в качестве промежуточного сервера для распространения других троянов, может установить зараженные файлы на свои сервера и оттуда распространять их на другие устройства. Его использование может привести к нежелательным последствиям, таким как утечки данных, неполадки в сети.

Горизонтальным перемещением называют перемещение злоумышленника в сети с целью распространения зараженного кода или взлома системы [3]. Для реализации перемещения требуется пакет инструментов «Impacket». Он является открытым и бесплатным, написан на языке Python. Предоставляет пользователям возможность анализировать протоколы сети и форматы файлов, связанные с сетевыми службами, такими как SMB, LDAP, SNMP.

Импакт анализ используется для улучшения тестирования. Его можно провести с помощью «PowerSploit». Это набор инструментов и скриптов PowerShell, используемых для атак на компьютеры и сети.

Программы по выявлению уязвимостей системы играют важную роль в обеспечении безопасности информации и защите от потенциальных угроз. Выбор конкретного инструмента или программы зависит от потребностей организации, её инфраструктуры и доступных ресурсов. Специалистам в области безопасности стоит регулярно проводить сканирование уязвимостей и оперативно реагировать на обнаруженные проблемы для обеспечения надёжной защиты системы.

Список источников

1. Стандарт ISO/IEC 27001: 2022.

2. Сканеры уязвимостей [Электронный ресурс] Режим доступа: www.anti-malware.ru (Дата обращения: 20.04.2024).

3. Чекулаева, Е. Н. Управление информационной безопасностью: учебное пособие / Е. Н. Чекулаева. – Йошкар-Ола: Поволжский государственный технологический университет, 2020. – 153 с.

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Бутузова Д. Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Грошев А. С. – аспирант ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Бутузова Д. Д. – написание статьи, сбор материала, обработка материала (60 %).

Голембиовская О. М. – идея, научное редактирование текста (20 %).

Грошев А. С. – сбор материала, обработка материала (20 %).

Конфликт интересов отсутствует.

Научная статья
УДК 004.8

Анализ особенностей нарушителей информационной безопасности в сфере здравоохранения

Дарья Дмитриевна Бутузова[1]✉, Кирилл Андреевич Седаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] enikeevadara9@gmail.com✉, http://orcid.org/0009-0000-1789-7297
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624

Аннотация. Рассмотрено построение модели нарушителя для объектов защиты в сфере здравоохранения. Указаны классификации потенциальных нарушителей целостности и безопасности информационных баз медицинских учреждений, а также основные этапы создания модели нарушителя.

Ключевые слова: внешний нарушитель, внутренний нарушитель, злоумышленник, модель нарушителя, объект здравоохранения.

Для цитирования: Бутузова Д. Д., Седаков К. А. Анализ особенностей нарушителей информационной безопасности в сфере здравоохранения // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 27–30.

В современном мире защита конфиденциальной информации становится всё более актуальной темой, особенно в организациях сферы здравоохранения. Медицинские учреждения становятся более популярны для атак злоумышленников, их главной целью является похищение конфиденциальной информации, а именно персональных данных и медицинской информации. Большой упор специалисты по информационной безопасности в здравоохранительных объектах должны делать на защиту от утечки личных данных, чтобы избежать шантажа и компрометации пациентов. Внедрение современных технических средств и проведение мероприятий организационного характера способны предотвратить серьёзные инциденты [1].

Главным методом организационного характера является разработка модели нарушителя информационной безопасности. Модель нарушителя — это модель, описывающая потенциальных нарушителей, содержащая информацию об уровне их знаний, целях, степенях возможностей и способах реализации угроз [2]. При создании модели нарушителя учитывается техническая и программная оснащённость злоумышленника, его знания об объектах системы, наличие или отсутствие доступа к ним, сведения об имеющихся в распоряжении у злоумышленника средств для атак, о его подготовке [3].

Помимо этого, указывается описание каналов, через которые нарушитель проводит атаку, проводится обоснование того, какие нарушители исключаются из списка потенциальных.

Начальным этапом создания модели нарушителя является анализ информационной системы медицинского учреждения. В ходе исследование идёт составление примерного списка актуальных нарушителей системы.

Обратимся к известному банку источников угроз. Банк угроз ФСТЭК выделяет три типа нарушителей по уровню безопасности. К низкому типу относится нарушитель, обладающий базовыми возможностями и повышенными базовыми возможностями. Это обычный человек, который может как владеть знаниями о различных инструментах для работы с системой, так и не иметь этих знаний вовсе. К низкому типу можно отнести: конкурирующие медицинские организации, поставщики услуг связи, системные администраторы [4].

К среднему типу относится человек, который имеет доступ к закрытым данным, например, к информации об уязвимостях системы. К среднему типу можно отнести: разработчиков программных и аппаратных средств, террористические группировки.

Высокий тип определяет человека или группу лиц, которые имеют достаточно возможностей для реализации продолжительных угроз безопасности информации, разработки и внедрения уязвимостей программного обеспечения на этапе его поставки. Этой деятельностью занимаются иностранные спецслужбы.

Имеется два типа нарушителей на основании признака принадлежности к медицинской информационной системе. Внешний нарушитель — это человек, который не имеет права нахождения на пределах территории, где размещено оборудование медицинской информационной системы (МИС). Внутренний нарушитель — это человек, который имеет право нахождения на территории организации.

Внутренний нарушитель может не иметь доступа к ресурсам системы, но он может совершить удалённую атаку на МИС. Его целью является хищение данных, нарушение работы системы или её полный вывод из строя, а также самоутверждение.

На территории предприятий существует ряд ограничений, которые влияют на возможности внутреннего нарушителя. Эти ограничения включают организационно-технические меры: тщательный подбор персонала, его повышение квалификации, допуск посторонних лиц на территорию учреждения, организация и проведение работ по информационной безопасности. К внутренним нарушителям относятся администраторы, операторы, обслуживающий персонал, пациенты, сотрудники, обслуживающие телекоммуникационные системы и программное обеспечение. Они несут наибольший риск для МИС.

Злоумышленник имеет информацию о системе, которая разделяется на: общую информацию — содержит назначение и характеристики МИС;

эксплуатационную информацию — доступна из эксплуатационной документации; чувствительную информацию — дополняет эксплуатационную информацию о МИС.

У нарушителя присутствуют определённые средства атаки, которые включают в себя программное и аппаратное обеспечение, самостоятельно разработанное оборудование, купленные технические приспособления. Точная оценка средств атаки у нарушителя невозможна, ведь на это влияют разные факторы (финансовые средства нарушителя, установленное на здравоохранительных объектах оборудование и т. д.), но есть возможность определить примерные характеристики средств атак.

В рамках этого этапа необходимо указать классификацию уровней несанкционированного доступа к защищённым объектам, которая представлена в виде стека протоколов TCP/IP [5]. Различают уровень технических каналов, сетевой уровень, канальный, транспортный, прикладной, физический, а также уровень вредоносного воздействия, уровень системы защиты информации и уровень закладных устройств.

Первостепенной целью атак на МИС является хищение конфиденциальной информации, которая поможет злоумышленнику в шантаже посетителей здравоохранительного учреждения, продаже сведений о пациенте, что в целом ведёт к нарушению врачебной тайны.

К объектам атак можно отнести: защищённую информацию, документацию, техническое и программное обеспечение, помещения, каналы связи. К каналам атак относятся: каналы доступа к объекту атаки (акустический, физический, визуальный), штатные средства, носители информации, убранные из использования и неправильно утилизированные, съёмные носители информации, незащищённые каналы связи, документация.

Основные способы атак составляют: атаки на уязвимости системы, хищение отходов, перехват информации, искажение информации в незащищённых каналах связи, модификацию программных средств с использованием вредоносных программ, методы социальной инженерии.

На последнем этапе разработки модели угроз формируются требования к безопасности объекта в виде списка сценариев действий по проникновению нарушителя в систему. Обращается особенное внимание на воздействия внешних и внутренних факторов, которые помогут нарушителям достичь своей цели.

Модель нарушителя детально описывает и классифицирует по признакам злоумышленников, производящих атаки на систему; служит источником основных каналов, целей и объектов атак, включает в себя список примерных атак на МИС.

Таким образом определение нарушителей информационной безопасности в сфере здравоохранения является важной задачей в формировании эффективной системы защиты информации, ведь при соблюдении требований можно избежать хищения данных, которое, в свою очередь, может привести к негативным последствиям.

Список источников

1. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. – Рн/Д: Феникс, 2017. С. 324.

2. Рытов М.Ю., Мусиенко Н.О., Губсков Ю.А., Минин Ю.В. Аудит и мониторинг состояния объектов информатизации в процессе проектирования комплексных систем защиты информации значимых объектов критической информационной инфраструктуры. Приборы и системы. Управление, контроль, диагностика. 2022. № 10. С. 10-18. https://elibrary.ru/item.asp?id=351232113;

3. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. – М.: Гелиос АРВ, 2017. – 336 с. – URL: http://www.iprbookshop.ru/46584530.html;

4. Белов, А.С. Модернизация системы информационной безопасности: подход к определению периодичности / А.С. Белов, М.М. Добрышин, Д.Е. Шугуров. – М.: Инсайд, 2022. С. 76-80;

5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ, НИЦ ИНФРА –М, 2017. – 416 с. – URL: http://www.iprbookshop.ru/3587330.html.

Статья поступила в редакцию19.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Бутузова Д. Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Бутузова Д. Д. – написание статьи, сбор материала, обработка материала (50 %).

Седаков К. А. – идея, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004:056

Информационные войны и различные подходы к их изучению

Татьяна Вячеславовна Васина[1], Кирилл Евгеньевич Шинаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] tata.vasina.666@gmail.com, https://orcid.org/0009-0009-9243-3869
[2] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. В статье дается определение информационной войне. Указывается значимость информации во все исторические периоды. Рассматриваются различные подходы к изучению феномена информационных противоборств.

Ключевые слова: информационная война, информация, пропаганда, информационная система, дезинформация.

Для цитирования: Васина Т. В., Шинаков К. Е. Информационные войны и различные подходы к их изучению // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 31–34.

В условиях глобализации информационных процессов и развития современных технологий, информация стала основным инструментом воздействия на мнение общественности. Такое понятие как «информационная война» (англ. Information warfare) все чаще фигурирует в работах ученых [1].

Не смотря на относительную новизну понятия, история показывает, что особая значимость в период сражений и различного рода противоборств отдавалась психологическому воздействию на противника во все времена. Так, еще китайский военноначальник Сунь-Цзы, в своем трактате «Искусство войны» первым определил роль информационного воздействия на противника: «Одержать сотню побед в сражениях — это не предел искусства. Покорить противника без сражения — вот венец искусства», указывая на важность подрыва духа войск [4].

Распространение слухов и агитационных листовок, содействие радио и телевиденья — то, что использовалось и продолжает использоваться как способ информационного воздействия на людей. С развитием технологий к ним добавились вбросы фейковой информации, взломы баз данных и хакерские атаки. Из года в год информация становится все более опасным оружием в руках злоумышленников, именно поэтому вопрос информационной войны актуален сейчас как никогда.

Информационная война — феномен достаточно разноплановый, что затрудняет присвоение ему точного определения. В данной работе используется полипарадигмальный подход при изучении, с целью исследовать все его аспек-

ты. Это позволит получить более объемное понимание явления и на основе полученной информации сделать вывод касаемо природы информационных войн.

В настоящее время существует множество подходов к рассмотрению аспектов информационных войн. В. А. Лисичкин, Л. А. Шелепин и А. Г. Караяни рассматривают информационную войну в рамках психологической парадигмы. Информационное воздействие, в их теориях, сопоставляется с психологическим и определяется как скрытое влияние на индивидуальное, групповое и массовое сознание с помощью пропаганды, дезинформации и различного рода манипуляций. Разрушение базовых традиционных ценностей и формирование нового мышления, выгодного для противника — вот главные цели информационной войны, согласно данному подходу [2].

Многие ученые придерживаются геополитического аспекта, в котором информационная война рассматривается как способ противоборства государств без использования военной техники, оружия и физической силы. И. А. Михальченко называет данное явление целостной технологией, способной осуществлять порабощение одних групп людей другими в условиях современного мира, где осуществление глобального открытого противоборства, ввиду распространения оружия, способного навредить всей планете, нежелательно. Подобной точки зрения придерживаются исследователи А. М. Соколова и Д. Б. Фролов, определяя информационную войну как особую форму политических отношений. Информация в данном подходе рассматривается как инструмент достижения превосходства во всех сферах государственной деятельности [2].

Социально-коммуникативный аспект как основной рассматривают М. Ю. Павлютенкова и Д. А. Швец. По мнению ученых информационная война представляет собой коммуникативную технологию, направленную на достижение информационного превосходства в интересах национальной стратегии. На первое место в данной теории выходит изучение именно информации, как главенствующего компонента влияния на чужие информационные ресурсы, с целью защиты собственных [2].

Сторонники конфликтологического подхода, такие как Р. Шафрански, Дж. Дериан, Д. Ронфельдт рассматривают информационную войну как вид военного конфликта, выступающего как часть или как самостоятельное военное действие, преследующее цель разрушение информационных систем противника для его дезориентации [2].

Наиболее полное виденье феномена информационной войны представляется возможным при системном подходе. В работах С. П. Расторгуева, С. Н. Бухарина и В. В. Цыганова информационная война выступает как закономерный процесс. Согласно работам ученых, воздействие информационных систем друг на друга в условиях постоянного развития неизбежно. По их мнению, главная преследуемая цель — превосходство в духовной и политической сферах, которое достигается путем дезинформации или уничтожения другой стороны [2].

Таким образом, проанализировав различные подходы к изучению вопроса существования информационных войн, можно сделать вывод касаемо их определения. По нашему мнению, наиболее точным будет определение российского политолога Андрея Викторовича Манойло, который определяет информационную войну как противоборство сторон, посредством распространения специально подготовленной информации и противодействия аналогичному внешнему воздействию на себя [3].

В современном международно-правовом пространстве существует множество документов, обеспечивающих защиту граждан от вредоносной информации, таких как всеобщая декларация прав человека, конвенция по правам человека и другие. Однако, ни в одном из данных документов не встречается понятия информационной войны, что затрудняет регулирование противоправной деятельности по воздействию на массовое сознание посредством информации [5].

Таким образом, можно сделать вывод о необходимости изучения всех аспектов такого понятия как информационная война, что поможет установить четкие критерии для регулирования данного вопроса.

Список источников

1. Аюрова, А. М. Информационная война как феномен информационного общества / А. М. Аюрова // Экспериментальные и теоретические исследования в современной науке : Сборник статей по материалам II международной научно-практической конференции. Том 2 (2) : Ассоциация научных сотрудников "Сибирская академическая книга", 2017. – С. 67-76. – EDN ZGHGNH.

2. Кунакова, Л. Н. Информационная война как объект научного анализа (понятие и основные характеристики информационной войны) / Л. Н. Кунакова // Альманах современной науки и образования. – 2012. – № 6. – С. 93-96. – EDN OZGEKF.

3. Манойло А.В. Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта. Киев: psyfactor.org (2005). Материалы V Международной научно-практической конференции «Информационные технологии и безопасность», вып. №8, 2005. С. 73-80.

4. Мао Цзэдун. Вопросы стратегии партизанской войны против японских захватчиков. Избранные произведения. Том 2. Москва: Издательство иностранной литературы, 1953.476 с.

5. Руф В. С. Правовой взгляд на концепцию информационной войны// Уральский журнал правовых исследований. 2022. № 4. С. 84-89. DOI 10.34076/2658 512X 2022 4 84.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Васина Т. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004:056

Методики управления потоками информации как способ защиты от негативных информационных воздействий

Татьяна Вячеславовна Васина[1]✉, **Кирилл Евгеньевич Шинаков**[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] tata.vasina.666@gmail.com✉, https://orcid.org/0009-0009-9243-3869
[2] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. В статье затрагивается вопрос эффективного решения задач в условиях непрекращающегося потока информации, который окружает каждого современного человека. Рассматривается теория гидранта, как доказательство существования трудностей продуктивного и рационального использования времени при влиянии огромного объема информации. Предлагаются методики управления информационными потоками.

***Ключевые слова*:** информация, интернет, социальные сети, теория гидранта, поток информации.

Для цитирования: Васина Т. В., Шинаков К. Е. Методики управления потоками информации как способ защиты от негативных информационных воздействий // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 35–38.

Жизнь человека неразрывно связана с информацией. С момента зарождения человечества, сбор и систематизация полученных знаний играют важную роль в выживании. С каждым последующим поколением, полученный опыт преумножается, становится более комплексным.

Научно-технический прогресс и развитие информационных технологий делают информацию вездесущей. С распространением интернета и популяризацией социальных сетей каждую секунду мозг обрабатывает свежие новости, новые сведения и данные.

Объем получаемой современной человеком информации настолько велик, что справедливо прибегнуть к сравнению Мэттью Лоури, специалиста в области онлайн-коммуникации, который называет непрерывный поток информации «гидрантом» (от англ. firehose). Действительно, сети и гаджеты буквально сбивают напором сведений [1].

Представим среднестатистического современного человека, являющегося пользователем сети Интернет, социальных сетей, обладающего базовым набором гаджетов. Первый этап его утренней рутины — просмотр телефона. И тут же его поджидает волна уведомлений, писем, сообщений в социальных сетях, реклама. Появление приоритетных задач, перенос встреч, чат с коллегами, уве-

домление о поступлении заказа — все это сбивает только проснувшегося пользователя с толку. Но это далеко не конец, информация как снежный ком, лишь растет со временем, ведь ее поток непрерывен. Днем пользователь окружен радио, музыкой, рассказами коллег, разговором с боссом, друзьями. Вечером, когда, казалось бы, есть время для отдыха, он все еще под воздействием потока: новости, фильмы и сериалы, реклама и даже собственный мозг не дает человеку отдохнуть. Необходимость обработки сообщений занимает мысли каждую секунду.

Для того, чтобы контролировать «гидрант» в статье предлагаются следующие методики управления потоками информации.

1. Структурирование рутины.

Эта техника позволяет организовать каждый день так, чтобы синхронизировать время работы и время, когда мозг способен сосредоточиться лучше всего. Стоит проследить за своей работоспособностью и выяснить, наиболее продуктивные и эффективные промежутки времени.

К примеру, пик продуктивности пользователя приходится на утро. Тогда следует выделить 2–3 часа в этот период, чтобы поработать над самой главной задачей дня, ни на что не отвлекаясь. Согласно исследованиям, если сотрудника отвлекают или он отвлекается сам хотя бы раз в три минуты, ему необходимо в среднем 23 минуты, чтобы снова погрузиться в дела.

При этом, задача должна быть действительно сложной и важной. В течение дня обязательно возникнут непредвиденные обстоятельства или дополнительные встречи, из-за которых дела первостепенной важности так и останутся невыполненными.

Как правило, спустя 60–90 минут интенсивного труда концентрация снижается. В этом случае стоит перерыв, сменив деятельность.

Весь день также можно разделить на две части. Например, проводить встречи или созвоны сразу после обеда, а оставшееся время посвятить задачам, связанным с менеджментом и планированием работы. Проверять входящие сообщения и почту при этом можно всего дважды — утром и днём, чтобы не отвлекаться от дел.

2. Изучение — Перемещение в очередь или запас — Поделиться.

Эта методика помогает разделить бессистемный поток из «гидранта» на три категории: удобный список задач; личную библиотеку полезных материалов; источники информации, которой стоит поделиться с коллегами или друзьями. Заниматься таким распределением можно как утром, так и вечером.

Первый шаг подразумевает анализ всей поступающей информации. К ней относится всё, что угодно, от рабочих и личных писем до уведомлений из приложений и сайтов. Здесь важно понимать, что большинство из этого не требует незамедлительного ответа.

Открывать каждое сообщение и отвечать на него не слишком эффективно. Чтобы не терять концентрацию, лучше сосредоточиться на чём-то одном — например, только просматривать входящие. Если вы можете «просканировать»

их быстрее чем за две минуты, сделайте это. Если нет, добавьте в список задач, к которым нужно вернуться позднее.

Анализируйте поток входящих два раза в день. Когда делаете это утром, задавайте себе вопрос, насколько каждое сообщение срочное. Так у вас получится не тратить драгоценное время, которое хотелось бы посвятить самой важной задаче дня.

На следующем этапе несрочные входящие, выполнение которых займёт больше двух минут, можно разделить по двум направлениям.

Первое — это то, что нужно прочитать, например онлайн-ресурсы, которые вы хотите изучить и обдумать. Сохраняйте их в избранном в браузере или в заметках. Таким образом сформируется личная библиотека полезных материалов, которую потом можно использовать при необходимости.

Второе — это то, что нужно сделать. Переносите дела в бумажный ежедневник или электронный планировщик. Во-первых, написанное лучше запоминается, а во-вторых, список задач всегда под рукой.

Последний шаг — опубликовать ссылки на понравившиеся материалы в своих личных аккаунтах или переслать в рабочие чаты, если вы уверены, что они будут интересны и полезны коллегам.

3. Доведение начатого до конца.

Это касается всех задач, которыми человек занимается. Как только пользователь решает оставить задачу невыполненной, фоновые мысли о ней сразу же заполняют мозг. При этом, взяться за нее, зачастую, очень проблематично. Таким образом, есть риск не только переполнить свое и без того уставшее сознание ненужной информацией, но вовсе забыть про необходимость закончить то или иное дело. Подводя итог изложенному, стоит заметить, что теория гидранта подразумевает непрерывность потока информации, от которой страдает каждый современный человек. В условиях, бесконечных новостей, сообщений, сведений и рекламы, эффективность и продуктивность может снижаться. Использование предложенных в статье методик направленно на управление потоками информации, помогая распределить и структурировать ее. Таким образом, пользователь может снизить негативное информационное воздействие, оказывающее влияние на его психическое и физическое здоровье.

Список источников

1. Лайфхакер [Электронный ресурс] – Режим доступа: https://lifehacker.ru/, свободный (Дата обращения 13.02.2024).

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Васина Т. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Васина Т. В. – написание статьи, сбор материала, обработка материала (70 %).

Шинаков К. Е. – идея, научное редактирование текста (30 %).

Конфликт интересов отсутствует.

Научная статья
УДК 004:056

Негативное влияние социальных сетей как феномен современности

Татьяна Вячеславовна Васина[1]✉, **Кирилл Евгеньевич Шинаков**[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] tata.vasina.666@gmail.com✉, https://orcid.org/0009-0009-9243-3869
[2] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. *Д*анная статья определяет роль социальных сетей в современном обществе, дает краткую характеристику самых востребованных в России сервисов. Приведен перечень потенциальных угроз социальных сетей. Предложены пути устранения негативного воздействия их использования.

Ключевые слова: социальные сети, негативное воздействие, информационные технологии, информатизация.

Для цитирования: Васина Т. В., Шинаков К. Е. Негативное влияние социальных сетей как феномен современности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 39–43.

Технический прогресс, распространение сети Интернет и развитие информационных технологий — вот реалии, в которых приходится жить современному человеку.

Мир захватили социальные сети. День большинства людей не проходит без интернета: скроллинг ленты, просмотр видео, новостей, общение с друзьями — все это не обходится без помощи всемирной паутины.

Практические все сферы жизни теперь перемещены в онлайн: дружба, отношения, хобби, интересы, работа. Каждый день социальными сетями пользуются миллиарды людей по всему миру. Согласно статистике DataReportal Digital 2023 Global Overview Report на начало 2023 года в Российской Федерации насчитывалось 127,6 млн интернет-пользователей. В январе число пользователей социальных сетей составило 106,0 млн пользователей, что составляет 73,3 % от общей численности населения [3].

Наиболее популярными социальными сетями в России являются ВКонтакте и Одноклассники, принадлежащие крупной корпорации VK. Платформы имеют огромное количество инструментов; есть возможности для создания абсолютно разного контента: клипов, подкастов, сообществ, историй, постов. Системы монетизации делают сети подходящими для продвижения собственного бизнеса и блога.

Одно из самых популярный приложений, ставшее самым скачиваемым в мире в 2020 году и захватившее внимание более миллиарда зрителей — TikTok — сервис для создания и просмотра коротких видеороликов.

Telegram — мессенджер, появившийся в России не так давно, однако уже успевший полюбиться пользователям. Предоставляет возможности для общения, создания каналов, в которых можно делиться контентом, секретных чатов и чат-ботов.

По заказу НИУ «Высшая школа экономики» в октябре 2022 года было проведено исследование, которое показало, что средняя продолжительность суточного времяпрепровождения в социальных сетях составляет более 4 часов. Эти результаты показывают, как много упомянутые интернет ресурсы значат для современного человека. Однако, несмотря на кажущиеся преимущества и безобидность, сервисы могут нести в себе угрозу не только для индивида, но и для общества в целом.

В приведенной ниже таблице приведены проблемы самых распространенных в России социальных сетей и представлены потенциальные угрозы для пользователя, к которым они могут привести.

Название социальной сети	Недостатки социальной сети	Потенциальная угроза
ВКонтакте, Одноклассники	Частый взлом аккаунтов и большое количество вредоносных (фишинговых) ссылок	Пользователи данных социальных сетей часто сталкиваются со взломом аккаунтов [1]. В следствие чего мошенники заполучают переписки, персональные данные и контакты пользователя, что может повлечь за собой шантаж. Вредоносные ссылки, по которым даже опытный пользователь может случайно перейти, — серьезная угроза для конфиденциальной информации. Они также являются инструментом мошенников для взломов страниц.
	Кибербуллинг	Кибербуллинг, или травля в интернете, оказывает негативное влияние на здоровье на двух уровнях: физическом и психологическом. Жертвы буллинга испытывают стресс и тревожность. Исследования показывают, что данный вид психологического насилия за последние годы увеличил количество

Название социальной сети	Недостатки социальной сети	Потенциальная угроза
		суицидов среди подростков [4]. Сильный стресс, в свою очередь, сказывается на здоровье: человек может испытывать бессонницу, проблемы с пищеварением и пищевым поведением [2].
	Высокие возможности поисковой системы	Делают доступ к группам и видеороликам с порнографическим и иным вредоносным содержанием простым.
	Большой объем личной информации, требующийся при регистрации и открытый доступ к информации о нахождении в сети	При регистрации в ресурсах требуется большой пласт личной информации, уязвимость которой очень высока. Более того, социальные сети показывают нахождение или отсутствие пользователя в сети, время его последнего посещения сайта, а также девайс, с которого осуществляются действия. Это может стать реальной угрозой для пользователя, его жизни и имущества.
TikTok	Огромный поток быстрого контента	Длительный просмотр коротких видеороликов, которые отвечают запросам пользователя могут вызвать дофаминовую зависимость (дофаминовая зависимость — стремление к получению удовольствия, обусловленное химическим веществом в мозге — дофамином), вызванную предвкушением чего-то приятного и интересного. Просматривая поток захватывающих роликов, мозг подсаживается на ощущение радости, которое приносит дофамин. Данная зависимость ведет к рассеянному вниманию, что затрудняет принятие решений и выполнение задач, требующих концентрации. Более того, бесконечный скроллинг социальной сети может привести к разбалансировке нервной системы, результатом которой являются гипертро-

Название социальной сети	Недостатки социальной сети	Потенциальная угроза
		фированные особенности личности.

Таким образом, справедливо говорить о негативном влиянии социальных сетей.

Существует множество способов, к которым может прибегнуть любой пользователь для того, чтобы обезопасить себя от негативного воздействия, или снизить его. Для этого необходимо окружить себя контентом, который интересен и безопасен. В статье рассмотрены методы настройки контента на примере пользователя, который увлечен изобразительным искусством.

Настройка алгоритмов рекомендаций схожа во всех социальных сетях. Для получения более персонализированного контента пользователь должен:

1. Больше взаимодействовать с контентом, который нравится. Алгоритмы устроены так, что предлагают нам информацию, основываясь на нашем предыдущем поведении. Таким образом, если пользователь заинтересован в изобразительном искусстве, то самым простым вариантом окружения себя полезным контентом будут лайки, репосты, комментирование и сохранение постов с подобной информацией.

2. Подписываться на сообщества и аккаунты людей, контент которых вызывает интерес. Для рассматриваемого пользователя, идеальным вариантом станет подписка на аккаунты художников, дизайнеров, а также сообщества музеев, картинных галерей и выставок.

3. Отмечать нежелательный контент. Во всех социальных сетях есть возможность скрыть нежелательный контент. Например, для обозначенного выше пользователя, спортивный контент является неинтересным, соответственно он будет только засорять ленту ненужной информацией. Минимизации таких постов поспособствует отметка записи как нежелательной или неинтересной и скрытие ее из новостной ленты.

4. Проводить анализ своих подписок и друзей. Большинство социальных сетей предлагают в рекомендации контент контактов и сообществ. Полезным с точки зрения формирования правильного контента станет стабильная проверка страниц, на которые пользователь подписан. Следует окружить себя теми, кто делится действительно интересующим его контентом. Если же сообщество сменило свою тематику — незамедлительно отписываться.

При этом, стоит помнить, что настройка алгоритмов рекомендаций — непрерывный процесс. Поэтому лишь регулярность пользовательской активности сможет ослабить негативное влияние социальных сетей.

Подводя итог вышесказанному, стоит отметить, что использование социальных сетей является неотъемлемой частью жизни современного человека. Однако, не стоит забывать, что они могут нести в себе потенциальную угрозу.

Необходимо учитывать их негативное влияние, и знать, как сделать времяпрепровождение в интернете более безопасным.

Список источников

1. ТАСС : информ. агентство России : сайт. Москва. Обновляется в течение суток. URL: https://tass.ru/ekonomika/12212773 (дата обращения: 15.03.2024).

2. Шогенов Б.Ю., Кумахова Д.Б. Влияние стресса на человека: электронная версия. URL: https://cyberleninka.ru/article/n/vliyanie-stressa-na-cheloveka (Дата обращения: 1.04.2024).

3. DataReportal Digital 2023: Russian Federation [Электронный ресурс] – URL: https://datareportal.com/reports/digital-2023-russian-federation (Дата обращения: 20.03.2024).

4. JAMA Network Open. Association of Cyberbullying Experiences and Perpetration With Suicidality in Early Adolescence. URL: https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2793627.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Васина Т. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Васина Т. В. – написание статьи, сбор материала, обработка материала (70 %).

Шинаков К. Е. – идея, научное редактирование текста (30 %).

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004:056

Факторы негативного информационного воздействия в условиях развития информационных войн

Татьяна Вячеславовна Васина[1], Кирилл Евгеньевич Шинаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] tata.vasina.666@gmail.com✉, https://orcid.org/0009-0009-9243-3869
[2] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. В данной статье рассматриваются факторы негативного информационного воздействия в условиях современной информационной войны.

Ключевые слова: информация, инфоксикация, дезинформация, информационное негативное воздействие.

Для цитирования: Васина Т. В., Шинаков К. Е. Факторы негативного информационного воздействия в условиях развития информационных войн // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 44–47.

В наши дни, вездесущность информации приобрела невиданные масштабы. Очевидно, жизнь каждого современного человека пронизана данными, новостями, статистиками и так далее. Ученые и специалисты таких областей как социология, психология и медицина все чаще говорят об инфоксикаци, то есть перенасыщении мозга человека информацией, в условиях, когда он просто не может справиться с ее объемом.

Несомненно, средства массовой информации можно рассматривать как благо, которое дает современному человеку возможность узнавать новости быстро и объемно. Тем не менее, современные СМИ кроют в себе множество недостатков, способных навредить человеку.

С развитием технологий, социальных сетей, все больше информации нас окружает. Несмотря на очевидные плюсы, такие как возможность узнать информацию быстро, во всех деталях, взглянуть на ситуацию с разных сторон, изучив различные мнения, есть причины говорить в возможном негативном информационном воздействии.

В работе рассмотрено негативное информационное воздействие как сумма всех встречающихся негативных факторов, которые могут нести в себе скрытую угрозу:

$$N = P_1 + P_2 + P_3,$$

где N — абсолютное негативное информационное воздействие;

Р — факторы, оказывающие негативное воздействие.

В таблице 1 представлены факторы, оказывающие негативное информационное воздействие в виде таблицы с примерами и возможными последствиями.

Таблица 1

№	Фактор, оказывающий негативное воздействие	Пример	Результат
1	Незамедлительная передача с места события	Теракты 11 сентября 2001 года	Формируется ложно чувство срочности, формирует важность предмета информации. Человек погружается в событие, что может повлечь за собой посттравматический синдром.
2	Дробление информации	Норд-Ост	Затрудняет осмысленный анализ поступающей информации, делает человека уязвимым, путает в событиях. Не позволяя собрать картину происходящего воедино.
3	Избыточная информация	Колумбайн	Появление подражателей.

Для более детальной оценки целесообразно рассмотреть факторы подробно.

Незамедлительная передача с места события кажется вполне правильным подходом в освещении происшествий. Таким образом, при возникновении ряда опасностей, население осведомляется молниеносно. Однако, примером негативного влияния незамедлительной передачи информации являются теракты 11 сентября 2001 года в США, когда боевики-смертники террористической организации "Аль-Каида" захватили четыре пассажирских самолета, направив два из них на башни Всемирного торгового центра, а два других на Пентагон и, предположительно, на Белый дом или Капитолий. Информация передавалась мгновенно. Многие тележурналисты и их съемочные группы искали информацию и вели репортажи в прямом эфире из мест, максимально близких к местам терактов. Однако, информация с таких происшествий обычно является эмоционально перегруженной, от чего зритель погружается в событие, ощущая на себе невероятное эмоциональное напряжение, что в дальнейшем может отразиться на психике.

В так называемом Норд-Осте можно проследить еще один фактор, который может оказать негативное влияние на человека — дробление информации. «Норд-Ост» стал первым в России терактом, активное освещение которого велось в интернете, в том числе в блогах тех, кто находился у Театрального центра. Из происшествия сделали практически реалити-шоу. Велись переговоры с террористами, на место прибывали звезды и депутаты. Однако важные детали

происшествия поступали порционно, что не позволяло собрать картину происходящего воедино и осмыслить происходящее.

Пример негативного влияния избыточной информации четко прослеживается в «Колумбайне», где двое старшеклассников Эрик Харрис и Дилан Клиболд расстреляли 12 учеников и одного учителя. Харрис и Клиболд покончили с собой прямо в школе, оставив после себя дневники и манифест. Главным следствием трагедии стало ее превращение в культовое событие, чему активно способствовали средства массовой информации. Произошедшее в «Колумбайне» было далеко не первым массовым убийством в американских образовательных учреждениях, но никогда ранее издания не освещали школьную стрельбу настолько широко. Впоследствии журналисты детально рассказывали о ходе судебного процесса, личностях и биографиях убийц. В открытом доступе оказались дневник Харриса с человеконенавистническими идеями и мотивами преступления, а также записи процесса бойни в школе с камер видеонаблюдения. Это повлекло за собой волну школьных убийств и появление группы подражателей [1].

Исходя из вышесказанного, можно сделать вывод о том, что максимально негативное воздействие оказывается на человека при суммировании данных факторов.

Решение этих проблем лежит в создании жесткой политики для средств массовой информации, которая будет включать такие аспекты как:

1. СМИ должны публиковать информацию в полном объеме, не дробя ее на небольшие части. Получая сведения, адресат должен иметь общую картину происходящего.

2. Важным условием политики является достоверность информации во всех официальных источниках. Новость не должна разниться от одной новостной передачи к другой.

3. Утаивание важной информации недопустимо в раках предлагаемой политики.

4. СМИ должны перестать романтизировать жестокость. Художественные фильмы об убийцах и террористах должны подвергаться цензуре и не транслироваться по общедоступным каналам средств массовой информации.

Данная политика средств массовой информации будет оказывать благоприятное влияние на социокультурную ситуацию в стране. Доверие медиапространству будет повышаться, а отсутствие кадров жестокости в общем доступе снизит случаи насилия в реальной жизни.

Список источников

1. Шувалов, Л. А. Влияние средств массовой информации на популяризацию феномена скулшутинга / Л. А. Шувалов // Вестник Тверского государственного университета. Серия: Филология. – 2022. – № 1(72). – С. 149-154. – DOI 10.26456/vtfilol/2022.1.149. – EDN GLLHWK.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Васина Т. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.53

Анализ систем управления ложными целями с открытым исходным кодом

Денис Александрович Вислобоков[1]✉, Илья Сергеевич Шишкин[2]
[1, 2] Тамбовский государственный технический университет, Тамбов, Россия
[1] denis.vislobokov@mail.ru✉, https://orcid.org/0009-0006-6986-4132
[2] ilya.shishkin.14@bk.ru, https://orcid.org/0009-0004-6413-8364

Аннотация. В статье выполнен сравнительный анализ открытого программного обеспечения (ПО) категории Deception Technology, рассмотрена история появления данной технологии. Результаты позволяют оценить функционал и разнообразие доступных решений и выбрать наиболее подходящее для конкретных потребностей организации.

Ключевые слова: информационная безопасность, кибербезопасность, системы обнаружения вторжений, honeypot, deception, открытое ПО.

Для цитирования: Вислобоков Д. А., Шишкин И. С. Анализ систем управления ложными целями с открытым исходным кодом // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 48–53.

Введение

В настоящее время обеспечение безопасности информационных ресурсов становится все более важной задачей в условиях роста угроз кибербезопасности. Одним из подходов к повышению защиты является использование концепции «deception» (от англ. «обман»), которая направлена на создание ложных представлений о сетевой инфраструктуре с целью затруднения атак и оповещения о них. Это один из вариантов системы обнаружения вторжений (IDS, Intrusion Detection System).

Цель исследования заключается в проведении обзора существующих решений с открытым исходным кодом в области deception с целью выявления их особенностей, преимуществ и ограничений. Актуальность данного исследования обусловлена необходимостью повышения эффективности киберзащиты в условиях постоянно меняющихся угроз и методов атак.

История deception: эволюция концепции обмана в кибербезопасности

Первые упоминания о применении обмана в компьютерных системах можно отнести к концепции «honeypot» (ханипот), которая появилась в 1990-х годах. Идея заключалась в создании ловушки или приманки: ложного компьютерного ресурса, который привлекал злоумышленников, давая возможность анализировать их действия и защищать реальные системы [1].

С течением времени и с развитием технологий, концепция deception стала более сложной и разнообразной. Вместо простых ханипотов стали разрабатываться и применяться более сложные методы обмана. В результате появились целые платформы для развёртывания и управления ложными целями, включающие в себя создание фальшивых сетевых ресурсов, искажение информации о конфигурации сети, а также маскировку реальных активов под ложные.

В современных системах кибербезопасности deception может играть ключевую роль в стратегиях защиты информации. Он позволяет создавать дополнительные барьеры для злоумышленников, усложняя процесс атаки и повышая шансы на обнаружение их действий.

Сравнительный анализ deception-систем в виде открытого ПО

Выбор подходящей deception-системы может быть сложным, учитывая разнообразие коммерческих и открытых решений, доступных на рынке. Многие подобные системы предлагаются в виде коммерческих продуктов, зачастую входящих в целую систему безопасности того же производителя. Они обладают широким функционалом и удобством использования, разработаны для использования в большинстве из возможных сетей и устройств, а также имеют поддержку и постоянные обновления.

Решения, построенные на открытом исходном коде, представляют собой интересную альтернативу коммерческим продуктам, обеспечивая гибкость, прозрачность и возможность самостоятельной настройки под конкретные потребности организации.

Анализ направлен на выявление особенностей и функциональных возможностей нескольких известных открытых систем управления ложными целями, их архитектуры, поддерживаемых протоколов и сервисов, а также интеграционных возможностей. Это позволит оценить преимущества и ограничения каждого решения и поможет принять обоснованное решение при выборе deception-системы на основе открытого исходного кода.

В качестве анализируемых представлены следующие системы: T-Pot, DejaVU, OWASP Honeypot, Chameleon, Honeytrap, CHN и MHN.

T-Pot — это универсальная платформа с возможностью распределения, поддерживающая несколько архитектур (amd64, arm64), для создания ловушек, более 20 типов ловушек и бесчисленные варианты визуализации с использованием стека Elastic. Она также предоставляет анимированные карты атак в реальном времени и множество инструментов безопасности для дополнительного улучшения опыта с deception [2].

DejaVU — это deception-платформа, которая может использоваться для развертывания приманок как в облаке (AWS), так и во внутренней сети. Поддерживает 14 типов серверных приманок и 4 клиентских [3].

OWASP Honeypot — это открытое ПО, написанное на языке Python, предназначенное для создания ханипотов и сетей из них легким и безопасным способом. Этот проект совместим с Python 3.x и протестирован на Mac OS X и Linux [4].

Chameleon предлагает 19 настраиваемых ловушек для мониторинга сетевого трафика, активности ботов и учетных данных пользователей (DNS, HTTP-прокси, HTTP, HTTPS, SSH, POP3, IMAP, SMTP, RDP, VNC, SMB, SOCKS5, Redis, Telnet, Postgres, MySQL, MSSQL, Elastic и LDAP) [5].

Honeytrap — это расширяемая и открытая система для запуска, мониторинга и управления ловушками, поддерживающая несколько операционных систем, таких как Linux, MacOS и Windows [6].

CHN (Community Honey Network) позволяет автоматизировать развертывание ловушек и управление ими. Поддерживает следующие ханипоты: Cowrie, Dionaea, Conpot, RDPHoney, UHP [7].

MHN (Modern Honey Network) — это централизованный сервер для управления и сбора данных с ловушек. MHN позволяет быстро развертывать сенсоры и сразу же собирать данные, которые можно просматривать через удобный веб-интерфейс. Скрипты развертывания ловушек включают несколько распространенных технологий, включая Snort, Cowrie, Dionaea и glastopf [8].

Далее требуется определить критерии сравнения рассматриваемых систем. Основными параметрами, определяющими функциональность подобных решений, являются:

- поддерживаемые операционные системы (ОС);
- поддерживаемые системы виртуализации;
- поддерживаемые облачные сервисы;
- типы приманок в зависимости от используемых протоколов и сервисов;
- безагентность, определяющая возможность размещения ловушек без дополнительного ПО на хостовой части и понижающая риск обнаружения злоумышленником.

Результаты сравнения представлены в таблицах 1 и 2.

Таблица 1

Сравнение систем T-Pot, DejaVU, OWASP Honeypot, Chameleon

Разработчик	Deutsche Telekom Security	Camolabs	OWASP	QeeqBox
Наименование ПО	T-Pot	DejaVU	OWASP Honeypot	Chameleon
Поддерживаемые ОС для развертывания системы	Debian 11	Представляет собой модифицированный Debian	Mac OS X, Linux (Debian/Ubuntu)	Linux
Поддерживаемые ОС для размещения приманок	Docker-совместимые Linux	Linux, MacOS и Windows	Docker-совместимые	Linux, MacOS и Windows
Поддерживаемые системы виртуализации	UTM, VirtualBox, VMware vSphere/ESXi, Fusion, Workstation, KVM	VirtualBox, VMware ESXi	Не указано	Не указано
Поддерживаемые облачные сервисы	Telekom OTC, AWS	AWS	Не указано	AWS

Окончание табл. 1

Разработчик	Deutsche Telekom Security	Camolabs	OWASP	QeeqBox
Типы приманок	ADB, Cisco ASA, Citrix ADC, ICS/SCADA, SSH, Telnet, DNS, NTP, SSDP, CHARGEN Random/mock UDP, Elasticsearch, LDAP, HTTP Proxy, HTTPS, IMAP, POP3, Redis, Postgres, SMB, SNTP, VNC, DICOM, BLACKHOLE, EPMAP, FTP, HTTP, MEMCACHE, MIRROR, MQTT, MSSQL, MYSQL, PPTP, SIP, TFTP, UPNP, IRC, PJL, IPP, RDP, DHCP, SMTP, HL7/FHIR	MYSQL, SNMP, HTTP, TELNET, SMB, FTP, TFTP, Tomcat, Apache, Basic Auth, SSH, SMTP, RDP, VNC, HONEYCOMB, ICS/SCADA, NBNS, MITM, SSDP, Email	FTP, SSH, HTTPS, SMTP и ICS	DNS, HTTP Proxy, HTTP, HTTPS, SSH, POP3, IMAP, STMP, RDP, VNC, SMB, SOCKS5, Redis, TELNET, Postgres, MySQL, MSSQL, Elastic, ldap
Безагентское решение	Да	Да	Да	Нет

Таблица 2

Сравнение систем Honeytrap, CHN и MHN

Разработчик	DTACT	Jesse Bowling	Pwnlandia
Наименование ПО	HoneyTrap	CHN	MHN
Поддерживаемые ОС для развертывания системы	Mac OS X, Linux (Debian/Ubuntu), FreeBSD	Ubuntu, CentOS, Mac OS X	CentOS 6, Ubuntu 16.04/18.04
Поддерживаемые ОС для размещения приманок	Linux, MacOS	Ubuntu, CentOS, Mac OS X	Ubuntu 14.04/16.04
Поддерживаемые системы виртуализации	Не указано	Не указано	Не указано
Поддерживаемые облачные сервисы	Не указано	Не указано	Не указано
Типы приманок	DNS, HTTP Proxy, HTTP, HTTPS, SSH, POP3, IMAP, SMTP, RDP, VNC, SMB, SOCKS5, Redis, TELNET, Postgres, MySQL, MSSQL	SSH, Telnet, BLACKHOLE, EPMAP, FTP, HTTP, MEMCACHE, MIRROR, MQTT, MSSQL, MYSQL, PPTP, SIP, SMB, TFTP, UPNP, ICS, TCP, RDP	SSH, Telnet, BLACKHOLE, EPMAP, FTP, HTTP, HTTPS, MEMCACHE, MIRROR, MQTT, MSSQL, MYSQL, PPTP, SIP, SMB, TFTP, UPNP, ICS
Безагентское решение	Нет	Да	Да

Результаты сравнения представленных deception-систем показывают, что среди открытого ПО данного типа есть достаточно развитые решения, которые

к тому же имеют возможность доработки под конкретные условия использования.

В качестве наиболее устоявшегося продукта можно отметить систему T-Pot за счёт совместимости со множеством платформ и значительным списком поддерживаемых типов приманок.

Заключение

Обзор существующих открытых решений в области deception-систем демонстрирует, что данное направление в области кибербезопасности получило широкое распространение и продолжает активно развиваться. Введение deception-технологий позволяет создавать дополнительные слои защиты информационных систем, усложняя задачи атакующим и увеличивая вероятность обнаружения атак.

Анализ представленных решений выявил их разнообразие и функциональные возможности, что позволяет пользователям выбирать наиболее подходящую систему в соответствии с потребностями и особенностями их инфраструктуры. Так, система T-Pot отличается широкой совместимостью с различными платформами и многообразием поддерживаемых типов приманок, что делает ее одним из наиболее привлекательных решений. Другие открытые аналоги также заслуживают внимания, так как предлагают некоторые уникальные возможности, например, совместимость с Windows и Mac OS.

Также стоит отметить, что многие из представленных систем продолжают своё развитие, разработчики занимаются расширением функционала и совместимости как с различными платформами, так и с другими средствами безопасности.

Для дальнейшего совершенствования deception-систем важно продолжать исследования в этой области, учитывая постоянно меняющиеся угрозы и требования кибербезопасности. Это позволит разработчикам и пользователям находить новые способы защиты информационных ресурсов и эффективно бороться с современными киберугрозами.

Список источников

1. Spitzner L. Honeypots: Tracking Hackers. Addison Wesley. 2002. URL: http://www.it-docs.net/ddata/792.pdf.

2. T-Pot - The All In One Multi Honeypot Platform. URL: https://github.com/telekom-security/tpotce.

3. DejaVU - Open Source Deception Platform. URL: https://github.com/bhdresh/ Dejavu.

4. OWASP Honeypot. URL: https://github.com/OWASP/Python-Honeypot.

5. Chameleon. URL: https://github.com/qeeqbox/chameleon.

6. Honeytrap. URL: https://github.com/honeytrap/honeytrap.

7. Community Honey Network. URL: https://communityhoneynetwork.readthedocs .io/en/stable.

8. Modern Honey Network. https://github.com/pwnlandia/mhn.

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Вислобоков Д. А. – студент кафедры «Информационные системы и защита информации», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «ТГТУ».

Шишкин И. С. – студент кафедры «Информационные системы и защита информации», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «ТГТУ».

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004

Исследование проблематики обеспечения безопасности международных переводов в условиях деглобализации

Денис Дмитриевич Воробьёв[1]✉, Дмитрий Андреевич Лысов[2]✉, Константин Владимирович Зольников[3]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3] АО «Научно-исследовательский институт электронной техники», Россия
[1] dan.vorob2012@ya.ru✉, https://orcid.org/0009-0000-0881-6782
[2] lysovdmitriia@gmail.com✉, https://orcid.org/0009-0003-9666-7191
[3] k.v.zolnikov@gmail.com

Аннотация. В последнее время актуализировались вопросы, связанные с безопасностью международных переводов и платежей в условиях санкций. Предметом исследование является разбор текущей ситуации и методы ее разрешения. Особое внимание уделено принципу работы интернациональных платежей. В статье затрагивается тема осуществления денежных манипуляций через посредников. Даётся сравнение различных путей решения проблем. Автор приходит к выводу, что проблема постепенно решается и в ближайшем будущем обеспечение безопасности будет на высшем уровне.

Ключевые слова: деглобализация, SWIFT, платежи, переводы, НСПК, Мир, Visa, MasterCard, СНГ, Турция, иностранные банки, мошенничество.

Для цитирования: Воробьёв Д. Д., Лысов Д. А., Зольников К. В. Исследование проблематики обеспечения безопасности международных переводов в условиях деглобализации // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 54–58.

Ещё несколько лет назад нельзя было подумать о том, что отправить деньги заграницу станет настоящим испытанием, когда раньше для это требовалось буквально пару кликов и несколько секунд. Решение западного мира об отключении России от международных переводов после начала СВО не заставило себя долго ждать. Это и ускорило процесс деглобализации — процесса уменьшения взаимозависимости и взаимосвязанности между странами. Это означает изменение тенденции глобализации, когда страны стали более тесно связаны в экономическом, политическом и культурном отношениях. Деглобализация проявляется в сокращении международной торговли, иностранных инвестиций, сокращении международного сотрудничества и усилении протекционистской политики.

Такое случается не только в период военных действий. Достаточно вспомнить середину марта 2020 года, когда ВОЗ объявила пандемию COVID-19. Коронавирус и другие глобальные сбои выявили риски, связанные со сложными международными цепочками поставок. Это подталкивает страны и компании к перепрофилированию производства.

Предыдущий механизм международных финансовых транзакций в Российской Федерации был организован следующим образом: клиент предоставлял своему банку необходимые данные о получателе (включая имя, номер счета), а также название и SWIFT-код банка-получателя для его идентификации. Затем банк клиента осуществлял перевод средств через сеть SWIFT для безопасной доставки денег в банк-получатель. При этом средства могли быть конвертированы в валюту получателя. Наконец, банк-получатель принимал средства и зачислял их на счет получателя. **SWIFT (Society for Worldwide Interbank Financial Telecommunication)** — расшифровывается как Общество всемирной межбанковской финансовой телекоммуникации. SWIFT сам по себе не является банком. Он не хранит и не переводит средства. Это глобальная сеть обмена сообщениями, которую банки и финансовые учреждения используют для безопасной отправки инструкций и информации о финансовых транзакциях. Каждый банк в сети SWIFT имеет уникальный код, который позволяет точно идентифицировать его для упрощения переводов. Когда вы отправляете деньги за рубеж, банки используют сеть SWIFT для передачи деталей перевода, гарантируя, что он дойдет до нужного адресата. По такому принципу работают все мировые банки.

Отключение российской банковской системы от SWIFT не оправдало себя [5]. Для этого вернемся в 2014 год. После ввода санкций США платежные международные платёжные системы Visa и MasterCard второй раз в истории (впервые — в Иране) остановили обслуживание карт нескольких российских банков в торговых точках и банкоматах международной сети [2]. Была начата подготовка поправок в Федеральный закон «О национальной платёжной системе» с целью инфраструктурно и информационно замкнуть процесс осуществления денежных переводов внутри России. Так и появилась «Национальная система платёжных карт» и «Национальная платёжная система» [1].

Национальная система платёжных карт стала аналогом SWIFT для россиян, так как проведение всех операций по картам любых платежных систем стало осуществляться исключительно через данный сервис. Отметим, что НСПК является оператором «Мира» — российской национальной платежной системы, которая занимается обработкой всех транзакций внутри страны и развитием выпуска собственных платежных карт.

«Мир» появился в 2015 году. Тестирование и отладка заняли 2 года и в 2017 году стартовал массовых выпуск этих карт с появлением указа об обязательном переводе всех бюджетных выплат на карты национальной платежной системы [3].

На момент апреля 2024 года речи о переподключении SWIFT к РФ или о возвращении Visa и MasterCard не идёт. Вероятнее всего, россияне и вовсе забудут о некогда существовавших ПС, указанных ранее.

Спустя 2 года появилось множество способов осуществлять платежи и переводы заграницу. Например, открытие банковского счета в странах СНГ, таких как Беларусь или Казахстан, где банк имеет подключение к системе SWIFT или использование виртуальных платёжных карт, предоставляемых банками стран, например, Турции или ОАЭ.

Действительно, некоторые банки Беларуси (не попавшие под санкции), открывают счета в банках негражданам (нерезидентам) их страны. Но, как правило, это недешево, так как следует учитывать затраты на дорогу, проживание и питание. По самым скромным меркам тариф и расходы на поездку обойдутся не менее чем в 33 тыс. российских рублей. [4].

Однако, в Киргизии доступна возможность оформить карту удалённо — через посредника. Здесь и кроется проблема безопасности. Кроме того, что вы оформляете доверенность на имя посредника, так ещё у него будет возможность завладеть всеми вашими личными данными и реквизитами карты, в том числе CVV-код на обороте карты. Это сразу лишает вас каких-либо гарантий сохранности средств. Разумеется, в данном варианте получения карты предоплата 100 %.

И второй, не менее популярный способ — использование виртуальных карт иностранных (не СНГ-стран) банков. Еще в конце 2023 года турецкие карты мог получить любой желающий, пройдя регистрацию по номеру телефона. В таком случае, можно было хранить на счёте до 1500 турецких лир, позже — 2750 турецких лир (по курсу на апрель 2024 это около 7 900 руб.) и плюс ко всему — отсутствие 3DSecure. Несколько позже эта схема прекратила работать и турецкие банки стали требовать скан заграничного паспорта и фото лица вместе с ним. Но кроме таких ужесточений стали доступны существенные плюсы — появление 3DSecure. Для подтверждения операции код приходил на электронную почту или в СМС, что как бы уже лишало мошенников проводить сомнительные операции с картой. 2750 лир — это отнюдь не большой лимит и подойдет только для мелких покупок в интернете. Съездив в Турцию, а именно в головной офис данного банка, подписав контракт и удостоверив личность, вы повысите лимит до 500 тысяч лир, а это ни много ни мало полтора миллиона рублей в месяц. Важно отметить, при покупке на иностранном сайте в валюте типа Доллара США или Евро конвертация будет происходить по текущему курсу. Это говорит о том, что пользователю необязательно иметь несколько карт разных банков — для Евро, Долларов или другой валюты.

Проблема безопасности здесь заключается в трудности прямого перевода средств в турецкий банк. Зачастую каждый второй владелец данной карты пополняет её через посредника на разных торговых площадках. Вы вводите номер карты в незнакомых вам онлайн-кассах, переводите тысячи рублей

незнакомому вам человеку и ждёте пополнения карты. Посредник, в свою очередь, при поступлении ему ваших средств переводит лиры со своей турецкой карты (уже подтвержденной в Турции) на вашу. Или просто забирает ваши деньги и блокирует вас. При попытке купить турецких лир через посредника может прийти вот такое сообщение от банка (рис. 1).

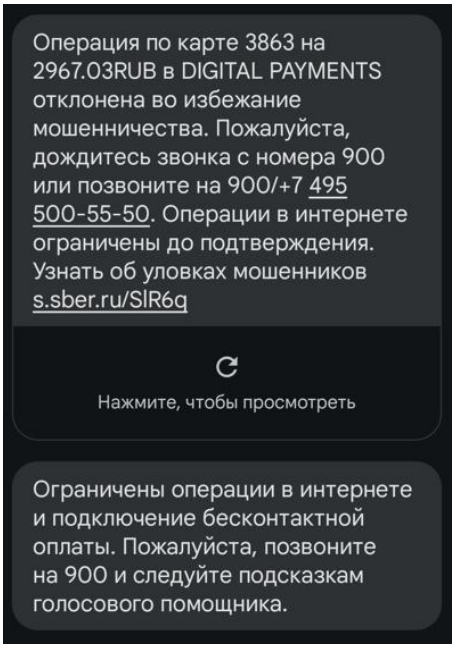


Рис. 1. Сообщение от Сбер банка

Операция была отклонена молниеносно, деньги остались на карте. Сотрудник позвонил, проверил информацию, тщательно допросил и предупредил о последствиях. После этого на 24 часа картой пользоваться нельзя было (кроме переводов через мобильное приложение).

Будущее стабильных международных платежей в РФ выглядит туманно. Если мировые гиганты платежных систем все же вернутся на российский рынок, то о былой славе можно забыть. Доверие подорвано. Разве что использовать в качестве второй и неосновной карты. Но нельзя оставлять надежды, что НСПК и «Мир» официально подключат страны, которые сейчас отвергают эту ПС. Проблема безопасности международных платежей уже активно решается и ПС Золотая Корона официально внедрила у себя пополнение турецких карт, оформленных на россиян, что сводит процент опасностей до нуля.

Проблема обеспечения безопасности международных переводов в условиях деглобализации постепенно становится менее актуальной, но оставляет за собой определенные риски. Отчетливо видно, что даже в такой изоляции находятся специалисты, которые готовые предлагать свои решения, которые помогут обеспечить комфорт, скорость и безопасность международных платежей.

Список источников

1. Данные о платежах по российским картам запретят передавать за рубеж – URL: https://web.archive.org/web/20160322174917/http://www.rbc.ru/economics/21/03/2014/912777.shtml (дата обращения: 01.04.2024).
2. Visa и Mastercard заблокировали операции банков Ковальчука и Ротенбергов – URL: https://web.archive.org/web/20160327204640/http://www.rbc.ru/economics/21/03/2014/912600.shtml (дата обращения: 01.04.2024).
3. Мир (платёжная система) – URL: https://ru.wikipedia.org/wiki/Мир_(платёжная_система) (дата обращения: 01.04.2024).
4. Как открыть банковскую карту в Беларуси в 2024 – URL: https://journal.tinkoff.ru/belarus-card/ (дата обращения: 01.04.2024).
5. Отключение от SWIFT не помогло! В Японии признали, что обрушить экономику России не удалось – URL: https://tsargrad.tv/news/otkljuchenie-ot-swift-ne-pomoglo-v-japonii-priznali-chto-obrushit-jekonomiku-rossii-ne-udalos_529240 (дата обращения: 04.04.2024).

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Воробьёв Д. Д. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

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

Зольников К. В. – к. т. н., ведущий инженер АО «НИИЭТ».

Вклад авторов

Воробьёв Д. Д. – сбор материала, обработка материала, написание статьи (80 %).

Лысов Д. А. – идея (10 %).

Зольников К. В. – обработка материала, написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Выявление освоенностей подходов к процессу компьютерной криминалистики

Алексей Петрович Горлов[1]✉, Дмитрий Андреевич Лысов[2]✉, Вероника Дмитриевна Медведева[3]✉, Вероника Вячеславовна Кузина[4]✉
[1, 2, 3, 4] Брянский государственный технический университет, Брянск, Россия
[1] apgorlov@gmail.com✉, https://orcid.org/0009-0003-3100-3466
[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. В настоящей статье авторами обоснована оценка современного состояния преступлений в сфере информационно-телекоммуникационных технологий. Представлена характеристика понятия «форензика» в направлении компьютерной криминалистики, определены сферы её применения, описаны этапы криминалистического процесса, а также проанализированы отечественные решения, применяемые в расследовании киберпреступлений.

Ключевые слова: компьютерная криминалистика, форензика, кибербезопасность, информационная безопасность, IT-технологии.

Для цитирования: Горлов А. П., Лысов Д. А., Медведева В. Д., Кузина В. В. Выявление освоенностей подходов к процессу компьютерной криминалистики // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 59–62.

В современном мире, где информационные технологии играют ключевую роль, проблема кибербезопасности становится все более актуальной. Развитие компьютерных наук нарастает с каждым годом, технологии постоянно совершенствуются и интегрируются в нашу повседневную жизнь, что приводит к необходимости обеспечения безопасности личной информации. Однако, необходимо помнить, что вместе с прогрессом технологий происходит и эволюция киберугроз, что приводит к расширению масштабов киберпреступности. Важным инструментом в борьбе с киберпреступностью являются знания в области компьютерной криминалистики.

В криминалистике уделено особое внимание такому явлению, как форензика, которое закрепилось за компьютерной ее частью, т. е. обозначает именно «компьютерная криминалистика» [1]. *Форензика* изучает методы расследования, оценки, изъятия и архивирования доказательств с электронного устройства с целью их использования в юридических разбирательствах [2].

Форензика играет важную роль в сфере компьютерной криминалистики и выполняет ряд критически важных функций:

1. Разработка тактики расследования и сбора доказательств, связанных с компьютерной информацией.

2. Создание методов и инструментов для сбора и анализа доказательств киберпреступлений.

3. Определение уникальных характеристик преступлений, связанных с компьютерной информацией, с криминалистической точки зрения.

Компьютерная криминалистика широко применяется в различных областях:

1. Расследование уголовных преступлений, где компьютерная информация является целью, инструментом или источником доказательств.

2. Сбор и анализ цифровых доказательств в гражданских делах, особенно в случаях нарушения интеллектуальной собственности, связанных с программным обеспечением, цифровым контентом и торговыми марками в Интернете.

3. Расследование страховых случаев, включая нарушение договоров и мошенничество, особенно в отношении компьютерных систем и цифровых активов.

4. Корпоративные расследования нарушений безопасности и меры по защите конфиденциальных данных.

5. Военные и разведывательные операции по сбору, уничтожению и восстановлению компьютерной информации в ходе кибератак и защите собственных систем.

6. Защита личной информации граждан в цифровом формате и их прав в отношении электронных документов и информационных систем.

Расследование, проводимое криминалистами и специалистами, проходит через следующие стадии:

1. Сбор информации и данных с компьютерных носителей предъявляет требования к проведению идентификации, указанию источников, установлению происхождения информации и объектов, а также к обеспечению их конфиденциальности, целостности и доступности.

2. Экспертный анализ собранной информации содержит извлечение и интерпретацию данных с носителей, декодирование и выделение той информации, которая имеет отношение к расследованию.

3. Анализ избранной информации осуществляется с применением научных методов для получения достоверных ответов.

4. Представление результатов исследования и анализа в соответствии с законом и представляются в понятной форме.

Для успешного расследования киберпреступности необходимы определенные инструменты. Поскольку иностранных поставщиков не так много, *отечественные компании предлагают отличные решения, позволяющие специалистам точно зафиксировать момент преступления и собрать надлежащие доказательства:*

1. Managed XDR (MXDR) — решение от компании Group-IB, позволяющее централизованно управлять защитой всей инфраструктуры, а также проводить расследования кибератак.

2. Threat Intellegence — решение, позволяющее быстро определить актуальный источник угрозы на основе данных о тактиках, инструментах и активности злоумышленников.

Известие о программном обеспечении для форензики в России началось несколько позднее, чем в других странах, однако уже есть *уникальные программные решения для проведения цифровых экспертиз в компьютерной сфере после совершения правонарушений [4]*.

1. AccessData Forensic Toolkit — программное обеспечение для проведения цифровой криминалистической экспертизы. Используется для анализа и восстановления данных с различных носителей информации, таких как жёсткие диски, USB-накопители, мобильные устройства и т. д.

2. Browser Forensic Tool — инструмент для криминалистического анализа данных веб-браузера. Позволяет исследовать историю посещений веб-сайтов, сохранённые пароли, файлы cookie и другие данные, которые могут быть полезны при расследовании инцидентов безопасности или анализе поведения пользователей.

3. The Sleuth Kit (TSK) — библиотека инструментов для проведения криминалистического анализа файловых систем. Предоставляет набор функций для извлечения и анализа данных с жёстких дисков и других носителей информации.

4. Encrypted Disk Detector — инструмент для криминалистического анализа данных, который может помочь обнаружить зашифрованные диски и файлы. Используется для восстановления данных и расследования преступлений, связанных с использованием зашифрованных носителей информации.

Таким образом, в свете быстрого научно-технического прогресса и повсеместного использованием интернета, *компьютерная криминалистика приобретает все большее значение и пользуется спросом. Следует отметить, что уход из страны зарубежных вендоров никак не сказался на уровне и качестве российской форензики.*

Список источников

1. Андропова, О. И., Голубев, Г. А. Компьютерная криминалистика: современное состояние и перспективы / О. И. Андропова, Г. А. Голубев // Материалы ежегодного криминалистического форума. Под общей редакцией А. А. Сапожкова. Санкт-Петербург, 2019. – С. 125-131. (дата обращения 18.04.2024).

2. Федотов, Н. Н. Форензика – компьютерная криминалистика / Н. Н. Федотов ; Николай Николаевич Федотов. – Москва : Юридический мир, 2007. – 359 с. (дата обращения: 20.04.2024).

3. Лебедков, С. В., Яковлев Д. Е. Сущность и природа «форензики» // Научные междисциплинарные исследования. 2021. №4. (дата обращения 20.04.2024).

4. Домин, К. Е. К вопросу о выделении криминалистического исследования электронных носителей информации как новой отрасли криминалистической техники // Библиотека криминалиста. Научный журнал. 2013. № 5 (10). – С. 176-177. (дата обращения 21.04.2024).

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Горлов А. П. – к. т. н., доцент 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», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

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

Вклад авторов

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

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

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Анализ угроз информационной безопасности в системах промышленного контроля

Кирилл Константинович Грибачев[1]✉, Максим Валерьевич Ковалев[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] zorgemauh@gmail.com✉, https://orcid.org/0009-0004-9548-135X
[2] makskovalew@mail.ru, https://orcid.org/0009-0000-2312-2279

Аннотация. Системы промышленного контроля (SCADA, ICS) являются неотъемлемой частью промышленных предприятий и инфраструктуры. Однако, с ростом цифровизации и интеграции этих систем в глобальные сети, угрозы информационной безопасности для них значительно увеличились. В статье проводится анализ угроз информационной безопасности в системах промышленного контроля в российском сегменте, с использованием статистических данных за 2020, 2021 и 2022 годы. Рассматриваются основные типы угроз, такие как кибератаки, физические атаки, ошибки человека и технические неполадки. В статье приводятся рекомендации по улучшению информационной безопасности в системах промышленного контроля и выводы о необходимости постоянного мониторинга и анализа угроз для обеспечения надежной работы промышленных предприятий в России.

Ключевые слова: информационная безопасность, системы промышленного контроля, SCADA, ICS, кибератаки, угрозы, мониторинг, Россия.

Для цитирования: Грибачев К. К., Ковалев М. В. Анализ угроз информационной безопасности в системах промышленного контроля // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 63–65.

Системы промышленного контроля (SCADA, ICS) являются неотъемлемой частью промышленных предприятий и инфраструктуры в России. Они используются для управления технологическими процессами, контроля качества продукции, мониторинга и диагностики оборудования. Однако, с ростом цифровизации и интеграции этих систем в глобальные сети, угрозы информационной безопасности для них значительно увеличились. В статье проводится анализ угроз информационной безопасности в системах промышленного контроля в российском сегменте, с использованием статистических данных за 2020, 2021 и 2022 годы.

Угрозы информационной безопасности в системах промышленного контроля в России могут быть разделены на несколько категорий:

1. Кибератаки — намеренные действия злоумышленников, направленные на получение несанкционированного доступа к системам промышленного контроля, кражу конфиденциальной информации, модификацию или уничто-

жение данных, нарушение работы систем. Согласно отчету компании Positive Technologies, в 2020 году 239 предприятий зафиксировали 220 атак на системы промышленного контроля. В 2021 году 209 предприятий подверглись кибератакам, 183 из которых были совершены в отношении систем промышленного контроля. В 2022 году на 308 предприятиях 92 атаки были направлены на системы промышленного контроля [1].

2. Ошибки человека — неправильные действия сотрудников предприятия, такие как неверное конфигурирование оборудования, ошибки при эксплуатации программного обеспечения, несоблюдение правил информационной безопасности [2]. Согласно отчету компании Infowatch, в 2020 году 180 нарушений были вызваны ошибками человека. В 2021 году это число увеличилось до 184 нарушений, а в 2022 году показатель вырос до 193 нарушений, произошедших в результате ошибки человека [3].

3. Технические неполадки — сбои в работе оборудования или программного обеспечения, вызванные техническими причинами. Согласно данным компании Kaspersky, в 2020 году 48 % промышленных предприятий в России столкнулись с техническими неполадками в системах промышленного контроля. В 2021 году этот показатель вырос до 52 %, а в 2022 году составил 55 % [4].

Для решения существующих проблем в области обеспечения информационной безопасности в системах промышленного контроля на отечественных предприятиях рекомендуется применять комплексный подход. Среди мер, которые включает в себя такой подход, как основные и обязательные к исполнению можно выделить следующие:

1. Постоянный мониторинг и анализ угроз — необходимо постоянно мониторить сеть и системы промышленного контроля на предмет появления угроз, анализировать их и принимать меры по их предотвращению.

2. Сегментация сети и контроль доступа — необходимо разделять сеть на зоны безопасности, ограничивать доступ к системам промышленного контроля только для авторизованных пользователей и применять политику безопасности на основе ролей.

3. Регулярное обновление программного обеспечения и оборудования — необходимо регулярно обновлять программное обеспечение и оборудование, устанавливать патчи безопасности и проводить регулярные проверки на наличие уязвимостей.

4. Подготовка персонала — необходимо обеспечить подготовку персонала в области информационной безопасности, проводить регулярные тренинги и тестирования на знание правил безопасности.

5. Создание планов реагирования на инциденты — необходимо разработать планы реагирования на инциденты, включающие меры по предотвращению, обнаружению, реагированию и восстановлению после нарушений информационной безопасности [5].

Угрозы информационной безопасности в системах промышленного контроля являются серьезной проблемой для промышленных предприятий и инфраструктуры в России. Статистические данные за 2020, 2021 и 2022 годы сви-

детельствуют о том, что угрозы информационной безопасности в системах промышленного контроля в России остаются высокими. Необходимо продолжать уделять внимание этой проблеме и применять все необходимые меры для защиты систем промышленного контроля от угроз информационной безопасности. Для обеспечения надежной работы систем промышленного контроля необходимо применять комплексный подход, включающий постоянный мониторинг и анализ угроз, сегментацию сети и контроль доступа, регулярное обновление программного обеспечения и оборудования, подготовку персонала и создание планов реагирования на инциденты.

Список источников

1. Исследования. Аналитики Positive Technologies [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/.

2. Кирилина, Т.Ю. Нормативно-правовое регулирование информационной безопасности автоматизированных систем управления технологическими процессами / Т.Ю. Кирилина, Е.Н. Горбанева, А.В. Познякевич // Информационно-технологический вестник. – 2018. – №. 2 (16). – С. 78–85.

3. Исследования. Аналитики Infowatch Technologies [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/analitika/ (дата обращения 22.04.2023).

4. Исследования. Аналитики Kaspersky [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/about/press-releases (дата обращения 22.04.2023).

1. Дроботун, Е.Б. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя / Е.Б. Дроботун, О.В. Цветков // Программные продукты и системы. – 2016. – №. 3 (115). – С. 42–50.

Статья поступила в редакцию 25.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Грибачев К. К. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Ковалев М. В. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Грибачев К. К. – сбор и обработка материала, написание статьи (80 %).
Ковалев М. В. – научное редактирование текста (20 %).

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Международный опыт регулирования обработки персональных данных и его применимость в Российской Федерации

Кирилл Константинович Грибачев[1]✉, Кирилл Андреевич Седаков[2], Дмитрий Олегович Ермаков[3]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1] zorgemauh@gmail.com✉, https://orcid.org/0009-0004-9548-135X
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624
[3] nauchnajarota@yandex.ru, https://orcid.org/0009-0007-5540-2719

Аннотация. Регулирование обработки персональных данных является одним из ключевых направлений обеспечения информационной безопасности как отдельных граждан, так и организаций в целом. Целью данной статьи является анализ международного опыта регулирования обработки персональных данных и определение перспектив его применения в Российской Федерации.

Ключевые слова: обработка персональных данных, защита персональных данных, минимизация сбора данных, обеспечение точности и безопасности данных, гарантии прав субъектов персональных данных.

Для цитирования: Грибачев К. К., Седаков К. А., Ермаков Д. О. Международный опыт регулирования обработки персональных данных и его применимость в Российской Федерации // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 66–69.

Одним из основных международных документов, регулирующих обработку персональных данных, является Директива Европейского Союза 95/46/EC, которая устанавливает общие принципы защиты персональных данных и свободы их перемещения в Европейском Союзе [3.1]. В 2018 году ее сменил «Общий регламент по защите данных» (GDPR), который усилил требования к обработке персональных данных и ввел более строгие санкции за их нарушение. В США защита персональных данных регулируется секторальными законами, такими как «Закон о защите конфиденциальности детей в Интернете» (COPPA), «Закон о конфиденциальности здравоохранения и ответственности» (HIPAA) и «Закон о приватности финансовой информации» Грэмма-Лича-Блайли (GLBA). Кроме того, в США существует Федеральная торговая комиссия (FTC), которая занимается защитой прав потребителей, включая защиту персональных данных.

В странах Азии также существует ряд законов и нормативных актов, регулирующих обработку персональных данных. Например, в Японии действует «Закон о защите персональной информации» (APPI), а в Республике Корея — «Закон о защите персональных данных» (PIPA). Лучшие практики в области регулирования обработки персональных данных включают в себя принципы согласия на обработку данных, минимизации сбора данных, обеспечения точности и безопасности данных, а также гарантии прав субъектов персональных данных на доступ, исправление и удаление своих данных [3.2].

В Российской Федерации основным нормативным актом, регулирующим обработку персональных данных, является Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. Он устанавливает общие принципы и требования к обработке персональных данных, включая согласие субъектов персональных данных на их обработку, ограничения на перечень лиц, имеющих право обрабатывать персональные данные, и требования к обеспечению безопасности персональных данных.

Однако российское законодательство в сфере защиты персональных данных имеет ряд проблем и недостатков. Одной из основных проблем является отсутствие четких критериев оценки законности обработки персональных данных, что затрудняет ее эффективное регулирование. Кроме того, в российском законодательстве отсутствует явное разграничение полномочий между федеральными органами исполнительной власти, ответственными за защиту персональных данных, что также осложняет эффективное регулирование в этой сфере [3.3].

Несмотря на то, что российское законодательство в целом соответствует международным стандартам, его эффективность в сфере защиты персональных данных остается под вопросом. Это связано с рядом конкретных факторов:

1. Отсутствие четких критериев оценки законности обработки персональных данных: В российском законодательстве отсутствуют ясные критерии, позволяющие определить, соответствует ли обработка персональных данных требованиям закона. Это затрудняет как саморегулирование организаций, так и контроль со стороны государства.
2. Недостаточная прозрачность деятельности федеральных органов исполнительной власти, ответственных за защиту персональных данных: Федеральные органы исполнительной власти, ответственные за защиту персональных данных, не всегда обеспечивают достаточную прозрачность своей деятельности. Это затрудняет контроль со стороны граждан и общественности и осложняет взаимодействие организаций с государственными органами в сфере защиты персональных данных.
3. Низкий уровень осведомленности граждан о своих правах в сфере защиты персональных данных: Многие граждане России недостаточно информированы о своих правах в сфере защиты персональных данных. Это затрудняет реализацию этих прав и способствует нарушениям в обработке персональных данных [4].

Для повышения эффективности российского законодательства в сфере защиты персональных данных необходимо учитывать международный опыт и лучшие практики. Ниже приведены конкретные предложения по совершенствованию российского законодательства на основе международного опыта, с учетом статистических данных, таким образом, для повышения:

1. Внедрение офицера по защите данных (DPO): В ЕС и США организации должны иметь DPO для соблюдения GDPR. Согласно отчету Европейской комиссии, введение института DPO способствовало повышению уровня соблюдения требований GDPR на 25 %. В России также есть DPO, но его внедрение не обязательно. Рекомендуется сделать DPO обязательным для всех организаций, обрабатывающих персональные данные, для повышения защиты данных.
2. Уточнение критериев законности обработки данных: В ЕС и США есть четкие критерии для определения законности обработки данных. В России их нет, что затрудняет саморегулирование и контроль. Необходимо уточнить критерии, используя международный опыт.
3. Прозрачность федеральных органов в ЕС и США выше, чем в России. Например, в Европейском союзе и США федеральные органы регулярно публикуют отчеты о проведенных проверках и статистические данные о нарушениях прав субъектов персональных данных. В России такой доступ к информации остается недостаточным. Улучшение доступа к информации и прозрачность деятельности станут ключевыми факторами для повышения доверия к системе защиты персональных данных.
4. Информирование о нарушениях безопасности данных: В ЕС и США требования к информированию субъектов персональных данных строгие и направлены на защиту их интересов. Российское законодательство должно выработать аналогичные стандарты на основе международного опыта.
5. Повышение уровня осведомленности граждан о своих правах в сфере защиты персональных данных: В странах Европейского союза и США проводится активная работа по повышению уровня осведомленности граждан о своих правах в сфере защиты персональных данных. В России также проводится работа по повышению уровня осведомленности граждан, однако ее эффективность остается недостаточной. Согласно исследованию, проведенному компанией «РосБизнесКонсалтинг» в 2022 году, только 29 % россиян знают о своих правах в сфере защиты персональных данных.

Несмотря на то, что российское законодательство в целом соответствует международным стандартам в сфере защиты персональных данных, его эффективность остается под вопросом из-за ряда проблем и недостатков, таких как отсутствие четких критериев оценки законности обработки персональных данных, недостаточная прозрачность деятельности федеральных органов исполнительной власти, ответственных за защиту персональных данных, и низкий уровень осведомленности граждан о своих правах в этой сфере. Для повышения эффективности российского законодательства необходимо учитывать международный опыт и лучшие практики, включая внедрение офицера по защите

данных (DPO), уточнение критериев законности обработки данных, повышение прозрачности деятельности федеральных органов, введение строгих требований к информированию субъектов персональных данных о нарушениях безопасности их данных и повышение уровня осведомленности граждан о своих правах в сфере защиты персональных данных. Учитывая статистические данные и международный опыт, эти меры могут значительно улучшить ситуацию с защитой персональных данных в России.

Список источников

1. Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационноправовой портал «ГАРАНТ.РУ»: http://base.garant.ru/2569783/ (дата обращения 22.04.2023).

2. Гундаров А.В., Колесова Т.С., Максименко А.В. Международный опыт организации информационно-аналитической деятельности в правоохранительной системе // ЮристъПравоведъ. 2017. № 1 (80). С. 163–168.

3. 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 (дата обращения 22.04.2023).

4. Борисова С.А. Общие требования при обработке персональных данных работника и гарантии их защиты // Трудовое право. 2015. № 5. С. 35–39.

Статья поступила в редакцию 25.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Грибачев К. К. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Ермаков Д. О. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Грибачев К. К. – сбор и обработка материала, частичное написание статьи (70 %).

Седаков К. А. – научное редактирование текста (20 %).

Ермаков Д. О. – обработка материала, частичное написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Киберполигоны как новый вид заработка для ИТ-компаний

Егор Павлович Горбачев[1]✉, Елизавета Андреевна Музалевская[2], Анна Николаевна Вишнякова[3], Оксана Михайловна Голембиовская[4]
[1] Финансовый университет при Правительстве Российской Федерации, Москва, Россия
[2, 3, 4] Брянский государственный технический университет, Брянск, Россия
[1] me@septembernocturne.ru✉
[2] lizamuz2002@yandex.ru
[3] vshnv.a@yandex.ru
[4] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133

Аннотация. В современном мире, охваченном цифровыми технологиями, кибербезопасность становится одним из приоритетных направлений для организаций любого масштаба. В этой статье рассмотрена концепция киберполигонов как инновационного инструмента для обучения специалистов в области кибербезопасности и их потенциала как нового источника заработка для ИТ-компаний.

Ключевые слова: ИТ-компании, киберполигоны, информационная безопасность.

Для цитирования: Горбачев Е. П., Музалевская Е. А., Вишнякова А. Н., Голембиовская О. М. Киберполигоны как новый вид заработка для ИТ-компаний // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 70–72.

С развитием информационных технологий и увеличением числа киберугроз, ИТ-компании сталкиваются с необходимостью постоянного обучения своих специалистов в области кибербезопасности. Кроме того, они сталкиваются с растущим спросом на квалифицированных экспертов по информационной безопасности со стороны других организаций. Каким образом киберполигоны могут удовлетворить эти потребности и стать новым источником заработка для ИТ-компаний — это основной вопрос, который мы рассмотрим в данной статье.

Киберполигоны — это специализированные площадки, на которых проводятся тренировочные симуляции кибератак и киберзащиты. Их особенность заключается в том, что они предоставляют возможность специалистам получить практические навыки в области кибербезопасности, моделируя реальные сценарии атак и разрабатывая меры по их предотвращению [1]. Такие тренировки помогают повысить уровень киберстойкости компаний и подготовить специалистов к действию в случае реальной киберугрозы.

Основным принципом работы киберполигонов является создание условий для проверки защищенности информационной инфраструктуры компаний и организаций. Ит-компании могут использовать киберполигоны для обучения своих сотрудников, тестирования новых продуктов и услуг, а также для анализа уровня уязвимости своих систем перед реальными кибератаками [2].

Одним из ключевых преимуществ киберполигонов является возможность проведения практических тренировок без риска для бизнеса и безопасности организации. Кроме того, киберполигоны позволяют выявить слабые места в системах безопасности и принять меры по их устранению [3].

ИТ-компании могут использовать киберполигоны как инструмент для обучения своих сотрудников и повышения их квалификации в области кибербезопасности. Они также могут предлагать услуги обучения и тренировок для других компаний, как с целью заработка, так и с целью повышения уровня кибербезопасности в целом. Растущий спрос на услуги киберполигонов открывает перед ИТ-компаниями новые возможности для создания дополнительного источника дохода.

Исследования показывают, что использование киберполигонов в обучении персонала способствует более эффективному усвоению материала и повышает уровень подготовки специалистов по информационной безопасности. Это делает киберполигоны все более востребованным инструментом не только для обучения, но и для тестирования и повышения профессиональных навыков в данной области.

Важно отметить, что киберполигоны могут быть использованы не только IT-компаниями, но и государственными структурами, банковскими учреждениями, телекоммуникационными компаниями и другими организациями, работающими с ценной информацией.

Киберполигоны представляют собой перспективное направление в области обучения и повышения квалификации специалистов по кибербезопасности. Их эффективное использование позволяет ИТ-компаниям не только обеспечить безопасность своей информации, но и успешно конкурировать на рынке информационной безопасности, предлагая качественные обучающие услуги. Таким образом, киберполигоны действительно могут стать новым видом заработка для ИТ-компаний, принесших им не только дополнительную прибыль, но и повышение репутации и уровня кибербезопасности клиентов.

Список источников

1. Киберполигон // cyberpoly URL: https://cyberpoly.ru/ (дата обращения: 25.04.2024).

2. КИБЕРПОЛИГОН - SOLAR CYBERMIR // SOLAR URL: https://cybermir.ru/ (дата обращения: 25.04.2024).

3. Роль киберполигона в обеспечении ИБ // Security Vision URL: https://www.securityvision.ru/blog/rol-kiberpoligona-v-obespechenii-ib/ (дата обращения: 25.04.2024).

Статья поступила в редакцию 02.05.2024; принята к публикации 15.05.2024.

Информация об авторах

Горбачев Е. П. – студент факультета экономики и бизнеса, направление подготовки 38.03.01 – Экономика, профиль «Корпоративные финансы», ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации».

Музалевская Е. А. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Вишнякова А. Н. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Горбачев Е. П. – обработка материала, написание статьи (35 %).
Музалевская Е. А. – сбор материала, частичное написание статьи (30 %).
Вишнякова А. Н. – сбор материала, частичное написание статьи (25 %).
Голембиовская О. М. – идея, научное редактирование (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Этапы прогнозирования ущерба от реализации самых известных угроз

Егор Павлович Горбачев[1]✉, Елизавета Андреевна Музалевская[2], Максим Михайлович Голембиовский[3], Кирилл Евгеньевич Шинаков[4]
[1] Финансовый университет при Правительстве Российской Федерации, Москва, Россия
[2, 3, 4] Брянский государственный технический университет, Брянск, Россия
[1] me@septembernocturne.ru✉
[2] lizamuz2002@yandex.ru
[3] maksim32region@yandex.ru
[4] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. В условиях постоянно изменяющихся киберугроз и развития технологий в сфере информационной безопасности важно иметь возможность прогнозировать потенциальный ущерб, который может быть причинен при реализации самых известных угроз. В данной статье рассматриваются этапы прогнозирования ущерба от кибератак, основные методы анализа и оценки угроз, а также методы предотвращения возможного ущерба.

Ключевые слова: информационная безопасность, реализация угроз, прогнозирование ущерба.

Для цитирования: Горбачев Е. П., Музалевская Е. А., Голембиовский М. М., Шинаков К. Е. Этапы прогнозирования ущерба от реализации самых известных угроз // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 73–75.

Современные информационные системы сталкиваются с разнообразными угрозами, которые могут привести к серьезным последствиям для организаций и государств. Поэтому важно иметь систему прогнозирования ущерба от возможных кибератак. Прогнозирование ущерба позволяет принять меры по обеспечению безопасности информационных систем заранее и минимизировать возможные убытки.

Этапы прогнозирования ущерба:

1. Анализ угроз:

- Идентификация угроз: На этом этапе идентифицируются различные типы угроз, которые могут оказать воздействие на информационную систему. Это могут быть кибератаки, вирусы, физические угрозы и другие.

- Оценка уязвимостей: Проводится анализ уязвимостей информационной системы, которые могут быть использованы злоумышленниками для совершения атак.

2. Оценка ущерба:

- Финансовый ущерб: Оценивается потенциальный финансовый ущерб, который может быть причинен в результате успешной кибератаки. Это включает утрату доходов, затраты на восстановление системы, штрафы и компенсации.

- Нематериальный ущерб: Кроме финансового ущерба, также оценивается возможный негативный имидж компании, потеря доверия клиентов, снижение репутации и другие нематериальные последствия.

3. Предотвращение ущерба:

- Разработка мер безопасности: На основе выявленных угроз и потенциального ущерба разрабатываются меры по обеспечению безопасности информационной системы. Это включает в себя установку антивирусного ПО, брандмауэров, многофакторной аутентификации и других технических средств защиты.

- Обучение персонала: Проводятся тренинги и обучение персонала по правилам безопасности, а также осведомляются о текущих угрозах и способах защиты.

- Разработка планов реагирования: Создаются планы реагирования на инциденты, включая шаги по быстрому восстановлению системы и меры по минимизации ущерба.

Основные методы анализа и оценки угрозы, а также методы предотвращения возможного ущерба включают в себя следующие подходы:

1. Методы анализа и оценки угрозы:

- Метод деревьев атак: Этот метод заключается в разработке модели атаки, позволяющей идентифицировать возможные уязвимости и пути проникновения злоумышленников в информационную систему.

- Метод вероятностной оценки: Позволяет оценить вероятность возникновения угрозы и ее возможные последствия. Это помогает определить приоритетность рисков и уделить внимание наиболее значимым угрозам.

- Метод SWOT-анализа: Позволяет выявить сильные и слабые стороны системы в контексте возможных угроз, а также определить возможности для улучшения защиты и управления рисками.

2. Методы предотвращения ущерба:

- Разработка политики безопасности: Создание и внедрение политики безопасности информационной системы, включающей в себя правила доступа, шифрование данных, регулярное обновление ПО и другие меры.

- Регулярное обновление системы: Важно поддерживать систему в актуальном состоянии, устанавливая исправления безопасности, обновления и патчи для устранения известных уязвимостей.

- Многоуровневая защита: Использование комплексной системы защиты, включая фаерволы, антивирусное ПО, системы мониторинга и детекции угроз, чтобы создать "оборонительный зонтик" от различных типов атак.

Прогнозирование ущерба от реализации угроз — важный инструмент для обеспечения безопасности информационных систем. Правильное проведение

этапов анализа, оценки и предотвращения ущерба позволяет эффективно реагировать на угрозы и минимизировать возможные риски. В современном мире обеспечение кибербезопасности становится все более актуальным, поэтому методы прогнозирования ущерба играют важную роль в обеспечении стабильности информационных систем.

Список источников

1. Анализ угроз информационной безопасности // SEARCHINFORM URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/analiz-ugroz-informatsionnoj-bezopasnosti/ (дата обращения: 25.04.2024).

2. Планирование затрат на информационную безопасность // Anti-Malware URL: https://www.anti-malware.ru/analytics/Technology_Analysis/economic_planning (дата обращения: 25.04.2024).

3. Оценка информационной безопасности бизнеса // Корпоративный менеджмент URL: https://www.cfin.ru/appraisal/business/special/infosec.shtml (дата обращения: 25.04.2024).

Статья поступила в редакцию 02.05.2024; принята к публикации 15.05.2024.

Информация об авторах

Горбачев Е. П. – студент факультета экономики и бизнеса, направление подготовки 38.03.01 – Экономика, профиль «Корпоративные финансы», ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации».

Музалевская Е. А. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности», ФГБОУ ВО «БГТУ».

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

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Горбачев Е. П. – обработка материала, написание статьи (35 %).

Музалевская Е. А. – сбор материала, частичное написание статьи (30 %).

Голембиовский М. М. – сбор материала, частичное написание статьи (15 %).

Шинаков К. Е. – идея, научное редактирование (20 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Основы бизнес-планирования расходов компании на обеспечение информационной безопасности

Егор Павлович Горбачев[1]✉, Елизавета Андреевна Музалевская[2], Станислав Владимирович Сафоненко[3], Кирилл Евгеньевич Шинаков[4]
[1] Финансовый университет при Правительстве Российской Федерации, Москва, Россия
[2, 3, 4] Брянский государственный технический университет, Брянск, Россия
[1] me@septembernocturne.ru✉
[2] lizamuz2002@yandex.ru
[3] ssafonenko691@yandex.ru
[4] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. В настоящей статье рассматриваются основные аспекты планирования расходов компании на обеспечение информационной безопасности. Проанализированы методы анализа угрозы, оценки рисков и предотвращения возможного ущерба. Представлены стратегии и рекомендации по эффективному управлению информационной безопасностью в современной корпоративной среде.

Ключевые слова: информационная безопасность, бизнес-планирование, планирование расходов.

Для цитирования: Горбачев Е. П., Музалевская Е. А., Сафоненко С. В., Шинаков К. Е. Основы бизнес-планирования расходов компании на обеспечение информационной безопасности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 76–78.

Информационная безопасность является одним из ключевых аспектов деятельности любой компании в условиях современного цифрового мира. Правильное бизнес-планирование расходов на обеспечение ИБ играет решающую роль в защите конфиденциальности, целостности и доступности данных компании. В данной статье рассматриваются основные этапы и методы данного процесса.

Бизнес-планирование расходов компании на обеспечение информационной безопасности (ИБ) играет ключевую роль в современной бизнес-среде, где цифровые угрозы становятся все более сложными и разнообразными.

Для успешного планирования расходов на обеспечение ИБ необходимо учитывать несколько важных аспектов:

1. Анализ угроз и рисков:

- Начинать необходимо с оценки уровня угроз для вашей компании. Идентифицировать потенциальные уязвимости и угрозы, с которыми компания может столкнуться.

- Проводить анализ вероятности возникновения различных угроз и потенциального ущерба, который они могут причинить.

2. Установление бюджета на ИБ:

- Разработать бюджет на информационную безопасность, который будет соответствовать уровню риска и потенциальным угрозам.

- Учесть расходы на обновление программного обеспечения, закупку оборудования, обучение сотрудников и другие меры по обеспечению ИБ.

3. Выбор приоритетов и стратегий защиты:

- Определить приоритетные направления в области информационной безопасности и основные задачи, на которые будет направлен ваш бюджет.

- Разработать стратегии защиты данных, включая политики безопасности, меры по предотвращению инцидентов, резервное копирование и мониторинг систем безопасности.

4. Внедрение и мониторинг:

- Реализовать запланированные меры по обеспечению информационной безопасности и обеспечить их надлежащее функционирование.

- Установить систему мониторинга и аудита, чтобы следить за изменениями в уровне безопасности и оперативно реагировать на угрозы.

Бизнес-планирование расходов на обеспечение ИБ является неотъемлемой частью управления рисками и обеспечения безопасности в современном бизнесе. Вложения в информационную безопасность помогут компании минимизировать потенциальные угрозы и обеспечить сохранность важных данных и репутации предприятия.

Интеграция процессов управления рисками, бизнес-планирования расходов и стратегий по обеспечению ИБ позволяет компаниям эффективно справляться с современными угрозами информационной безопасности и обеспечивать устойчивое развитие бизнеса в цифровой среде.

Такая структура статьи позволит рассмотреть все релевантные аспекты бизнес-планирования расходов на обеспечение информационной безопасности и предоставить читателям полезную информацию о методах и стратегиях этого важного процесса.

Список источников

1. Планирование затрат на информационную безопасность // Anti-Malware URL: https://www.anti-malware.ru/analytics/Technology_Analysis/economic_planning (дата обращения: 25.04.2024).

2. Оценка информационной безопасности бизнеса // Корпоративный менеджмент URL: https://www.cfin.ru/appraisal/business/special/infosec.shtml (дата обращения: 25.04.2024).

3. Сколько стоит информационная безопасность // positive technologies URL: https://www.ptsecurity.com/ru-ru/research/analytics/is-cost-2017/ (дата обращения: 25.04.2024).

Статья поступила в редакцию 02.05.2024; принята к публикации 15.05.2024.

Информация об авторах

Горбачев Е. П. – студент факультета экономики и бизнеса, направление подготовки 38.03.01 – Экономика, профиль «Корпоративные финансы», ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации».

Музалевская Е. А. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Сафоненко С. В. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Горбачев Е. П. – обработка материала, написание статьи (35 %).
Музалевская Е. А. – сбор материала, частичное написание статьи (30 %).
Сафоненко С. В. – сбор материала, частичное написание статьи (25 %).
Шинаков К. Е. – идея, научное редактирование (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.5

Особенности защиты центров обработки данных от физических атак

Максим Леонидович Гулак✉
Брянский государственный технический университет, Брянск, Россия
gml13@yandex.ru✉, http://orcid.org/0009-0009-3131-4292

Аннотация. Рассмотрены проблемы физических атак на центры обработки данных и серверные помещения, а также проведен анализ способов противодействия таким атакам.

***Ключевые слова*:** физическая безопасность, информационная безопасность, центр обработки данных, защита ЦОД, защита серверных, «красная команда».

Для цитирования: Гулак М. Л. Особенности защиты центров обработки данных от физических атак // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 79–83.

Обеспечение безопасности данных — одна из основных задач, стоящих перед любым юридическим лицом, являющимся владельцем центра обработки данных (ЦОД). Центр обработки данных, по сути, представляет собой банк данных колоссальной емкости, в котором хранятся и обрабатываются сведения самой разной направленности. На обеспечение требуемого нормативными актами регулятора уровня защищенности как самих данных в ЦОД, так и доступа к хранящимся данным могут затрачиваться десятки миллионов рублей. Должна использоваться цельная система защитных средств и механизмов различного назначения. Например, для защиты системы ЦОД от проникновения извне применяют межсетевые экраны, системы обнаружения вторжений, шлюзы VPN, для того, чтобы сгладить и локализовать последствия от произошедших инцидентов и сбоев выполняются резервирование и кластеризация, устанавливаются резервные источники бесперебойного питания, применяются различные меры, направленные на повышение надежности и постоянной готовности.

Один из менеджеров по продукции для IT-инфраструктуры компании Rittal А. Нилов сказал: «В России научились строить ЦОД с защищенными сетями и высоконадежным оборудованием, но недооценивают физические риски». И действительно, именно деятельность по защите ЦОД от физических атак до настоящего времени является той областью, которой уделяют незаслуженно мало внимания.

Для обеспечения физической безопасности центров обработки данных можно сформулировать несколько задач. Первая и традиционно основная зада-

ча обеспечения физической безопасности ЦОД носит превентивный характер и заключается в предотвращении проникновения посторонних в защищаемые помещения. Вторая задача решается в случае, если несанкционированное проникновение произошло, и заключается в как можно более быстрой идентификации злоумышленников. Решение третьей задачи призвано обеспечить полную защиту оборудования ЦОД от негативного или вредного воздействия различных природных и техногенных факторов. Для того, чтобы центр обработки данных был защищен в соответствии с требованиями нормативных актов, решать поставленные задачи необходимо заранее, задолго не только до запуска ЦОД в работу, но и до его организации.

Как указывалось выше, для обеспечения требуемой защищенности, в том числе и от нанесения физического воздействия, требуется применение сбалансированной многоуровневой системы обеспечения безопасности, включающей в себя и компоненты физической защиты ЦОД. При этом должна быть реализована и внедрена система защиты, предполагающая наличие нескольких периметров безопасности (внешних и внутренних) с расчетом на то, что в случае преодоления злоумышленником одного периметра безопасности, остальные останутся в неприкосновенности и система безопасности в целом продолжит функционировать.

В данной статье рассмотрим проблему физических атак на центры обработки данных и серверные помещения, а также проанализируем способы противодействия таким атакам.

Физическая безопасность ЦОД, как структурная составляющая системы защиты от информационных угроз, имеет много различных аспектов. Сведя воедино все меры и требования, включая защиту от вредных примесей и пыли, пожаров, контроль прохода сотрудников и т.д., то получим весьма длинный список мер:

- грамотное планирование местоположения ЦОД;
- управление периметром;
- использование списка сотрудников для авторизованного доступа;
- контроль доступа в здание и к оборудованию;
- реагирование на инциденты и чрезвычайные ситуации;
- RFID-инвентаризация оборудования;
- соответствие стандарту ГОСТ Р ИСО/МЭК 27000-2021 «Системы менеджмента информационной безопасности»;
- резервирование ресурсов;
- применение систем сигнализации и видеонаблюдения и др.

Однако, если не учитывать изъяны и недостатки инфраструктуре центра обработки данных, создающие возможность незаконного проникновения внутрь помещения, например, серверной, то несмотря на истраченные на обеспечение физической безопасности сотни тысяч рублей, будет велик риск НСД или других инцидентов. Для выявления и фиксации таких изъянов и недостатков системы защиты могут быть приглашены группы профильных специалистов, квалификация и компетентность которых позволяет оценить возможную

эффективность применения злоумышленниками различных методик, направленных на получение несанкционированного доступа в защищённые помещения, в том числе и методов социальной инженерии. Эти группы экспертов получили название «красные команды».

Такие команды при проведении проверки могут использовать не только общепринятые, но и собственные приёмы, перечень и суть которых стараются не разглашать и не афишировать для сохранения фактора неожиданности для потенциальных злоумышленников.

Однако, разработчики и проектировщики ЦОД в профилактических целях должны выполнять определенные действия и применять «профилактические заготовки» для предотвращения возникновения инцидентов безопасности и следующих за ними проблем.

Особое внимание при проектировании ЦОД или серверной следует обратить на выбор проекта прокладки коммуникаций в ЦОД с учётом выделения мест для размещения вспомогательного оборудования и средств связи. Если проектированием занимается опытная команда, она обязательно уделит внимание некоторым неявным аспектам.

1. Из-за повсеместно применяемых фальшполов и подвесных потолков реальные нижние и верхние границы помещения не совпадают с фактическим полом или потолком, что вполне могут использовать злоумышленники, сняв, например, потолочную плитку в соседней комнате и пробравшись в защищённое помещение с установленным оборудованием ЦОД или серверную, воспользовавшись имеющимся свободным пространством между потолком или полом и фальшстеной или вентиляционными отверстиями.

Типичной защитой от подобных происшествий является установка внутри таких проходов различных препятствий, снятие или деформирование которых будет обязательно замечено. В качестве таких препятствий в проходах можно смонтировать проволочную сетку или съёмные металлические ограждения. На случай, если злоумышленник для проникновения в защищаемое помещение перережет проволоку, для защиты от подобных инцидентов желательно установить дополнительные датчики сигнализации. Не рекомендуется использовать для создания препятствий мягкие материалы, например, гипсокартон. Они будут лишь создавать иллюзию защищённости, но обеспечить полноценную безопасность не смогут.

Также необходимо держать в тайне детальный план технических проходов.

2. Вскрытие дверного замка на входе в здание или помещение — один из наиболее очевидных и распространённых приемов проникновения. Не сильно улучшает ситуацию установка кодовых замков.

Скрытая установка злоумышленником беспроводной камеры может позволить злоумышленнику преодолеть такое препятствие. Камерами могут воспользоваться и «красные команды» для изучения степени защищённости помещения. С помощью видеокамеры злоумышленник или «красная команда» могут подсмотреть код, который набирают при входе в серверную.

Рекомендуется использовать исключительно электронные замки, которые можно открыть по биометрии или с помощью смарт-карты. Они способны обеспечить более высокий уровень защищённости. Следует учитывать, что даже электронные замки не могут в полной мере обеспечить защиту системы и данных ЦОД, поскольку существует аппаратное и программное обеспечение, позволяющие считывать со смарт-карты входной код.

3. Наличие запасного или служебного входа часто является обязательным условием, однако, с точки зрения защищенности помещений, это – скрытая опасность несанкционированного проникновения. Практика показывает, что проникнуть внутрь помещения через запасной или служебный вход бывает обычно намного проще, чем через охраняемый основной.

По статистике, излюбленными приемами незаконного проникновения в здание через служебный вход являются представиться монтажником или настройщиком оборудования, разносчиком пиццы или грузчиком.

Один из способов снижения рисков — установка даже на запасном и служебном проходе турникета, через который единовременно может пройти лишь один человек. Желательно также наличие охранника, который будет следить, чтобы у проходящих людей были при себе бейджи или иные отличительные признаки.

4. Когда все остальные приёмы не позволили злоумышленнику проникнуть в здание он может воспользоваться методами социальной инженерии, которая срабатывает почти всегда.

С рисками компрометации с использованием методов социальной инженерии следует бороться, обучая сотрудников ИБ-грамотности.

В статье рассмотрены лишь наиболее очевидные способы несанкционированного проникновения в центры обработки данных и обеспечения физической защищённости ЦОД и серверных и ее проверки. Задача обеспечения безопасности — это задача комплексная. Инциденты, связанные со взломом с применением грубой силы, случаются достаточно редко, но к ним надо быть готовыми.

Список источников

1. 187-ФЗ: практические рекомендации при выполнении. – Режим доступа: ttps://www.anti-malware.ru/practice/methods/187-recommendations-for-implementing-the-law.

2. Угрозы информационной безопасности. – Режим доступа: https://www.anti-malware.ru/threats/information-security-threats.

3. Защита центров обработки данных (ЦОД). – Режим доступа: https://www.anti-malware.ru/security/protection-data-processing-centers.

4. Реализация мер физической безопасности на стороне Selectel. – Режим доступа: https://docs.selectel.ru/servers-and-infrastructure/certified-data-center-segment/about/implemented-security-measures/?ysclid=lssqhtldax214788882.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторе

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

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Анализ возможностей нарушения неприкосновенности частной жизни за счёт утечки информации с устройств дополненной реальности

Диана Игоревна Денисеня[1]✉, Дмитрий Андреевич Лысов[2]✉, Юрий Юрьевич Громов[3]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1] d.diana1519@gmail.com✉, https://orcid.org/0009-0004-6440-7632
[2] lysovdmitriia@gmail.com✉, https://orcid.org/0009-0003-9666-7191
[3] nauchnajarota@yandex.ru

Аннотация. В данной статье рассмотрена возможности утечки личных данных с устройств дополненной реальности, при помощи взлома.

Ключевые слова: устройства дополненной реальности, Apple Vision Pro, конфиденциальность, защита персональных данных.

Для цитирования: Денисеня Д. И., Лысов Д. А., Громов Ю. Ю. Анализ возможностей нарушения неприкосновенности частной жизни за счёт утечки информации с устройств дополненной реальности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 84–87.

В наше время технологии дополненной реальности становятся все более популярными и распространёнными. Они предлагают уникальные возможности не только в областях развлечения, но и в областях профессионального применения. Однако, вместе с расширением функциональности устройств дополненной реальности, возрастает и риск нарушения приватности и утечки личных данных пользователей.

Выбирая устройство, которому мы доверим множество своих персональных данных, важно понять, каким образом взламываются системы, и какие компании подвергаются этому реже всего. Злоумышленники пользуются разными способами узнавания персональных данных пользователей, например методы обмана, использование уязвимостей серверов или применение шпионского ПО, которое может собирать данные о пользователе или устройстве непосредственно с хост-компьютера.

Компания Apple прикладывает много сил к защите личных данных пользователей. Поддержка моментально реагирует на неполадки и взломы. Но даже у такой большой корпорации были случаи глобальных утечек данных. Послед-

ний масштабный взлом Apple произошёл в 2021 году с помощью шпионского ПО «Pegasus». Тогда хакеры, выдающие себя за сотрудников правоохранительных органов, используя взломанные адреса почт, отправили запрос на разрешение использования личных данных пользователей. Сотрудники компании сообщили, что учётные записи были законны, но скомпрометированы злоумышленником [1].

В ходе данного взлома использовалось множество методов, таких как «Фишинг» [2], вредоносное ПО, социальная инженерия (психологические манипуляции и давление) и так далее. Каждый из методов имеет особую частоту применения (рис. 1).

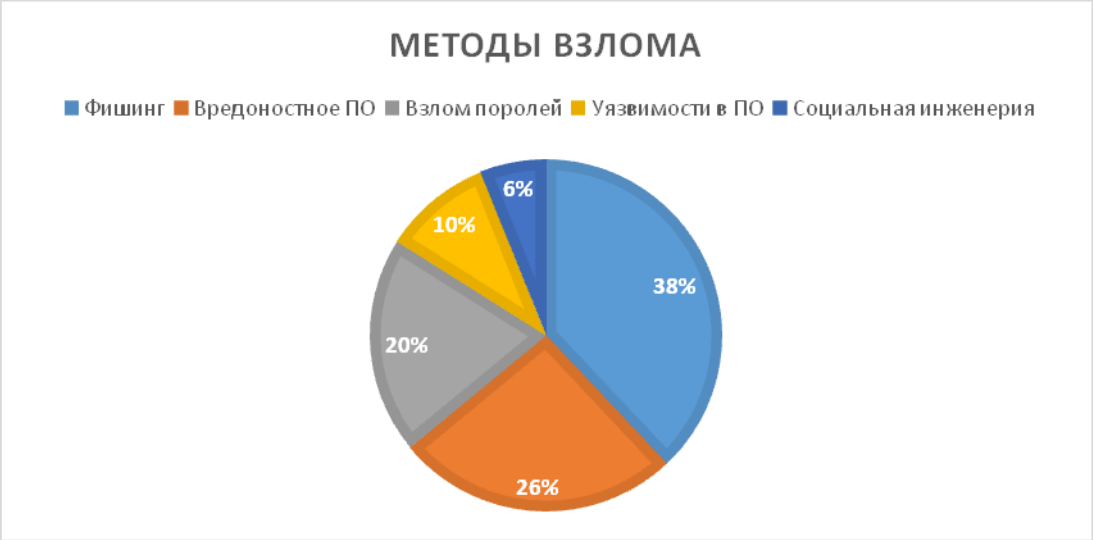


Рис. 1. Методы взлома

Необходимо понимать, что при потере персональных данных, идентификация преступника очень мала, поскольку правоохранительные органы не обладают достаточными техническими средствами для определения личности правонарушителя [4]. Вдобавок к этому, применение государственных санкций в случае утечки данных трудноосуществимо, так как возникает проблема в доказательстве правонарушения.

В связи с вышесказанным, количество преступлений, связанные с хищением личных данных, растёт. И несмотря на то, что компании постоянно борются с проблемами подобного рода, пользователи также должны заботиться о сохранности своих данных.

После выхода очков смешанной реальности Apple Vision Pro, сеть заполонили ролики, на которых видно, что люди используют устройство как дома, так и на улице.

Несомненно, пользователь устройства подобного рода вводит пороли и PIN-коды для разных задач. Из-за того, что датчики отслеживают движение рук, взломщик может абсолютно точно повторить PIN-код пользователя [6]. Вдобавок к этому, гарнитуры смешанной реальности могут включать отслеживание взгляда, что также может использоваться злоумышленниками.

Взлом такого масштабного ПО может представлять настоящую киберугрозу. В таком случае, чтобы увеличить защищённость своих устройств, необходимо придерживаться следующих правил:

1. Поддерживайте актуальность прошивки (обновления помогают избавиться от уязвимости в системе).
2. Используйте VPN (он защищает интернет-соединение, а изменённый IP-адрес позволяет сохранить конфиденциальность личности и данных).
3. Изучайте политику конфиденциальности (вы будете знать, в каком случае будут распространяться ваши данные, где они хранятся и кто имеет к ним доступ).
4. Ограничьте доступ к вашим данным.
5. Используйте WPA3 для защиты соединения (WPA3 является новым стандартом безопасности Wi-Fi сетей, который поддерживает ряд функций, направленных на защиту [3]).
6. Отключайте Bluetooth, когда не используете устройство смешанной реальности.
7. Проверьте настройки конфиденциальности (тогда вы убедитесь, что настройка устройства соответствует вашим требованиям).

Всегда будьте бдительны и обращайте внимание на любые подозрительные действия.

Список источников

1. Apple и Meta [Электронный ресурс] URL: https://appleinsider.ru/sudy-i-skandaly/apple-i-meta-po-oshibke-slili-dannye-xakeram-ix-obmanuli-kak-detej.html (дата обращения: 24.03.2024).
2. What is phishing? Examples, types, and techniques [Электронный ресурс] URL: https://www.csoonline.com/article/514515/what-is-phishing-examples-types-and-techniques.html (дата обращения: 20.04.2024).
3. Wi-Fi Alliance introduces Wi-Fi CERTIFIED WPA3 security [Электронный ресурс] URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security (дата обращения: 09.04.2024).
4. Иванова А.П. Утечка персональных данных: большая проблема в цифровую эпоху // Журнал: Социальные и гуманитарные науки. 2020. —9 с.
5. Новые механизмы защиты беспроводной сети WPA3 и OWE [Электронный ресурс] URL: https://help.keenetic.com/hc/ru/articles/360005697520-Новые-механизмы-защиты-беспроводной-сети-WPA3-и-OWE (дата обращения: 09.04.2024).
6. Риски безопасности и конфиденциальности в виртуальной и дополненной реальности [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/threats/security-and-privacy-risks-of-ar-and-vr (дата обращения: 09.04.2024).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Денисеня Д. И. – студент кафедры «Информатика и программное обеспечение», направление подготовки 09.03.01 – Информатика и вычислительная техника, ФГБОУ ВО «БГТУ».

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

Громов Ю. Ю. – директор института автоматики и информационных технологий ФГБОУ ВО «ТГТУ», кафедра «Информационные системы и защита информации».

Вклад авторов

Денисеня Д. И. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Лысов Д. А. – написание статьи, научное редактирование текста (30 %).

Громов Ю. Ю. – обработка материала, частичное написание статьи (20 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Основные особенности в обеспечении безопасности информации в организациях сферы здравоохранения

Марина Васильевна Дерюгина[1]✉, Кирилл Андреевич Седаков[2], Евгений Юрьевич Негодяев[3], Вячеслав Сергеевич Румянцев[4]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3, 4] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1] marina.deryugina7@gmail.com✉, https://orcid.org/0009-0000-1606-1391
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624
[3, 4] nauchnajarota@yandex.ru, https://orcid.org/0009-0007-5540-2719

Аннотация. Организации сферы здравоохранения в наше время всё чаще и чаще сталкиваются с угрозами информационной безопасности из-за обработки больших объемов информации. Рассматривается проблема информационной безопасности в организациях сферы здравоохранения, а именно: изучаются угрозы, с которыми они сталкиваются, какие атаки могут происходить и их последствия.

Ключевые слова: информационная безопасность, сфера здравоохранения, угрозы безопасности информации.

Для цитирования: Дерюгина М. В., Седаков К. А., Негодяев Е. Ю., Румянцев В. С. Основные особенности в обеспечении безопасности информации в организациях сферы здравоохранения // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 88–91.

С развитием технологий растет спрос на них во всех сферах жизни, включая здравоохранение. Медицинские учреждения переходят на электронную документацию, начинают использовать технологии интернета вещей, также и носимых пациентами, вследствие чего увеличиваются риски безопасности информации. В организациях, которые еще не используют современные технологии, все это происходит в ручном виде, что не исключает человеческий фактор ошибок или недопустимых действий. При этом данные необходимо обрабатывать в оперативном режиме и разные части информации обрабатываются разными людьми.

В медицинских учреждениях в больших объемах обрабатываются персональные данные. Определение персональных данных устанавливается Федеральным законом от 27.07.2006 № 152 «О персональных данных». Персональные данные — это любая информация, относящаяся к прямо или косвенно оп-

ределенному, или определяемому физическому лицу [3]. Эти данные включают в себя общедоступную и специальные категории данных:

- фамилия, имя, отчество;
- дата рождения;
- место проживания;
- история болезни;
- аллергии и хронические заболевания;
- состояние здоровья и т. п.

Также все организации обязаны соблюдать законы и нормативные акты, регулирующие обработку и защиту информации.

Злоумышленники все чаще атакуют медицинские учреждения из-за отсутствия должного уровня защиты и высокой стоимости таких данных. В прошлом году медицинские учреждения стали второй по популярности целью для хакеров, с 11 % успешных вторжений, 96 % из которых были целенаправленными, а 64 % осуществлены при помощи вредоносного ПО [2]. В стране пока нет единой государственной информационной системы в области здравоохранения, но существуют самые распространенные средства — медицинские информационные системы, облачные хранилища, и приложения с локальным или сетевым хранилищем. Однако не все учреждения обладают достаточным уровнем информационной безопасности или ресурсами для обновления систем.

Специфика информации требует более ответственного отношения к обработке, хранению и передаче данных. Последствия реализации атак на медицинские учреждения могут привести к утечке или шифрованию персональных данных пациентов, а далее к возникновению угроз здоровью. Постановка неправильных диагнозов самими врачами из-за утраты данных или предложение медицинских услуг самими злоумышленниками на основе полученной информации. Также потери финансов и репутации, из-за недоверия людей, органов контроля безопасности информации.

Угрозы информационной безопасности в здравоохранении включают в себя различные аспекты, такие как программы-вымогатели, DDoS атаки, фишинг и другие. Многие медицинские учреждения не обеспечивают достаточной защиты из-за отсутствия автоматизированных систем учета и документооборота или использования устаревших средств из-за высокой стоимости обновления и сложности совместимости. По данным «Лаборатории Касперского», 54 % медицинских организаций продолжают использовать устаревшие операционные системы, что существенно повышает уровень уязвимости [1].

Злоумышленники всегда ищут слабые места в системе, и уровень защиты определяется уязвимыми компонентами. Минимальные комплекты безопасности могут приводить к различным уязвимостям, таким как недостаточная архитектура, отсутствие резервного копирования, передача и хранение данных без шифрования, открытые сети или недостаточные права доступа.

Помимо этого, основная проблема заключается не только в недооценке рисков, но и в отсутствии базового обучения персонала правилам работы с конфиденциальной информацией и обеспечению информационной безопасно-

сти, что открывает двери для как преднамеренных, так и случайных внутренних угроз. Решение проблемы требует четкого разграничения доступа к защищаемым данным и системам, внедрения обучающих программ по работе с конфиденциальной информацией и информационной безопасностью для персонала. Внедрение алгоритмов шифрования, средств авторизации, мониторинга, антивирусов, систем предотвращения утечек и обнаружения вторжений, создание резервных копий и постоянное обновление уже установленного программного обеспечения, с учетом специфики данных — это меры необходимые для обеспечения безопасности информации в организации [4].

Таким образом, ознакомившись с информационной безопасностью в медицинских учреждениях, можно сделать вывод о необходимости улучшения уровня защиты данных. Информационная безопасность становится все более актуальной задачей в сфере здравоохранения, требуя комплексного подхода ее обеспечения. Медицинским учреждениям необходимо уделить большее внимание и ресурсы для обеспечения информационной безопасности и защиты персональных данных.

Список источников

1. Kaspersky, российский интернет-портал компании, специализирующаяся на разработке систем защиты информации [Электронный ресурс] – URL: https://www.kaspersky.ru/about/press-releases/2021_laboratoriya-kasperskogo-v-polovine-rossijskih-medicinskih-uchrezhdenij-ispolzuetsya-oborudovanie-c-ustarevshej-os.

2. Positive Technologies, российский интернет-портал компании, специализирующаяся на разработке решений в сфере информационной безопасности [Электронный ресурс] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/.

3. О персональных данных: федеральный закон от 27 июля 2006 г. №152-ФЗ // Собрание законодательства Российской Федерации // [Электронный ресурс] – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.

4. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с. — URL: http://www.iprbookshop.ru/46584530.html;

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Дерюгина М. В. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Негодяев Е. Ю. – старший оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Румянцев В. С. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Дерюгина М. В. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – научное редактирование текста (30 %).

Негодяев Е. Ю. – обработка материала, частичное написание статьи (10 %).

Румянцев В. С. – обработка материала, частичное написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Особенности нормативно-правовой регламентации выбора средств защиты информации для обеспечения безопасности персональных данных в коммерческих организациях

Денис Андреевич Евтихов
Брянский государственный технический университет, Брянск, Россия
ansdean1@gmail.com, https://orcid.org/0009-0002-7105-0745

Аннотация. В статье рассматривается вопрос нормативно-правовой регламентации обеспечения безопасности персональных данных за счет выбора методов и средств защиты информации. Предложен алгоритм выбора методов и средств защиты для обеспечения безопасности персональных данных в коммерческой организации.

Ключевые слова: защита информации, безопасность персональных данных, нормативно-правовые акты.

Для цитирования: Евтихов Д. А. Особенности нормативно-правовой регламентации выбора средств защиты информации для обеспечения безопасности персональных данных в коммерческих организациях // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 92–95.

Современное общество все более осознает важность информационной безопасности в условиях активного использования информационно-коммуникационных технологий. Это связано с развитием информационного обмена и увеличением объёма конфиденциальной информации, касающейся каждого из нас. Коммерческие организации, работающие с персональными данными клиентов, обязаны соблюдать строгие требования законодательства в этой области. Одним из основных инструментов обеспечения безопасности персональных данных является выбор и применение соответствующих средств защиты информации. В рамках этого вопроса особое внимание уделяется выбору методов и средств защиты информации, а также их нормативно-правовой регламентации. В статье рассматриваются особенности процесса выбора средств и методов защиты в контексте российского законодательства.

В России существует множество Федеральных Законов, постановлений Правительства, приказов различных служб, регулирующих обработку персональных данных, но в этой статье будут рассмотрены только те, которые контролируют выбор методов и средств защиты информации.

Для определения алгоритма выбора средств и методов защиты необходимо проанализировать, каким способом происходит обработка персональных данных в организации. Обработка персональных данных может осуществляться как в информационной системе, так и без использования средств автоматизации. Для предприятий, обрабатывающих ПДн вручную (без использования ЭВМ), следует использовать перечень мер, указанных в постановлении Правительства РФ №687 [2]. Исходя из этого документа, организация обязана обеспечить раздельное хранение персональных данных, которые обрабатываются в различных целях. Следует добавить, что постановление Правительства также обязывает соблюдать условия, при которых будет исключен несанкционированный доступ к местам хранения. Как правило, эти требования выполняются путем использования запирающихся шкафов (сейфов), созданием должностных инструкций и положения о разграничении прав доступа к обрабатываемым персональным данным.

Особое значение приобретает вопрос обработки персональных данных в информационных системах. Для того, чтобы разобраться в нём, необходимо обратиться к нижеперечисленным документам. Первоначально рассмотрим Федеральный Закон «О персональных данных» [5]. Данный закон направлен на защиту личной информации граждан, в нем устанавливается ответственность за нарушение законодательства и правила сбора, хранения и обработки персональных данных. В статье 19, пункт 3 Федерального закона [5] говорится об установлении уровней защищенности и требований к защите ПДн. В связи с этим, следует акцентировать внимание на постановлении Правительства № 1119 [1]. Рассматриваемый документ устанавливает конкретные правила и предписания для обеспечения безопасности персональных данных граждан. Важной частью нормативно-правового акта является порядок определения актуальных угроз для ИСПДн, выделяется три типа угроз, и классификация уровня защищенности ПДн, она формируется в зависимости от категории ПДн, класса актуальных угроз, количества обрабатываемых субъектов и принадлежности субъектов к оператору. Далее согласно документу, оператор самостоятельно выбирает средства защиты на основе нормативно-правовой базы, утвержденной ФСТЭК и ФСБ России.

Постановление правительства [1] ссылает нас на приказ ФСБ №378 и приказ ФСТЭК №21. Стоит отметить, что приказ ФСБ регламентирует обеспечение безопасности персональных данных с помощью применения криптографических средств защиты информации [4]. Обратим особое внимание на приказ ФСТЭК №21 [3]. В документе выделяются 15 групп технических мер, которые необходимо применить для обеспечения безопасности. В каждой группе описаны средства, которые может использовать оператор. Акцентируем внимание на том, что приказ обеспечивает гибкость при выборе мер и средств защиты. Это является безусловным плюсом для оператора. Документ не заставляет строго выполнять все имеющиеся требования для уровня защищенности. Организация имеет право исключить те меры, которые изначально не учитывались из-за нехватки финансово-технических возможностей. Также стоит отметить важность

внедрения сертифицированных средств защиты информации. Это необходимо для прохождения процедуры аттестации информационной системы. Аттестация — это комплекс организационно-технических мероприятий, направленный на оценку защищенности обрабатываемых данных в информационной системе. Аттестация обязательна для государственных информационных систем, а также может быть проведена добровольно для любых желающих этого организаций. Список сертифицированных средств представлен в государственном реестре сертифицированных средств защиты информации.

В результате изучения нормативно-правовых актов в области защиты ПДн был сформирован алгоритм для коммерческих организаций по выбору средств защиты персональных данных, обрабатываемых в информационной системе персональных данных:

1. Изучение ФЗ «О персональных данных». Это необходимо для общего понимания концепции обработки и защиты персональных данных. На этом этапе оператор знакомится с общими положениями, узнает какие категории ПДн существуют, что является обработкой ПДн и так далее. Следует заметить, что именно в этом документе дается ссылка на постановление Правительства №1119.

2. Разбор ПП №1119. Несомненная важность этого документа заключается в описании порядка определения актуальных угроз и уровня защищенности. Оператору необходимо правильно выбрать тип угроз и уровень защищенности, так как от этих действий зависит список нужных мер и средств для установки.

3. Анализ приказов ФСТЭК №21 и ФСБ №378. В данных документах необходимо оценить предложенные меры для уровня защищенности в организации и составить перечень базовых мер. Из созданного списка мер исключить те, которые изначально не были учтены из-за нехватки технических возможностей. Далее выбрать подходящие защитные меры и сопоставить их с угрозами, которые являются актуальными для организации. Если все угрозы персональных данных не были перекрыта полностью, то стоит воспользоваться компенсационными мерами защиты.

4. Работа с государственным реестром сертифицированных средств защиты информации. На этом этапе анализируем составленный список мер и подбираем под них средства защиты. Выбор конкретных средств защиты информации должен осуществляться на основе анализа рисков и потребностей организации, а также с учетом требований законодательства. Необязательно выбирать множество различных средств защиты, порой бывает достаточно нескольких универсальных средств, которые будут перекрывать сразу все требования.

В заключении исследования по данной теме стоит подчеркнуть важность правильной работы с нормативно-правовой документацией в области защиты персональных данных. Особый акцент следует сделать на необходимости соответствия выбранных мер и средств защиты требованиям законодательства. Соблюдение всех необходимых норм позволит избежать штрафов, судебных исков, потери деловой репутации и других негативных последствий для организации. Разработанный алгоритм позволяет предприятию детально разобраться в

особенностях нормативно-правовой регламентации обеспечения информационной безопасности персональных данных и пошагово определить методы и средства, которые стоит использовать для реализации этой цели.

Список источников

1. Постановление Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119 // Официальный интернет-портал правовой информации. – 01.11.2012.
2. Постановление Правительства «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687 // Официальный интернет-портал правовой информации. – 2008.
3. Приказ ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 №21 // ФСТЭК России. – 2013.
4. Приказ ФСБ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014 № 378 // ФСБ России. – 2014.
5. Федеральный закон «О персональных данных» от 27.07.2006 № 152 // Президент России. – 2006.
6. Аверченков, В.И. Защита персональных данных в организации : монография / В.И. Аверченков, М.Ю. Рытов, Т. Р. Гайнулин. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 124 с.
7. Голембиовская, О.М. Формализация подходов к обеспечению защиты персональных данных : монография / О.М. Голембиовская, М.Ю. Рытов, К.Е. Шинаков. – Саратов : Ай Пи Эр Медиа, 2019. – 198 с.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторе

Евтихов Д. А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 621.396.6

Анализ повышения информационной безопасности техники РЭБ путём обеспечения надёжности с помощью мажоритарного резервирования

Александр Владимирович Зайцев[1], Олег Сергеевич Якушов[2]✉, Дмитрий Олегович Ермаков[3]
[1, 2, 3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1, 2, 3] nauchnajarota@yandex.ru✉, https://orcid.org/0009-0007-5540-2719

Аннотация. В данной статье рассмотрен вопрос управления рисками информационной безопасности техники РЭБ, в частности предложен способ повышения информационной безопасности, через обеспечение надёжности аппаратуры с помощью мажоритарного резервирования. Данный метод позволит снизить риски утечки данных и повысить надёжность техники радиоэлектронной борьбы, что в свою очередь повысит информационную безопасность.

Ключевые слова: информационная безопасность, надёжность, мажоритарное резервирование.

Для цитирования: Зайцев А. В., Якушов О. С., Ермаков Д. О. Анализ повышения информационной безопасности техники РЭБ путём обеспечения надёжности с помощью мажоритарного резервирования // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 96–99.

Введение

Характерной особенностью современного развития техники РЭБ является широкое применение методов и средств автоматики, вызванное переходом на автоматизированное и автоматическое управление многими производственными и технологическими процессами, созданием гибких производственных модулей, систем, комплексов. С экономической точки зрения, автоматизация является одним из основных направлений технического прогресса.

В современных условиях напряжённости, требуется постоянная готовность к любым ситуациям. Таким образом, на первый план выходит вопрос повышения надёжности средств радиоэлектронной борьбы. Кроме того, причиной, требующей повышения надёжности и информационной безопасности, является возрастание сложности технических систем, аппаратуры для их обслуживания, жёсткости условий их эксплуатации и ответственности задач, которые на них возлагаются. Недостаточная надёжность технических систем радиоэлектронной борьбы приводит к увеличению эксплуатационных затрат, сбоям и от-

казам, особенно модулей, имеющих наработку на отказ, которая в свою очередь может приводить к потерям или искажениям информации, как получаемой, так и передающей, простоям сопряжённых устройств и систем, невыполнении поставленных боевых задач, авариям.

Стоит отметить, что сбоем является событие, вызывающее временное нарушение реализации системой заданного класса алгоритмов, длительность которого не превышает некоторого временного порога $\tau_{ОТК}$, а восстановление работоспособного состояния не требует реконфигурации структуры системы. В свою очередь отказом называется событие, заключающееся в нарушении реализации заданного класса алгоритмов, длительность которого превышает некоторый временной порог $\tau_{ОТК}$, а для восстановления работоспособного состояния необходима реконфигурация системы [1, 4].

Таким образом, информационная безопасность обеспечивается надёжностью систем, модулей, аппаратуры, которая определяется надёжностью комплектующих элементов. Поэтому одним из основных и перспективных направлений обеспечения надёжности техники радиоэлектронной борьбы является резервирование.

Мажоритарное резервирование

Целью резервирования является обеспечение безотказности работы аппаратуры радиоэлектронной борьбы. Безотказность — это способность системы сохранять работоспособное состояние в течение заданного времени. Вероятность безотказной работы — это вероятность того, что при заданных условиях эксплуатации на заданном интервале времени не произойдет ни одного отказа.

В случае, когда можно считать, что интенсивность отказов системы $\lambda(t) = const$, то вероятность безотказной работы достаточно хорошо описывается экспоненциальным законом распределения:

$$P(t) = \exp(-\lambda t),$$

где λ — интенсивность отказов системы;

t — время нахождения системы в рабочем состоянии.

Вероятность появления отказа $Q(t)$ связана с вероятностью безотказной работы соотношением: $Q(t) = 1 - P(t) = 1 - \exp(-\lambda t)$.

Среднее время наработки до первого отказа $T_{СР}$ определяет, какое время система будет функционировать до первого отказа: $T_{СР} = \int_0^\infty P(t)dt = \frac{1}{\lambda}$.

Данный тип резервирования относится к резервированию с применением логических схем. Выходной сигнал системы формируется мажоритарным устройством, в котором наименьшее число входных сигналов приводит к появлению выходного сигнала [2]. Для обеспечения симметричности функций безотказности наименьшее число входных сигналов мажоритарного устройства и число резервных устройств связано соотношением [4]:

$l = \frac{m+1}{2}$.

Вероятность безотказной работы системы с мажоритарным резервированием описывается зависимостью:

$$P_{MP}(t) = \sum_{i=0}^{m-l} C_m^{l+i} p^{l+i}(t)[1-p(t)]^{m-l-i},$$

где $p(t)$ — вероятность безотказной работы не резервированного устройства.

При этом, заданным является предположение, что вероятность безотказной работы самого мажоритарного устройства равна единице. В случае мажоритарного резервирования при кратности резервирования равной трем имеем зависимости:

$$P_{MP}(t) = \sum_{i=0}^{1} C_3^{2+i} p^{2+i}(t)[1-p(t)]^{1-i} = 3p^2(t) - 2p^3(t).$$

Известно, что для случая мажоритарного резервирования при среднеквадратической ошибке одного канала равного σ справедливо выражение:

$$\sigma_{MP} = \frac{\sigma}{1.5},$$

т. е. ошибка уменьшается в полтора раза [4].

Оценивая проблему надежности и точности комплексно, целесообразно использовать логику с полным использованием резерва: мажоритарное резервирование — дуплексная схема резервирования замещением — одноканальная схема [3].

Заключение

В заключение можно отметить, что резервирование применяется в сложных технических системах, отказы в которых недопустимы по условиям работы. Мажоритарное резервирование применительно к технике радиоэлектронной борьбы обеспечит надёжность аппаратуры, что в свою очередь повысит информационную безопасность, снизит риски утечки информации или выхода из строя радиоэлектронных модулей.

Список источников

1. Тимошенков С.П., Симонов Б.М., Горошко В.Н. Основы теории надежности. М.: Юрайт, 2014. 445с.

2. Лисунов Е.А. Практикум по надежности технических систем. М.: Лань, 2015. - 240 с.

3. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. М.: Либроком, 2013. - 584 с.

4. Системы управления летательными аппаратами : учебник для студентов высших учебных заведений, обучающихся по специальности "Системы управления летательными аппаратами" направления подготовки "Системы управления движением и навигация" / Анастасьин А. В. [и др.]; под общ. ред. Г. Н. Лебедева. – Москва : МАИ, 2007.

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Зайцев А. В. – д. т. н., профессор, преподаватель цикла боевой подготовки (специалистов радиоэлектронной борьбы с наземными системами управления войсками и оружием), Войсковая часть 61460.

Якушов О. С. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Ермаков Д. О. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Зайцев А. В. – идея, сбор материала.

Якушов О. С. – обработка материала, частичное написание статьи (50 %).

Ермаков Д. О. – написание статьи, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Основные угрозы в обеспечении безопасности информации в медицинских учреждениях

Яна Сергеевна Зейдлиц[1]✉, Кирилл Андреевич Седаков[2], Александр Алексеевич Рогозин[3], Сергей Максимович Егоров[4]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3, 4] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1] zeydlits70@mail.ru✉, https://orcid.org/0009-0002-9284-4624
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624
[3, 4] nauchnajarota@yandex.ru, https://orcid.org/0009-0007-5540-2719

Аннотация. В данной статье исследуются основные угрозы, с которыми сталкиваются медицинские учреждения в области обеспечения безопасности информации. Авторы рассматривают различные аспекты, такие как кибератаки, утечки конфиденциальных данных пациентов и другие возможные риски. Исследование направлено на выявление ключевых проблем и предложение эффективных мер по защите информации в сфере здравоохранения.

Ключевые слова: угрозы, безопасность информации, медицинские учреждения, кибератаки, конфиденциальность данных, риски, защита информации, сфера здравоохранения.

Для цитирования: Зейдлиц Я. С., Седаков К. А., Рогозин А. А., Егоров С. М. Основные угрозы в обеспечении безопасности информации в медицинских учреждениях // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 100–103.

Обеспечение безопасности информации в медицинских учреждениях является одним из важнейших аспектов их деятельности. Данные пациентов, в том числе медицинская история, результаты обследований, диагнозы, лечебные рекомендации и другая конфиденциальная информация, являются чрезвычайно важными и должны быть защищены от несанкционированного доступа, утечек и изменений.

Соблюдение конфиденциальности пациентов не только обязательно с точки зрения этики и законодательства, но и является основой доверия между пациентом и медицинским учреждением. Нарушение безопасности информации может привести к утечке личных данных пациентов, их финансовой информации, а также к возможным медицинским ошибкам и нарушению лечебного процесса.

Системы защиты информации в медицинских учреждениях должны соответствовать высоким стандартам и включать в себя шифрование данных, защиту доступа к информации, контроль доступа к базе данных, а также регулярные аудиты и мониторинг безопасности.

Все сотрудники медицинских учреждений также должны быть проинструктированы по соблюдению правил безопасности информации и обязаны работать в строгом соответствии с ними. Обучение персонала по вопросам информационной безопасности также является важной составляющей обеспечения безопасности информации в медицинских учреждениях.

Медицинские учреждения содержат огромное количество чувствительной информации о пациентах, включая личные данные, медицинскую историю, результаты тестов и прочие конфиденциальные сведения. В связи с этим, основные угрозы безопасности информации в медицинских учреждениях включают:

1. Кибератаки: хакеры могут пытаться взломать системы медицинских учреждений, чтобы получить доступ к личным данным пациентов. Это может привести к утечке конфиденциальной информации и ее неправомерному использованию.
2. Вредоносное программное обеспечение: зловредное ПО может быть развернуто в сети медицинского учреждения, чтобы получить доступ к чувствительным данным или причинить вред системе.
3. Утеря данных: несанкционированный доступ к данным или ошибки в системе могут привести к потере важных медицинских записей или личной информации пациентов.
4. Недостаточная защита мобильных устройств: использование мобильных устройств для доступа к медицинским данным может стать источником угрозы безопасности, если устройства не защищены должным образом.
5. Человеческий фактор: неправильное обращение с данными, недостаточная обученность персонала по вопросам безопасности информации и утеря средств аутентификации также могут стать угрозой безопасности в медицинских учреждениях.

Нарушение безопасности информации в медицинских учреждениях может иметь серьезные последствия как для самих учреждений, так и для их пациентов.

Во-первых, утечка конфиденциальной медицинской информации может привести к нарушению законов о защите данных и привлечению учреждения к ответственности. Это может привести к штрафам, репутационным потерям и даже закрытию учреждения.

Во-вторых, утечка медицинской информации может повлечь за собой серьезные последствия для пациентов. Их личные данные могут быть использованы в мошеннических целях, что может привести к краже личной информации или финансовых средств. Кроме того, утечка медицинской информации может повлечь за собой утечку медицинских секретов и нарушение приватности пациентов.

В-третьих, нарушение безопасности информации может привести к потере доверия со стороны пациентов и коллег. Пациенты могут потерять уверенность в учреждении и перестать обращаться за медицинской помощью, а коллеги могут утратить доверие к учреждению и его способности защищать их личные данные.

Поэтому защита конфиденциальности и безопасности информации в медицинских учреждениях является крайне важной, и учреждения должны принимать все необходимые меры для ее обеспечения и предотвращения возможных нарушений.

Медицинские учреждения имеют доступ к большому объему чувствительной информации, включая медицинские записи, личные данные пациентов, результаты тестов и прочие конфиденциальные данные. Поэтому важно принимать эффективные меры по защите информации в медицинских учреждениях, чтобы предотвратить утечку данных и сохранить приватность пациентов.

Ниже приведены основные меры, которые могут быть применены в медицинских учреждениях:

1. Установка и использование современных систем защиты данных, включая сетевые брандмауэры, антивирусное программное обеспечение, системы контроля доступа и допуска, шифрование данных и другие технологические средства защиты.
2. Обучение сотрудников медицинского учреждения правилам безопасности информации, включая обработку конфиденциальной информации, безопасность паролей, необходимые меры предосторожности в обращении с компьютерами и т.д.
3. Ограничение доступа к конфиденциальной информации только сотрудникам, которым это необходимо для выполнения своих обязанностей. Также важно устанавливать ограничения на доступ к данным в зависимости от уровня доверия и должности сотрудника.
4. Регулярное обновление программного обеспечения и аппаратного обеспечения, чтобы защищать системы от новых видов угроз и вирусов.
5. Резервное копирование данных, чтобы восстановить информацию в случае утери или повреждения системы.
6. Соблюдение законодательства о защите информации, таких как HIPAA в США или GDPR в Европейском союзе.

Все эти меры должны сочетаться и регулярно обновляться, чтобы обеспечить максимальную защиту конфиденциальной информации в медицинских учреждениях.

В заключение можно отметить, что безопасность информации в медицинских учреждениях играет критическую роль в обеспечении конфиденциальности данных пациентов и предотвращении возможных угроз для их здоровья и безопасности. Основные угрозы включают в себя хакерские атаки, утечки данных, несанкционированный доступ к медицинской информации и другие виды киберугроз. Для минимизации рисков необходимо применять современные технологии защиты данных, обучать персонал по вопросам информационной

безопасности и строго соблюдать законы о конфиденциальности медицинской информации. Постоянное обновление систем безопасности и мониторинг уязвимостей помогут предотвратить возможные угрозы и обеспечить надежную защиту информации в медицинских учреждениях.

Список источников

1. Центр информационной безопасности в здравоохранении (ЦИБЗ). URL: https://www.cibz.ru/ (дата обращения: 30.03.2024).
2. Федеральная служба по надзору в сфере здравоохранения (Росздравнадзор). URL: https://roszdravnadzor.gov.ru/ (дата обращения: 01.04.2024).
3. Информационно-аналитический центр по медицинской информационной безопасности (ИАЦ МИБ). URL: https://www.iacmib.ru/ (дата обращения: 31.03.2024).
4. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26.07.2017 № 187-ФЗ. URL: http://www.consultant.ru (дата обращения: 01.04.2024).

Статья поступила в редакцию 28.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Зейдлиц Я. С. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Рогозин А. А. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Егоров С. М. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Зейдлиц Я. С. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – написание статьи, научное редактирование текста (30 %).

Рогозин А. А. – обработка материала, частичное написание статьи (10 %).

Егоров С. М. – обработка материала, частичное написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Оценка подверженности активов актуальным угрозам информационной безопасности

Руслан Игоревич Зимин[1]✉, Егор Евгеньевич Чинил[2], Илья Сергеевич Гущин[3], Кирилл Евгеньевич Шинаков[4]
[1, 2, 3, 4] Брянский государственный технический университет, Брянск, Россия
[1, 2, 3] bryansk-tu@yandex.ru✉
[4] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. В современном цифровом мире, где информация стала одним из самых ценных активов, оценка подверженности активов актуальным угрозам информационной безопасности становится необходимостью для обеспечения защиты конфиденциальности, целостности и доступности данных. Этот процесс является ключевым в области информационной безопасности, поскольку позволяет идентифицировать уязвимости и риски, с которыми сталкиваются информационные ресурсы.

Ключевые слова: угрозы, информационная безопасность, уровень подверженности активов.

Для цитирования: Зимин Р. И., Чинил Е. Е., Гущин И. С., Шинаков К. Е. Оценка подверженности активов актуальным угрозам информационной безопасности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 104–107.

Защита информации — одна из приоритетных и часто недооцениваемых задач, которая встает перед организациями различного масштаба и различной сферы деятельности.

В настоящее время большая часть бизнес-процессов любого объекта производится в онлайн режиме, данные циркулируют в сети и это облегчает злоумышленникам возможность их получения. По данным НКЦКИ ежедневно на российские компании направлено более 170 кибератак. При этом осуществляемые кибератаки наносят организациям огромный ущерб — средний ущерб компаний от кибератак за 2023 год не менее 20 млн, без учёта репутационных потерь [1].

Приведенная статистика свидетельствует о том, что в вопросах целесообразности разработки и совершенствования защиты объекта от угроз безопасности информации также следует учитывать подверженность воздействию активов организации.

Уровень подверженности активов актуальным угрозам ИБ зависит от того, насколько масштабный ущерб возможен для актива в случае, если рассматриваемая угроза будет реализована на объекте.

Выделяется три уровня подверженности:

- Высокая подверженность воздействию — значительный или полный ущерб для актива.
- Средняя подверженность воздействию — средний или ограниченный ущерб.
- Низкая подверженность воздействию — незначительный ущерб или отсутствие такового.

Для каждого актива организации следует составить прогностическую карту возможного ущерба в случае реализации актуальных для организации угроз информационной безопасности. Уровень подверженности воздействию по каждой угрозы выставляется экспертным методом относительно специфики организации и критичности возможных последствий.

Общий уровень подверженности актива актуальным угрозам ИБ определяется по следующему правилу: если для всех угроз установлен низкий уровень подверженности воздействию — общий уровень подверженности актива актуальным угрозам ИБ низкий, если хотя бы для одной угрозы установлен средний уровень подверженности воздействию и при этом ни для одной не установлен высокий — общий уровень подверженности актива актуальным угрозам ИБ средний, если хотя бы для одной угрозы установлен высокий уровень подверженности воздействию — общий уровень подверженности актива актуальным угрозам ИБ высокий.

Пример прогностической карты представлен в таблице 1.

Таблица 1

Пример прогностической карты для оценки уровня подверженности актива актуальным угрозам ИБ

Активы Актуальные угрозы	Персональные данные работников	Сайт организации	Сервер отдела продаж
УБИ.1 Угроза утечки информации	Штрафы в соответствии с действующим законодательством ст. 13.11 КоАП РФ, до 100 тыс. руб. + компенсация морального ущерба в соответствии с исками (штат организации 40 человек). *Средний*.	На сайте обрабатываются ПДн клиентов организации, соответственно возможны штрафы в соответствии с действующим законодательством ст. 13.11 КоАП РФ, до 100 тыс. руб. + компенсация морального ущерба в соответствии с исками (средняя численность записей с	На сервере в том числе обрабатываются ПДн клиентов, соответственно возможны штрафы в соответствии с действующим законодательством ст. 13.11 КоАП РФ, до 100 тыс. руб. + компенсация морального ущерба в соответствии с исками (средняя численность записей с ПДн на сервере 1000). Помимо этого, разглашение условий договоров и порядка про-

Активы Актуальные угрозы	Персональные данные работников	Сайт организации	Сервер отдела продаж
		ПДн на сайте 350). *Высокий.*	даж может повлечь потерю клиентов и конкурентного преимущества. *Высокий.*
УБИ.6 Угроза отказа в обслуживании	Угроза не актуальна для рассматриваемого актива	Остановка работы сайта приведет к тому, что на время будет остановлен данный канал продаж, в среднем за день через сайт осуществляется продажа 3 клиентам на сумму около 210 тыс. руб. Восстановление работы сайта займет 1 день и будет в среднем стоить около 8 тыс. руб. *Средний.*	Остановка работы сервера приведет к остановке работы отдела продаж. В среднем через отдел продаж в день проходит 7 клиентов на общую сумму около 500 тыс. руб. Восстановление работы сервера займет 2 дня и будет стоить около 15 тыс. руб. *Высокий.*
УБИ.8 Угроза нарушения функционирования (работоспособности)	Угроза не актуальна для рассматриваемого актива.	Остановка работы сайта приведет к тому, что на время будет остановлен данный канал продаж, в среднем за день через сайт осуществляется продажа 3 клиентам на сумму около 200 тыс. руб. Восстановление работы сайта займет день и будет в среднем стоить около 8 тыс. руб. *Средний.*	Остановка работы сервера приведет к остановке работы отдела продаж. В среднем через отдел продаж в день проходит 7 клиентов на общую сумму около 500 тыс. руб. Восстановление работы сервера займет 2 дня и будет стоить около 15 тыс. руб. Если потребуется покупка нового сервера, организация потратит 130 тыс. руб. на покупку аналогичного и около недели на восстановления данных и корректной работы. *Высокий.*
Общий уровень подверженности	Средний	Высокий	Высокий

Таким образом, при помощи представленного подхода организация может рассчитать уровень подверженности актива актуальным угрозам ИБ и спрогнозировать возможный ущерб для объекта в случае реализации актуальных угроз ИБ.

Список источников

1. Самые крупные кибератаки 2023 года [Электронный ресурс] – Режим доступа: https://blog.cortel.cloud/2023/09/14/samye-krupnye-kiberataki-2023-goda/ (Дата обращения: 01.03.2024).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Зимин Р. И. – выпускник кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Чинил Е. Е. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Гущин И. С. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Зимин Р. И. – обработка материала, написание статьи (50 %).
Чинил Е. Е. – сбор материала, частичное написание статьи (17 %).
Гущин И. С. – сбор материала, частичное написание статьи (17 %).
Шинаков К. Е. – идея, научное редактирование (16 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 681.3

Новизна решенных научно-технических проблем при создании электронной компонентной базы космического назначения

Константин Владимирович Зольников[1], Анна Александровна Илунина[2], Артём Сергеевич Грошев[3], Николай Николаевич Литвинов[4], Павел Александрович Чубунов[5]

[1] АО «Научно-исследовательский институт электронной техники», Россия
[2, 3, 4] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[5] АО «Научно-исследовательский институт космического приборостроения», Россия
[1] k.v.zolnikov@gmail.com
[2] ilunina12@rambler.ru
[3] ArtGrosh@mail.ru
[4] nilit1990@mail.ru
[5] chubunov1@mail.ru

Аннотация. В статье обсуждается значительное увеличение требований к современным электронным компонентам (ЭКБ) в космической и военной отраслях, обусловленное необходимостью соответствия новым стандартам и технологиям. Рассматриваются три основных направления решения данной проблемы: развитие методов проектирования с учетом радиации, создание средств диагностики и контроля стойкости, а также разработка средств комплексного моделирования и автоматизации производства. Подчеркивается значимость внедрения новых технологий для обеспечения радиационной стойкости, улучшения надежности и оптимизации процессов проектирования и производства современных специализированных ЭКБ.

Ключевые слова: электронная компонентная база, радиация, стойкость.

Для цитирования: Зольников К. В., Илунина А. А., Грошев А. С., Литвинов Н. Н., Чубунов П. А. Новизна решенных научно-технических проблем при создании электронной компонентной базы космического назначения // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 108–113.

Существенно возросшие требования по: унификации и стандартизации; расширению сферы применения, полной автоматизации управления, дальности связи; обнаружению, сложности идентификации; сопровождению и точности управления, надежности; снижению габаритов, веса и стоимости, а также со-

вершенствованию систем активного противодействия с использованием электромагнитного и ионизирующего излучения с новыми амплитудно-временными характеристиками и сложным спектральным составом привели к необходимости создания современного поколения отечественной ЭКБ для космической и военной отрасли.

В основу их реализации положен предложенный авторским коллективом комплекс оригинальных научно-технических и конструкторско-технологических решений, обеспечивающих создание принципиально нового поколения высокопроизводительной, устойчивой к внешним воздействиям специализированной ЭКБ (микропроцессорных наборов, заказных и полузаказных БИС и СБИС) и ССиУ на их основе, отвечающих требованиям обеспечения надежного функционирования в заданных условиях (климатического диапазона, механических нагрузок, специальных внешних воздействий и др.).

Решение данной задачи осуществлялось по трем направлениям: развитию методов проектирования с учетом радиации, в том числе и космического пространства; создания средств диагностики и контроля стойкости в процессе проектирования и производства; созданию ЭКБ предельно высокой радиационной стойкости [1, 2, 3, 4].

Для реализации первой задачи — создания специализированной ЭКБ — были определены требования к современным СС и СУ двойного назначения, определена номенклатура и технические параметры ЭКБ, возможности отечественной электронной промышленности по их разработке и производству, проведена модернизация средств проектирования, в результате которой создана научная и промышленная инфраструктура разработки и производства специализированной ЭКБ и оценки ее стойкости.

Средства диагностики и оценки стойкости создавались на основе разработанных руководящих материалов и комплекса государственных стандартов «Климат-7» как автономные компоненты, построенные из типовых унифицированных модулей, на базе которых могут проводится испытаний. Они позволяли получить уникальную информацию по изменению характеристик элементов микросхем в процессе воздействия радиации.

К наиболее существенным результатам обладающим новизной можно отнести: обоснование требований к специализированной элементной базе, проведение глубокой ревизии существующей элементной базы, разработку широкой номенклатуры типовых элементов и СФ блоков с оптимизацией системо- и схемотехнических решений и параметров и создания новой элементной базы с улучшенными эксплуатационными характеристиками, обеспечивающей реализацию нового поколения СУ с требуемыми параметрами; оптимизацию структурно-логических решений СФ блоков микросхем, направленной на повышение надежности, в том числе за счет минимизации кратности резервирования и полной унификации и стандартизации всех модулей, межмодульных и межсистемных интерфейсов; введение в состав СФ-блоков подсистем со встроенными проблемно-ориентированными вычислителями; организацию распределенной

вычислительной среды с иерархическим управлением, обеспечивающие динамическое перераспределение задач между ними и восстановление работоспособности микросхемы после сбоев, вызванных внешними воздействиями и адаптации (перестройки) структуры и вычислительного процесса к возникающим не стандартным ситуациям и отказам; создание комплекса средств автоматизации проектирования, отработки конструкторско-технологической документации, организации и автоматизации производства, лабораторных исследований и испытания элементной базы, электронных модулей и ССиУ, автоматизации разработки программного обеспечения средств связи и управления и проведения вычислений.

Рассматривая задачу создания средств диагностики и контроля стойкости в процессе проектирования, производства и на стадии оценки стойкости и сертификации ЭКБ специального назначения можно отметить новизну заключающуюся в: разработке состава и последовательности испытаний, определении параметров критериев годности, создании методов измерения параметров, в том числе дистанционно, разработке алгоритмического и программного обеспечения диагностики функционирования ЭКБ, создании тестовых последовательностей наиболее информативного измерения электропараметров; разработке испытательного оборудования, способного в автоматизированном режиме проводить измерения критериальных параметров в процессе воздействия импульсных и статических видов радиации и в автоматическом режиме проводить измерения критериальных параметров при воздействии тяжелых заряженных частиц; разработке алгоритмического и программного обеспечения регистрирующей аппаратуры; создании средств диагностики стойкости на стадии проектирования и производства в том силе на пластинах; создании высоколокального неразрушающего диагностического комплекса, позволяющего максимально исследовать микросхемы на дефектоскопию по критерию радиационной стойкости.

Несмотря на то, что на момент постановки задачи создания нового поколения ЭКБ уровень развития методов моделирования, автоматизации проектирования и производства изделий радиоэлектронной и вычислительной техники был достаточно высок, с их помощью можно было решать лишь частные задачи.

Поэтому была поставлена задача разработки средств комплексного моделирования, автоматизации проектирования и производства специализированной элементной базы, которые должны обеспечивать возможности: моделирования систем по иерархическому принципу без ограничения их сложности (на системном, архитектурном, поведенческом, регистровом, функционально-логическом, схемотехническом и топологическом уровнях); моделирования и отладки базовых системных и проблемно-ориентированных алгоритмов и программ; обеспечения сквозного цикла и высокой эффективности моделирования; автоматизации процессов разработки конструкторско-технологической документации, производства, измерения и проведения испытаний.

Поставленная задача разработки средств комплексного моделирования, автоматизации проектирования и производства выполнялась в рамках нескольких десятков НИР и ОКР. В ходе ее реализации был существенно развит аппарат математического моделирования, систем автоматизации проектирования и производственных процессов. Были предложены оригинальные методы, модели и алгоритмы различных уровней моделирования — поведенческого, функционально-логического, схемотехнического, топологического, а также автоматизации процессов производства, измерения и испытания.

В первую очередь можно отметить существенный вклад авторов в развитие методологии, моделей и алгоритмов поведенческого моделирования; методов и алгоритмов экспресс-анализа электронных узлов на тестопригодность на начальных этапах их проектирования; методов и алгоритмов верификации логики, моделирования неисправностей и автоматизированной генерации тестов; моделей и алгоритмов схемотехнического моделирования; методологии, моделей и алгоритмов моделирования воздействия радиации на параметры микросхем и радиоэлектронных модулей; оптимизации системо- и схемотехнического базиса, и структурно-логических решений; методов и алгоритмов конструкторского проектирования, управления технологическим оборудованием, установками проведения измерений и испытаний, создание средств диагностики приборов на стадии производства по критерию радиационной стойкости.

Проведена программная реализация средств комплексного моделирования, автоматизации проектирования, производства, испытания и диагностики, которые включают несколько десятков комплексов программ.

На основе разработанных средств созданы рабочие места с использованием современных высокопроизводительных многопроцессорных серверов и рабочих станций, которые объединены в локальные вычислительные комплексы и единую вычислительную сеть базовых предприятий и организаций.

Разработка средств комплексного моделирования, автоматизации проектирования и производства позволила обеспечить заданные технические параметры и резко сократить цикл проектирования элементов и узлов ЭКБ, повысить достоверность проектирования, сократить объем проведения физического моделирования и очень трудоемких и дорогостоящих экспериментальных исследований. Цикл проектирования с помощью разработанных средств составляет для ЭКБ несколько недель, вместе с испытаниями несколько месяцев.

Решение задачи производства современной ЭКБ требует применения самых высоких наукоемких технологий.

Для этого была разработана и реализована программа развития базовых средств, в ходе которой были созданы автоматизированные рабочие места, оснащенные самой современной вычислительной техникой и технологическим оборудованием.

Разработаны физические основы важнейших процессов глубоко субмикронной (0,13 мкм и менее) технологии кремниевых КМОП СБИС.

В процессе реализации данной задачи с участием авторов был определена структура и состав средств автоматизации сквозного производства ЭКБ, с достижением требуемых технико-экономических показателей. Сформировано автоматизированное испытательное и измерительное оборудование по проверке технологических операций, проведению имитационных и стендовых испытаний, включая нестандартное, и сформированы и переданы в эксплуатацию пакеты оригинального ПО.

В рамках данной работы разработано современное поколение ЭКБ с радиационной стойкостью, соответствующей современному мировому уровню; которые являются важной составляющей СУ с обеспечением лучших в мире тактико-технических характеристик ракетных комплексов и космических летательных аппаратов.

За период выполнения работы выпущено несколько сотен миллионов микросхем двойного назначения — микропроцессоров, микроконтроллеров, ОЗУ, ЦАП, АЦП, а также заказных и полузаказных БИС.

Список источников

1. Технология разработки RTL модели описания изделия при разработке программно-аналитического комплекса САПР / Д.В. Шеховцов, А.М. Плотников, К.В. Зольников, А.И. Заревич // Моделирование систем и процессов. – 2023. – Т. 16, № 3. – С. 7.

2. Применение изделий полупроводниковой электроники в экстремальных условиях / М.И. Колесников, М.Э. Харченко, В.А. Дорохов, К.В. Зольников // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 46-56.

3. Применение элементов отрицательной логики при построении энергоэффективного комбинационного устройства / Ф.В. Макаренко, А.С. Ягодкин, О.А. Денисова [и др.] // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 56-66.

4. Полуэктов, А.В. Моделирование работы диода и оценка параметров его работы / А.В. Полуэктов, Р.Ю. Медведев, В.К. Зольников // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 85-93.

Статья поступила в редакцию 05.05.2024; принята к публикации 15.05.2024.

Информация об авторах

Зольников К. В. – к. т. н., ведущий инженер АО «НИИЭТ».

Илунина А. А. – к. филол. н., заведующий кафедрой иностранных языков ФГБОУ ВО «ВГЛТУ».

Грошев А. С. – аспирант ФГБОУ ВО «ВГЛТУ».

Литвинов Н. Н. – к. т. н., доцент ФГБОУ ВО «ВГЛТУ».

Чубунов П. А. – главный специалист АО «НИИКП».

Вклад авторов

Зольников К. В. – идея, сбор материала, обработка материала, частичное написание статьи (40 %).

Илунина А. А. – сбор материала, обработка материала, частичное написание статьи (15 %).

Грошев А. С. – сбор материала, обработка материала, частичное написание статьи (15 %).

Литвинов Н. Н. – сбор материала, обработка материала, частичное написание статьи (15 %).

Чубунов П. А. – сбор материала, обработка материала, частичное написание статьи (15 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 381.3

Развитие отечественной электронной компонентной базы космического назначения

Владимир Константинович Зольников[1], Артём Петрович Лапшин[2], Евгений Вячеславович Шмаков[3], Елена Альбертовна Маклакова[4]
[1, 2, 4] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[3] АО «Микрон», Россия
[1] wkz@rambler.ru
[2] lap109@mail.ru
[3] evsh@mikron.ru
[4] mak2022@mail.ru

Аннотация. В статье обсуждается важность развития радиационно-стойкой электронной компонентной базы (ЭКБ) для обеспечения национальной безопасности России в условиях современных вызовов. Авторы показывают, что существующие и новые ракетно-ядерное и высокоточное оружие, а также создание новой системы противоракетной обороны требуют новых технологий в космической отрасли для обеспечения необходимых параметров.

Ключевые слова: электронная компонентная база, космическое пространство, радиация.

Для цитирования: Зольников В. К., Лапшин А. П., Шмаков Е. В., Маклакова Е. А. Развитие отечественной электронной компонентной базы космического назначения // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 114–117.

В результате распада СССР существенно изменилась геополитическая обстановка в мире. Приближение военных баз НАТО к границам России, территориальные претензии ряда соседних государств, и особенно совершенствование ракетно-ядерного и высокоточного оружия, разработка новой глобальной системы противоракетной обороны нашим потенциальным противником, а также возможность проведения террористических актов против РФ с применением оружия массового поражения создают угрозу национальной безопасности нашей страны. Кроме того, угрозу безопасности нашей страны и отставание в высокотехнологических областях создает и потеря приоритетов в космической отрасли. На сегодняшний момент космические летательные аппараты и средства их вывода на орбиту требуют мощнейшей модернизации. Важнейшей проблемой является проблема длительного существования орбитальных станций,

возможность проводить экспедиции дальнего космоса, включая полет на Марс. Для создания ракетно–ядерного, высокоточного оружия совершенствования космической отрасли необходимо новое поколение электронной компонентной базы (ЭКБ) космического и специального назначения, стойкой к радиационному воздействию, электромагнитному импульсу и способное работать в широком диапазоне температур и различных механических нагрузок. Еще в СССР этой проблеме уделялось высокое внимание, сейчас приняты новые государственные программы развития данного направления, однако такие работы требуют постоянного совершенствования. Поэтому была поставлена и решена задача создания и серийного производства специализированной ЭКБ нового поколения для построения на ее основе систем управления (СУ) новых ракетных комплексов, комплексов противоракетной обороны, космических систем, потому что именно параметры данной ЭКБ определяют тактико-технические свойства новых комплексов и систем.

Как показал проведенный анализ в состав специализированной ЭКБ должна входить достаточно широкая номенклатура универсальных, заказных и полузаказных БИС и СБИС. Для снижения стоимости микросхем была поставлена и решена задача расширения сферы их применения для построения различных СУ объектов военного и гражданского назначения (авиационных, обслуживания аэродромов, космических, особо опасных и т. д.). С этой же целью СУ должны строиться как унифицированные и стандартизированные модули для возможности их применения в составе разнообразных вычислительных и радиотехнических систем космического и специального назначения. Современные СУ являются сложнейшей распределенной вычислительной сетью, для их создания необходима разработка специализированных высокопроизводительных микропроцессорных наборов, заказных и полузаказных БИС и СБИС. В то же время необходимо обеспечить надежность функционирования ССиУ в жестком климатическом диапазоне, при больших механических нагрузках и специальных внешних воздействиях, в первую очередь, радиационных и электромагнитных.

Таким образом, ЭКБ должна: обеспечивать возможности значительного расширения сферы применения; быть работоспособной в условиях статических и импульсных видов радиации с предельно высокой стойкостью; обеспечивать бесперебойную работу при воздействии тяжелых ядерных частиц, при этом должны быть функциональные характеристики на современном мировом уровне; обеспечить все требуемые показатели надежности с минимизацией коэффициента резервирования блоков, уменьшения массы, габаритов и потребления электроэнергии. Для создания новой ЭКБ также было проведено совершенствование методов испытаний, разработано новое испытательное оборудование, созданы новые средства оценки стойкости, в том числе и в процессе проектирования и производства ЭКБ. При этом в ходе решения данной задачи необходимо было создать научную и промышленную базу разработки, производства и испытания ЭКБ для построения нового поколения СУ.

Работы по созданию ЭКБ в связи с их важностью, были заданы стратегией развития электронной промышленности России на период до 2030 года (утв. при-

казом Министерства промышленности и энергетики РФ от 7 августа 2007 г. №311). Были приняты Федеральные целевые программы, в рамках которых предусмотрено направление «Радиационно стойкая электронная компонентная база». Следовательно, решение задачи создания нового поколения ЭКБ космического и специального назначения крайне актуальна. В данном направлении авторами работы представлен научный задел, который отражен в публикациях [1, 2, 3, 4, 5].

В результате проведенной работы созданы средства проектирования радиационно-стойких СФ-блоков электронной компонентной базы, методы прогнозирования и диагностики стойкости на всех этапах жизненного цикла проектирования и производства микросхем, на основе чего создана электронная компонентная база нового поколения космического и специального назначения. Они освоены в промышленности, производится серийный выпуск микросхем. За период выполнения работы выпущено несколько десятков миллионов микросхем специального назначения — микропроцессоров, микроконтроллеров, ОЗУ, ЦАП, АЦП, а также заказных и полузаказных БИС. Работы проводились на протяжении ряда лет, их развитие продолжается в настоящее время. Период широкой практической реализации — начало 2008, конец 2015 года. В результате стало возможно проводить работы по проектированию цифровых, аналоговых, цифро-аналоговых микросхем с проектными нормами 0,13 мкм.

Полученные микросхемы находятся на современном мировом уровне. В работе сделаны рекомендации их использования в космической и специальной технике. Наиболее показательно их эффективное применение в составе ракетно-космических комплексах «Протон», космических летательных аппаратов, комплексов типа С-400, «Бук», универсальных комплексах типа «Панцирь-1С», что явилось одним из базовых показателей достижения рекордных в мире тактико-технических характеристик комплексов. Показательно и то, что в результате проведенного комплекса работ созданы библиотеки элементов и компонентов СФ блоков, которые могут успешно использоваться для широкой номенклатуры предприятий электронной промышленности. Таким образом, создание микросхем приобретает универсальный характер с максимальным внедрением автоматических средств по обеспечению предельно высокой радиационной стойкости с минимизацией затрат.

Экономический эффект состоит из прямого и косвенного. Прямой экономический эффект складывается из разработки и продажи микросхем специального назначения, что только для АО «НИИЭТ» и АО «ВЗПП-сборка», где внедрены полученные решения, составляет почти 1 млрд рублей в год (более 200 000 штук в год). Косвенный экономический эффект складывается из эффективной и длительной работы космических летательных аппаратов, систем вооружения, где одной из базовых составляющих является электронная компонентная база, и может составить сотни миллиардов рублей. Отметим, что данные наукоемкие технологии определяют научно-технический прогресс в ведущих отраслях промышленности и соответствуют заявленной программе их эффективного развития и реального удвоения ВВП за десять лет.

Список источников

1. Повышение формализации задач верификации топологии и электрической схемы для систем автоматизированного проектирования / А.В. Полуэктов, К.В.Зольников, А.В. Ачкасов, Ю.А. Чевычелов // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 102-111.

2. Полуэктов А.В. Моделирование влияния электромагнитных полей на микросхемы / А.В. Полуэктов, Р.Ю. Медведев, К.В. Зольников // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 129-136.

3. Горбунов В.Г. сравнительный анализ методов "Прометей" и нечетких отношений в условиях принятия / В.Г. Горбунов, О.Л. Бордюжа, А.А. Пак // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 42-56.

4. Интеграция программного продукта Calibre в среду Cadence Virtuoso и повышение интеллектуальных свойств САПР проектировании микросхем / А.В. Полуэктов, Д.В. Шеховцов, И.В. Скоркин, П.А. Чубунов // Моделирование систем и процессов. – 2023. – Т. 16, № 4. – С. 71-80.

5. Тестирование и компиляция моделей цифровых блоков в программно-аналитическом комплексе САПР / Е.В. Грошева, П.А. Чубунов, Е.В. Шмаков [и др.] // Моделирование систем и процессов. – 2023. – Т. 16, № 3. – С. 30-41.

Статья поступила в редакцию 02.05.2024; принята к публикации 15.05.2024.

Информация об авторах

Зольников В. К. – д. т. н., профессор, директор института цифровых и интеллектуальных систем ФГБОУ ВО «ВГЛТУ».

Лапшин А. П. – аспирант ФГБОУ ВО «ВГЛТУ».

Шмаков Е. В. – главный конструктор АО «Микрон».

Маклакова Е. А. – д. т. н., профессор кафедры иностранных языков ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Зольников В. К. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Лапшин А. П. – сбор материала, обработка материала, частичное написание статьи (20 %).

Шмаков Е. В. – сбор материала, обработка материала, частичное написание статьи (20 %).

Маклакова Е. А. – обработка материала, частичное написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Упрощение процесса подбора средств защиты персональных данных путем автоматизированной оценки потенциальных угроз и уязвимостей

Ксенья Федоровна Капшукова[1]✉, Кирилл Андреевич Седаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] kapshukova323@mail.ru✉, https://orcid.org/0009-0004-5108-9620
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624

Аннотация. Рассмотрена роль автоматизированной оценки угроз и уязвимостей в упрощении процесса выбора средств защиты личных данных. Изучены основные преимущества использования автоматизированных систем.

Ключевые слова: защита данных, автоматизированная оценка, угрозы, уязвимости, выбор средств защиты, безопасность информации, личные данные.

Для цитирования: Капшукова К. Ф., Седаков К. А. Упрощение процесса подбора средств защиты персональных данных путем автоматизированной оценки потенциальных угроз и уязвимостей // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 118–120.

В современном мире, где цифровизация проникает во все сферы нашей жизни, защита персональных данных (ПДн) становится все более важной задачей в сфере информационной безопасности. В сети Интернет мы оставляем огромное количество личной информации, которая может стать объектом интереса для злоумышленников. Современная цифровая среда требует эффективных методов обеспечения безопасности данных, и автоматизированная оценка представляет собой мощный инструмент для анализа потенциальных рисков. Поэтому обеспечение безопасности данных становится необходимостью как для индивидуальных пользователей, так и для компаний и организаций.

Однако, выбор правильных средств защиты данных может быть сложной задачей. Существует множество инструментов и технологий, и определить, какие из них наиболее подходят для конкретной ситуации, требует глубокого понимания угроз и уязвимостей. В этом контексте автоматизированная оценка потенциальных угроз и слабостей становится ключевым элементом в упрощении процесса выбора средств защиты личных данных. Автоматизированная оценка угроз и уязвимостей является важным инструментом в арсенале организаций и компаний, стремящихся обеспечить надежную защиту личных данных своих пользователей.

Автоматизированные системы оценки угроз и уязвимостей используют различные методы анализа, включая сканирование уязвимостей, анализ логов,

машинное обучение и другие техники, чтобы идентифицировать потенциальные риски для безопасности данных. Они также могут учитывать специфические требования и контекст каждого конкретного случая, что позволяет предложить наиболее эффективные средства защиты.

Первый шаг в автоматизации процесса выбора состава средств защиты — это проведение анализа угроз и уязвимостей. Целью этого этапа является выявление потенциальных угроз безопасности и уязвимостей в инфраструктуре и приложениях, обрабатывающих персональные данные. Автоматизация процесса выбора средств защиты ПДн основана на использовании специализированных программных средств и алгоритмов, которые анализируют данные об угрозах и уязвимостях, а также характеристики самой организации и её информационных систем. Этот процесс включает в себя несколько этапов:

Сбор данных: Автоматизированные системы собирают информацию о существующих угрозах и уязвимостях, используя данные из различных источников, таких как базы данных уязвимостей, отчеты о кибератаках, обновления безопасности и т. д.

Анализ данных: Полученные данные анализируются с использованием специальных алгоритмов, которые оценивают уровень угроз и определяют наиболее вероятные сценарии атак.

Выбор средств защиты: На основе результатов анализа система предлагает оптимальный состав средств защиты ПДн, учитывая специфику угроз и уязвимостей, а также особенности инфраструктуры организации. Это может включать в себя использование антивирусного программного обеспечения, межсетевых экранов, систем обнаружения вторжений и других средств.

Реализация и мониторинг: Выбранные средства защиты внедряются в информационную систему организации, а затем постоянно мониторятся и обновляются для обеспечения эффективной защиты от новых угроз.

На основе результатов оценки угроз и уязвимостей производится выбор оптимального состава средств защиты. Этот процесс включает в себя выбор подходящих технологий и инструментов, таких как антивирусное программное обеспечение, средства мониторинга и обнаружения инцидентов, системы контроля доступа и другие. При выборе состава средств защиты необходимо учитывать особенности инфраструктуры, типы обрабатываемых данных и уровень угроз.

Одним из преимуществ автоматизированной оценки является ее скорость и масштабируемость. В отличие от ручного анализа, который может занять много времени и требовать значительных ресурсов, автоматизированные системы способны быстро обрабатывать большие объемы данных и выдавать результаты в реальном времени. Это особенно важно в условиях быстро меняющейся киберугрозы, когда реакция должна быть незамедлительной. Кроме того, автоматизированная оценка угроз и уязвимостей может помочь предотвратить ошибки, связанные с человеческим фактором, такие как упущение важных деталей или неправильное их толкование. Это повышает надежность и точность процесса выбора средств защиты данных, снижая риск возникновения критических уязвимостей.

Наконец, автоматизированная оценка угроз и уязвимостей может существенно сократить затраты на обеспечение безопасности данных. Путем оптимизации процесса выбора средств защиты и предотвращения инцидентов нарушения безопасности, компании и организации могут сэкономить как ресурсы, так и деньги.

Таким образом, наилучшим решением для упрощения процесса подбора средств защиты персональных данных является внедрение на предприятие автоматизированной системы оценки угроз и уязвимостей. Данная система обеспечит процесс защиты данных более доступным и эффективным.

Список источников

1. Белов, А.С. Модернизация системы информационной безопасности: подход к определению периодичности / А.С. Белов, М.М. Добрышин, Д.Е. Шугуров. – М.: Инсайд, 2022. С. 76-80;

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. — 416 с. — URL: http://www.iprbookshop.ru/3587330.html.

3. Рытов М.Ю., Мусиенко Н.О., Губсков Ю.А., Минин Ю.В. Аудит и мониторинг состояния объектов информатизации в процессе проектирования комплексных систем защиты информации значимых объектов критической информационной инфраструктуры. Приборы и системы. Управление, контроль, диагностика. 2022. № 10. С. 10-18. https://elibrary.ru/item.asp?id=351232113;

4. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с. — URL: http://www.iprbookshop.ru/46584530.html.

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Капшукова К. Ф. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Капшукова К. Ф. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – написание статьи, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.5

Анализ проблематики управления инцидентами информационной безопасности

Александр Вячеславович Кауров[1]✉, Оксана Михайловна Голембиовская[2], Владимир Константинович Зольников[3], Александр Сергеевич Мещеряков[4]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3, 4] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[1] Fng.ru@bk.ru✉, https://orcid.org/0009-0003-4066-1110
[2] Bryansk-tu@yandex.ru, https://orcid.org/ 0000-0002-6433-3133
[3] wkz@rambler.ru
[4] me_a_s13@mail.ru

Аннотация. Статья рассматривает проблематику управления инцидентами информационной безопасности в современном мире, где обеспечение безопасности данных является критически важным аспектом для предприятий и организаций. Описываются ключевые проблемы, затрудняющие эффективное управление инцидентами, такие как недостаток ресурсов, сложность идентификации инцидентов, отсутствие квалифицированных специалистов и недостаток стандартов и рекомендаций. Представлены математические модели для описания этих проблем. Для оптимизации процесса управления инцидентами предлагается использование современных технологий, включая системы управления инцидентами SIEM. Обсуждаются преимущества и ограничения SIEM-систем, их способность выявлять угрозы на ранней стадии и помогать организациям улучшить свою систему безопасности. В заключении подчеркивается актуальность управления инцидентами информационной безопасности для всех организаций и возможности оптимизации данного процесса через использование современных технологий и инструментов.

Ключевые слова: информационная безопасность, угрозы, управление инцидентами, SIEM, сложность идентификации, квалифицированные специалисты, стандарты и рекомендации, оптимизация управления инцидентами, ресурсы, эффективность работы, новые технологии.

Для цитирования: Кауров А. В., Голембиовская О. М., Зольников В. К., Мещеряков А. С. Анализ проблематики управления инцидентами информационной безопасности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 121–124.

Обеспечение информационной безопасности играет важную роль в современном мире, где информация стала ключевым активом для предприятий и организаций. С каждым днем возрастает число угроз информационной безопасности, требующих непрерывного мониторинга и анализа. С увеличением числа угроз и развитием технологий, управление инцидентами информационной безопасности приобретает особую значимость. В связи с этим возникает необходимость в анализе проблематики данного вопроса и поиске путей оптимизации управления инцидентами.

На сегодняшний день информация имеет особую ценность, с одной стороны утечка или утрата информации повлечёт материальный ущерб.

Число ИТ-преступлений в России за 2023 год выросло на 29,7 % в сравнении с 2022. Такую статистику официальный представитель Министерства внутренних дел (МВД) РФ Ирина Волк привела 8 февраля 2024 года. Это число может быть больше в 3-4 раза, так как около 3/4 всех киберпреступлений остаются не раскрыты. За последние шесть лет число киберпреступлений выросло в десять раз, а уровень киберпреступности более чем в 20 раз. Данные факты еще раз доказывают важность защиты информации [1].

Целью исследования является анализ проблематики управления инцидентами информационной безопасности, выявление основных проблем и возможностей оптимизации данного процесса с использованием современных технологий.

Однако существуют проблемы, затрудняющие эффективное управление инцидентами:

Недостаток ресурсов: с увеличением сложности информационных систем и числа потенциальных угроз возникают проблемы с наличием достаточного количества ресурсов для управления инцидентами.

Эта проблема, может быть выражена через математическую формулу следующим образом:

$$R = C + I,$$

где R — это общий объем ресурсов, доступных для управления инцидентами;
C — это количество доступных человеческих ресурсов;
I — это количество доступного оборудования и программного обеспечения.

Если R меньше, чем требуемый объем ресурсов (T), то организация сталкивается с недостатком ресурсов:

$$T > R.$$

1. Сложность идентификации: развитие технологий и появление новых угроз приводит к тому, что многие инциденты остаются незамеченными, что снижает качество реагирования на них.

Эта проблема может быть описана через формулу вероятности ошибки идентификации:

$$P = (N – I) / N,$$

где P — вероятность ошибки идентификации; N — общее количество возможных инцидентов; I — количество идентифицированных инцидентов.

Чем выше значение P, тем сложнее становится идентифицировать инциденты:

$P > 0$.

2. Недостаток квалифицированных специалистов может привести к ряду проблем, связанных с управлением инцидентами информационной безопасности. Организации могут испытывать трудности в поиске и найме квалифицированных специалистов, обладающих необходимыми навыками и знаниями для выполнения своей работы. Это может приводить к снижению эффективности работы, увеличению числа инцидентов и снижению уровня информационной безопасности в целом.

3. Отсутствие стандартов и рекомендаций также может создавать ряд проблем для организаций. Без четко определенных и понятных стандартов и рекомендаций, организациям может быть трудно разрабатывать и внедрять эффективные системы управления инцидентами. Это может привести к нарушениям законодательства, ухудшению качества работы и повышению рисков для информационной безопасности.

Современный мир ставит перед организациями все более высокие требования к обеспечению информационной безопасности. Появляются новые технологии и угрозы, которые требуют постоянного совершенствования систем защиты информации.

Для оптимизации процесса управления инцидентами используются различные подходы и инструменты, например, системы управления инцидентами SIEM.

SIEM-системы собирают и анализируют данные из различных источников, таких как системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS), системы мониторинга событий безопасности (SEIM) и другие. Затем они используют алгоритмы машинного обучения и искусственного интеллекта для выявления аномалий и потенциальных угроз [2].

Одним из основных преимуществ SIEM-систем является их способность обнаруживать угрозы на ранней стадии, что позволяет организациям быстрее реагировать и предотвращать серьезные последствия. Кроме того, они могут помочь организациям улучшить свою систему безопасности, выявляя слабые места и предлагая рекомендации по их устранению.

Однако, несмотря на все преимущества, SIEM-системы также имеют некоторые ограничения. Они могут быть сложными в настройке и использовании, и требуют определенного уровня знаний и опыта для эффективной работы. Кроме того, некоторые SIEM-системы могут быть дорогими в приобретении и обслуживании, что может стать препятствием для малых и средних предприятий.

Управление инцидентами информационной безопасности остается актуальным вопросом для всех типов организаций. Оптимизация данного процесса возможна благодаря использованию современных технологий и инструментов.

Список источников

1. Министерство внутренних дел российской федерации [Электронный ресурс] – URL: https://мвд.рф/contacts/presscenter (дата обращения:10.04.2024).

2. Быков А. А. Siem система - универсальный инструмент службы информационной безопасности [Электронный ресурс] – URL: https://cyberleninka.ru/article/n/siem-sistema-universalnyy-instrument-sluzhby-informatsionnoy-bezopasnosti (Дата обращения: 10.04.2024).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Кауров А. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Зольников В. К. – д. т. н., профессор, директор института цифровых и интеллектуальных систем ФГБОУ ВО «ВГЛТУ».

Мещеряков А. С. – студент ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Кауров А. В. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Голембиовская О. М. – научное редактирование текста (30 %).

Зольников В. К. – частичное написание статьи (10 %).

Мещеряков А. С. – частичное написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Анализ использования технологии Honeypot для повышения уровня защищенности информационных систем

Сергей Игоревич Коновалов[1]✉, Владимир Александрович Воронин[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] velvet1way@gmail.com✉, https://orcid.org/0009-0008-5867-635X
[2] voroni.vladimir.ozi@gmail.com, https://orcid.org/0009-0009-5380-2465

Аннотация. Рассматривается использование технологии honeypot как инструмента для повышения уровня защищенности информационных систем. Описываются основные типы ловушек, их преимущества и недостатки.

Ключевые слова: информатизация, хакерские атаки, honeypot, приманка, ловушка, атака, защита данных, угроза, приманка.

Для цитирования: Коновалов С. И., Воронин В. А. Анализ использования технологии Honeypot для повышения уровня защищенности информационных систем // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 125–128.

Стремительная информатизация современного общества обуславливает не только бурное развитие информационных технологий, но и возрастание угроз информационной безопасности. Количество хакерских атак на информационные системы неуклонно растет, что требует применения все более совершенных методов защиты.

В числе передовых методов защиты информационных систем от несанкционированного доступа и хищения данных особое место занимает технология honeypot.

Honeypot (ханипот, приманка, ловушка) — это преднамеренно скомпрометированная система, созданная, чтобы заманить хакеров и других киберпреступников в контролируемую среду, чтобы помочь специалистам по кибербезопасности увидеть, как они работают. Она имитирует реальную систему, но не содержит ценной информации, а все действия на ней фиксируются. Затем эксперты по кибербезопасности отслеживают атаки, чтобы получить представление о том, как злоумышленник получил доступ к онлайн-данным.

Получив доступ к honeypot, хакер, как правило, приступит к исследованию систем и данных, пытаясь выяснить как можно больше о них. Помимо этого, злоумышленник может попытаться совершить кражу информации, установку вредоносного ПО или намеренно нарушить нормальную работу ресурса. Кража может быть направлена на компрометацию конфиденциальных

сведений, таких как пользовательские пароли, номера банковских карт или коммерческую тайну. Установка вредоносного кода может преследовать целью получения постоянного доступа к honeypot или использования его в качестве стартовой площадки для атак на другие системы. Нарушение работоспособности honeypot может достигаться путем организации DoS-атак или иных вредоносных действий.

Все взаимодействия хакера внутри honeypot тщательно отслеживаются и анализируются его владельцем. Среди основных типов собранных данных можно выделить следующие: сочетания клавиш, вводимые злоумышленником, IP-адрес злоумышленника, имена пользователей и различные привилегии, используемые злоумышленником, данные, к которым злоумышленник получил доступ, удалил или изменил. Собранная информация позволяет идентифицировать новые угрозы, усовершенствовать методы киберзащиты, отслеживать злоумышленников. Honeypot помогает снизить потенциальный ущерб от хакерских атак путем отвлечения внимания нападающего от реальных систем, выиграть время для внедрения дополнительных средств обеспечения безопасности, а также собрать доказательства кибератаки, которые в дальнейшем могут быть использованы для поиска и привлечения хакеров к ответственности.

Классификацию honeypots можно произвести на основании разнообразных параметров.

Приманки можно дифференцировать в зависимости от того, являются ли они физическими или виртуальными [1]. Физические приманки представляются собой реальную машину с собственным IP-адресом, эта машина симулирует поведение, смоделированное системой [2]. Виртуальные приманки позволяют устанавливать и моделировать узлы в сети из разных операционных систем, но для этого необходимо имитировать TCP/IP целевой операционной системы. Этот механизм применяется чаще.

Ловушки можно классифицировать по их развертыванию. В зависимости от развертывания, ловушки могут быть разделены на производственные и исследовательские [3]. Производственные приманки просты в использовании, захватывают только ограниченную информацию и используются в основном корпорациями. Производственные приманки помещаются организацией в производственную сеть вместе с другими производственными серверами для улучшения их общего состояния безопасности. Как правило, производственные приманки — это приманки с низким взаимодействием, которые легче развертывать. Они дают меньше информации об атаках или нападающих, чем исследовательские приманки. Исследовательские ловушки запускаются для сбора информации о мотивах и тактике хакеров, нацеленных на различные сети. Эти приманки не повышают ценность конкретной организации; вместо этого они используются для изучения угроз, с которыми сталкиваются организации, и для изучения того, как лучше защитить себя от этих угроз. Исследовательские ловушки сложны в развертывании и обслуживании, захвате обширной информации и используются в основном военными или правительственными организациями. По уровню взаимодействия можно выделить 3 ос-

новные группы: приманки с низким, средним и высоким уровнем взаимодействия. Приманки снизким уровнем взаимодействия соответствуют очень ограниченному количеству сервисов и приложений, как в системе, так и в сети. Этот тип приманки можно использовать для отслеживания портов и служб (UDP, TCP). Для изучения атак на данном уровне в качестве приманки чаще всего используются поддельные данные и файлы. Среди наиболее известных инструментов стоит отметить Spectre и KFsensor. Говоря о приманках среднего уровня взаимодействия в первую очередь стоит учитывать, что они основаны на имитации операционных систем реального времени. Наиболее актуальными инструментами на это уровне будут являться Cowrie и HoneyPy. Приманки с высоким уровнем взаимодействия представляют собой подлинноуязвимое ПО которое обычно имеется в производственной системе, где взаимодействует с различными приложениями. Отдельно стоит отметить чистые приманки, которые представляются полномасштабную систему, работающую на различных серверах. Такая система полностью имитирует производственную.

В технологии honeypot можно выделить как преимущества, так и недостатки.

Honeypot не требовательна к ресурсам сети, способна предоставить комплексный отчет о всех действиях злоумышленника [4]. А также для данной технологии характерны высокие показатели отказоустойчивости. Однако, как и любая технология, honeypot имеет и свои недостатки: настройка параметров honeypot довольно сложная техническая задача, которую приходится решать вручную, а также для данной технологии свойственна пассивность, так как злоумышленник должен сам выбрать цель для атаки.

Таким образом, honeypot — это эффективный инструмент для сбора информации о методах и тактиках хакеров, а также для тестирования и оценки систем защиты информации. Но он не является панацеей и не может заменить другие меры защиты. Грамотное использование технологии honeypot в сочетании с другими мерами защиты значительно повышает уровень безопасности информационной системы.

Список источников

1. Provos, N. "A Virtual Honeypot Framework". USENIX. Retrieved. С. 52
2. Mairh, A; Barik, D; Verma, K; Jena, D (2011). "Honeypot in network security: asurvey". ACM (Association for Computing Machinery).: С. 601.
3. Honeypot (computing) // Wikipedia URL: https://en.wikipedia.org/wiki/Honeypot_%28computing%29 (дата обращения: 03.04.2024).
4. Исследование применения технологии deception дляпредотвращения угроз кибербезопасности // KyberLeninka URL: https://cyberleninka.ru/article/n/issledovanie-primeneniya-tehnologii-deception-dlya-predotvrascheniya-ugroz-kiberbezopasnosti/viewer (дата обращения: 03.04.2024).

Статья поступила в редакцию 06.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Коновалов С. И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем», ФГБОУ ВО «БГТУ».

Воронин В. А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Коновалов С. И. – идея, сбор материала, обработка материала, написание статьи (50 %).

Воронин В. А. – научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.55

Анализ основных способов шифрования информации в мобильных устройствах

Коновалов Сергей Игоревич[1]✉, Владимир Александрович Воронин[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] velvet1way@gmail.com✉, https://orcid.org/0009-0008-5867-635X
[2] voroni.vladimir.ozi@gmail.com, https://orcid.org/0009-0009-5380-2465

Аннотация. Рассматриваются основные методы шифрования информации в мобильных устройствах, а также перспективы квантовой криптографии. Подчеркивается важность постоянного развития и улучшения методов шифрования в контексте изменяющихся угроз информационной безопасности, чтобы обеспечить эффективную защиту данных пользователей мобильных устройств.

Ключевые слова: шифрование, мобильные устройства, безопасность, квантовая криптография, виртуальная частная сеть.

Для цитирования: Коновалов С. И., Воронин В. А. Анализ основных способов шифрования информации в мобильных устройствах // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 129–132.

В современном информационном обществе мобильные устройства становятся неотъемлемой частью повседневной жизни, обеспечивая широкий спектр функциональных возможностей, включая хранение и передачу информации. Вместе с растущей зависимостью от мобильных устройств возрастает и потребность в обеспечении безопасности личных данных пользователей. Одним из ключевых методов защиты персональной информации является шифрование, которое обеспечивает конфиденциальность путем ее преобразования в непонятный для посторонних вид. Однако, с увеличением сложности атак и появлением новых методов взлома, необходимо постоянное исследование и усовершенствование существующих методов шифрования, повышение их эффективности и устранение уязвимостей.

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц [1]. Главным образом, шифрование служит для соблюдения конфиденциальности передаваемой информации. Схема шифрования обычно использует псевдослучайный ключ шифрования, сгенерированный алгоритмом. При это уполномоченный получатель может легко расшифровать сообщение с помощью ключа, предоставленного составителем.

С помощью шифрования обеспечиваются три состояния безопасности информации: конфиденциальность, целостность и идентицифицируемость [2]. Конфиденциальность заключается в том, что информация скрыта от неавторизованных пользователей. Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им. В этом смысл идентифицируемости. Целостность же заключается в предотвращении ее изменения при передаче или хранении.

Существует несколько основных методов шифрования информации в мобильных устройствах.

Первый метод, шифрование диска, представляет собой процесс защиты данных, хранящихся на жестком диске мобильного устройства. При использовании этого метода данные становятся недоступными без соответствующего пароля или ключа доступа. При использовании шифрования диска данные на мобильном устройстве остаются защищеннымидаже в случае утери или кражи устройства. Существующие операционные системы, такие как iOS и Android, предоставляют встроенные инструменты для шифрования диска, обеспечивая дополнительный уровень защиты.

Второй метод, шифрование сообщений, направлен на защиту переписки в мессенджерах и SMS-сообщениях от несанкционированного доступа. Некоторые из наиболее популярных мессенджеров, такие как WhatsApp и Telegram, предоставляют встроенные средства шифрования сообщений. Это означает, что текстовые сообщения, отправляемые через эти платформы, автоматически шифруются на устройстве отправителя и расшифровываются только на устройстве получателя, что обеспечивает конфиденциальность и безопасность переписки.

Третий метод, шифрование файлов, направлен на защиту отдельных файлов на мобильном устройстве. Этот подход особенно полезен для хранения личных документов, финансовых данных или корпоративных отчетов, доступ к которым должны иметь только авторизованные пользователи. Существует множество приложений и программ, предназначенных для шифрования файлов на мобильных устройствах, что позволяет пользователям выбирать наиболее подходящий вариант в зависимости от их потребностей. Например, некоторые приложения предлагают шифрование с использованием сильных алгоритмов, таких как Advanced Encryption Standard (AES), который является одним из наиболее надежных и широко используемых методов. Другие приложения могут предоставлять дополнительные функции, такие как возможность создания защищенных хранилищ или возможность шифрования файлов перед их передачей через интернет.

Четвертый метод, шифрование Virtual Private Network (VPN), обеспечивает защиту интернет-соединения мобильного устройства путем шифрования всего трафика и перенаправления его через удаленный сервер. Когда пользователь устанавливает VPN-соединение на своем мобильном устройстве, весь трафик, который проходит через интернет, включая передачу данных между

устройством и веб-серверами, шифруется. Затем этот зашифрованный трафик перенаправляется через удаленный сервер, где он дешифруется и отправляется в интернет. Это позволяет скрыть реальный IP-адрес пользователя и обеспечить анонимность его онлайн-активности. Особенно актуальным становится шифрование VPN при использовании общедоступных Wi-Fi сетей, таких как те, которые предоставляются в кафе, аэропортах или отелях. В таких сетях данные пользователя могут быть уязвимы для атак злоумышленников, таких как перехват трафика или внедрение вредоносного программного обеспечения. Использование VPN обеспечивает дополнительный уровень защиты, шифруя всю передаваемую информацию и предотвращая несанкционированный доступ к ней.

Отдельно стоит отменить наиболее современный метод шифрования — квантовое. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике. Она рассматривает случаи переноса информации с помощью объектов квантовой механики [3]. В процессе отправки и приема информации используются физические средства, такие как электроны в электрических токах или фотоны в линии волоконной оптической связи. Любая попытка перехвата изменит состояние квантового объекта, что будет заметно для отправителя и получателя, что делает атаку обнаружимой. Однако, несмотря на свои перспективы, квантовая криптография все еще находится на ранней стадии развития и сталкивается с рядом технических и технологических ограничений. Например, создание и поддержание квантовых каналов связи требует сложных технических решений и высоких затрат, а также существуют технические вызовы в создании надежных квантовых систем связи.

Таким образом, различные методы шифрования играют важную роль в обеспечении безопасности данных на мобильных устройствах. Однако, с учетом постоянно меняющихся угроз, необходимо проводить исследования и разработки новых методов шифрования для дальнейшего улучшения защиты конфиденциальной информации и обеспечения безопасности мобильных устройств.

Список источников

1. Мэйволд, Э. Безопасность сетей : учебное пособие : Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с.

2. Шнайер Б. Прикладная криптография. - 2-е изд. - М.: 2002. - 610 с.

3. Криптографические средства защиты: что это такое // Академия Selectel URL: https://clck.ru/39sGLn (дата обращения: 04.04.2004).

Статья поступила в редакцию 06.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Коновалов С. И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем», ФГБОУ ВО «БГТУ».

Воронин В. А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Коновалов С. И. – идея, сбор материала, обработка материала, написание статьи (50 %).

Воронин В. А. – научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Основные критерии выбора средств защиты медицинских информационных систем

Сергей Игоревич Коновалов[1]✉, Кирилл Андреевич Седаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] velvet1way@gmail.com✉, https://orcid.org/0009-0008-5867-635X
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624

Аннотация. Рассмотрены ключевые вопросы информационной безопасности в сфере здравоохранения и важная роль компьютеризации в повышении качества и эффективности медицинской помощи. Особое внимание уделяется значимости создания и основным характеристикам автоматизированной системы принятия решений при выборе средств и методов защиты медицинских информационных систем (МИС), направленной на оптимизацию процессов обслуживания пациентов и хранения медицинских данных.

Ключевые слова: медицинские информационные системы, персональные данные, информатизация здравоохранения, компьютеризация здравоохранения угрозы безопасности данных, электронное здравоохранение.

Для цитирования: Коновалов С. И., Седаков К. А. Основные критерии выбора средств защиты медицинских информационных систем // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 133–136.

В наше время, важность всестороннего обеспечения информационной безопасности становится все более актуальной, особенно в контексте информатизации всех аспектов общественно-экономической жизни. Здравоохранение не исключение: процессы хранения и обработки медицинской информации становятся все более автоматизированными и компьютеризированными. Поддержание безопасности данных в здравоохранении становится ключевым элементом для улучшения качества, эффективности и доступности медицинской помощи для всех слоев населения. С ростом информатизации возрастает и необходимость в разработке и применении современных и надежных компьютерных систем и технологий в контексте данной области.

В сложившейся ситуации отмечается тенденция к развертыванию крупных региональных и национальных медицинских информационных систем (МИС). Это направление развития связано с интеграцией передовых информационных технологий в сферу здравоохранения, что способствует улучшению

качества обслуживания, сокращению времени на проведение диагностических процедур и повышению точности диагностики. Кроме того, такие системы обеспечивают возможность для удаленных консультаций, обследований и обработки первичных данных. Важнейшей задачей при внедрении подобных систем является обеспечение безопасности информации, особенно учитывая цифровой формат хранения данных, который обеспечивает их доступность и сохранность в долгосрочной перспективе, но требует эффективных мер по защите от несанкционированного доступа.

Среди наиболее развитых направлений электронного здравоохранения выделяются консультативные сети, обеспечивающие связь между медицинскими специалистами и пациентами, системы электронных медицинских карт, содержащих полную историю болезни и аптечную информацию, а также диспетчерские системы, обеспечивающие координацию и оперативную реакцию в рамках скорой медицинской помощи.

Однако, одновременно с развитием МИС и ростом объема медицинской информации, так же возрастают риски и угрозы в данной области, в первую очередь связанные с персональными данными [1]. Обратимся к базовой модели угроз безопасности персональных данных при их обработке в информационных системах. Угрозы безопасности персональных данных делятся на два основных подвида: угрозы утечки информации по техническим каналам и угрозы несанкционированного доступа к информации [2].

Технические каналы утечки данных охватывают различные аспекты, включая звуковую и видеоинформацию. Например, аудиозаписи могут содержать чувствительные беседы между врачом и пациентом, которые могут быть скомпрометированы. Точно так же, видеоматериалы, такие как записи операций или медицинских процедур, могут содержать личную информацию о пациентах и могут стать объектом утечки, если не обеспечивается надлежащая защита данных.

При анализе угроз несанкционированного доступа к медицинской информации важно рассматривать такие аспекты, как возможность нелегального вторжения в оперативную среду компьютеров путем эксплуатации уязвимостей в штатных программных компонентах. Эти угрозы могут привести к нарушению конфиденциальности данных и целостности системы.

Согласно статистике, подведенной компанией Positive Technologies, специализирующаяся на разработке решений в сфере информационной безопасности, медицина лидирует по утечкам данных [3]. Медучреждения уже пятый год подряд остаются в тройке самых атакуемых отраслей. Они чаще всего становились источником утечек данных среди организаций. Более чем в 80% случаев атаки приводили к утечкам данных о клиентах (в основном персональных данных и медицинской информации).

Несмотря на продолжающийся процесс интеграции информационных технологий и развитие систем информационной безопасности в медицинских учреждениях, следует отметить, что часто они применяют различные реализации, которые не совместимы между собой. В настоящее время основное внима-

ние уделяется автоматизации фискальных и отчетных функций, вместо улучшения качества таких систем для более эффективного использования ресурсов. Количество полнофункциональных систем информационной безопасности все еще недостаточно. В связи с этим возникает необходимость создания единой системы информационной безопасности, обеспечивающей совместимость и согласованность различных аспектов в медицинских учреждениях.

Наиболее комплексным решением является разработка автоматизированной системы принятия решений выбора средств и методов защиты медицинских информационных систем. Такая система предоставляет возможность анализа текущих угроз и рисков, а также предлагает оптимальные варианты защиты, учитывая специфику конкретной МИС.

Автоматизированная система должна учитывать все этапы жизненного цикла информации, начиная с её поступления в систему и первичной обработки, и заканчивая уничтожением данных или истечением срока их хранения.

Более того, такая система должна обеспечивать комплексную и глобальную информационную защиту для конкретной МИС, а не только фрагментарную. Она должна использовать современные методы и инструменты информационной безопасности на всех этапах разработки МИС. Для предотвращения внешних атак рекомендуется ввести контроль над серверами и использовать антивирусную защиту как на серверах, так и на рабочих станциях. При разработке архитектурного решения следует классифицировать хранимые данные по степени конфиденциальности и значимости, а также использовать многоуровневую аутентификацию пользователей с использованием USB-ключей, смарт-карт, паролей, файловых ключей и т. д. Не менее важно также максимально разделить устройства между изолированными участками с помощью аппаратного зонирования, а программное зонирование или маскирование следует использовать в качестве дополнительного средства защиты.

Следует отметить, что для обеспечения всесторонней защиты системы необходимо опираться на самые доступные и актуальные программные решения. В России наблюдается увеличенное внимание к развитию отечественных технологий и программ в области медицины, что стимулирует быстрый рост отечественного производства медицинских информационных систем и повышение их конкурентоспособности на рынке.

Индустрия разработки программного обеспечения является одной из наиболее динамично развивающихся отраслей экономики России [4]. В настоящее время все чаще руководители медицинских организаций принимают решения об использовании ИТ-инфраструктуры и внедрении новых технологий, основываясь на оценке их эффективности.

Таким образом, разработка и внедрение систем и методов защиты медицинских информационных систем играют ключевую роль в обеспечении информационной безопасности и конфиденциальности медицинской информации. Это в свою очередь способствует повышению качества медицинского обслуживания и укреплению доверия пациентов к системе здравоохранения.

Список источников

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» URL: https://docs.cntd.ru/document/902330983 (дата обращения: 02.04.2024).

2. Федеральный закон «О персональных данных» // Президент России URL: http://letters.kremlin.ru/info-service/acts/9 (дата обращения: 02.04.2024).

3. Число кибератак в России и в мире // TAdviser URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5 (дата обращения: 03.04.2024).

4. Медицинские информационные системы как объект оценки: факторы и тенденции развития // CyberLeninka URL: https://cyberleninka.ru/article/n/meditsinskie-informatsionnye-sistemy-kak-obekt-otsenki-faktory-i-tendentsii-razvitiya (дата обращения: 03.04.2024).

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Коновалов С. И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем», ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Коновалов С. И. – идея, сбор материала, обработка материала, написание статьи (50 %).

Седаков К. А. – научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Анализ проблемы использования технологий и методов искусственного интеллекта злоумышленниками в области информационной безопасности

Карина Владимировна Короткова[1]✉, Дмитрий Андреевич Лысов[2]✉
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] marus.korotkova@yandex.ru✉, https://orcid.org/0009-0007-2396-4469
[2] lysovdmitriia@gmail.com✉, https://orcid.org/0009-0003-9666-7191

Аннотация. В настоящее время технологии искусственного интеллекта (ИИ) являются неотъемлемой частью цифровой среды и переворачивают привычные модели работы в различных сферах. Однако, вместе с ростом развития ИИ, злоумышленники стали активно применять эти технологии в целях усовершенствования своих кибератак. В данной статье рассматриваются некоторые примеры использования злоумышленниками ИИ для выполнения различного рода атак.

Ключевые слова: искусственный интеллект, кибератаки, дипфейк, фишинг, злоумышленники.

Для цитирования: Короткова К. В., Лысов Д. А. Анализ проблемы использования технологий и методов искусственного интеллекта злоумышленниками в области информационной безопасности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 137–139.

Технологии искусственного интеллекта активно внедряются в различные отрасли для улучшений и автоматизации многих процессов. По данным «McKinsey» наблюдается рост инструментов генеративного ИИ, а также следует информация о том, что более трети опрошенных респондентов заявили об увеличении инвестиций в ИИ в своих организациях [1]. Однако, важно отметить, что с развитием ИИ возрастает риск злоупотреблений данными технологиями со стороны злоумышленников, а это, в свою очередь, создает значительные угрозы безопасности данных, конфиденциальности и целостности системы в целом.

В настоящее время огромное значение использованию ИИ отводится сфере кибербезопасности. Инструменты, основанные на ИИ, могут анализировать огромные объемы данных в режиме реального времени, выявлять закономерности и аномалии, указывающие на вредоносную деятельность, и прогнозировать потенциальные нарушения безопасности.

Злоумышленники также идут в ногу со временем и начинают активно применять ИИ для усложнения и увеличения объема своих атак. Используя алгоритмы ИИ, хакеры могут автоматизировать атаки, обходить традиционные меры безопасности и использовать уязвимости в системах. Ко всему прочему, определенная часть инструментов, применяющих технологии ИИ, не требует высокой квалификации или специальных навыков, что позволяет применять их даже начинающим хакерам. В сети активно распространяются такие инструменты, как, например, FraudGPT, позволяющий создавать фишинговые письма, фишинговые web-страницы и вредоносный код; Evil-GPT — инструмент для генерации BEC-атак на электронную почту; дистрибутив ОС Kali Linux, который уже содержит в себе множество инструментов для взлома паролей и проведения пентестов [2]. Это ставит ряд вызовов перед обществом, увеличивая необходимость проявлять повышенную бдительность при работе с информацией. Одной из основных проблем в борьбе с атаками с использованием ИИ является сложность различения законного и вредоносного контента, созданного с помощью ИИ. Злоумышленники могут использовать ИИ для создания убедительных фишинговых электронных писем, дипфейков и другого вводящего в заблуждение контента, чтобы обманом заставить пользователей раскрыть конфиденциальную информацию или передать деньги. Примером использования дипфейка был обман финансового сотрудника транснациональной компании с целью вынудить выплатить 25 миллионов долларов мошенниками, выдающими себя за финансового директора компании во время видеоконференции [3]. Традиционным мерам безопасности может быть трудно обнаружить эти атаки, генерируемые искусственным интеллектом, поскольку они имитируют поведение человека и постоянно развиваются.

Алгоритмы машинного обучения (ML) и глубокого обучения (DL) лежат в основе систем обнаружения вторжений (IDS) на базе искусственного интеллекта. Эти алгоритмы могут обучаться на основе исторических данных для выявления моделей вредоносного поведения и аномалий в сетевом трафике. Тем не менее, несмотря на огромные усилия исследователей, IDS по-прежнему сталкивается с проблемами в повышении точности обнаружения при одновременном снижении частоты ложных срабатываний и в обнаружении новых вторжений [4]. В настоящее время системы ML и DL на основе IDS пока внедряются в качестве потенциальных решений для эффективного обнаружения вторжений в сети. Это дает злоумышленникам возможность использовать уязвимости в своих целях. Злоумышленники также в качестве инструментов для проведения своих атак могут использовать алгоритмы ML и DL, чтобы, например, вводить ложные данные, манипулировать процессом обучения систем, обманывать систему, заставляя ее классифицировать их вредоносные действия как обычное поведение.

Для защиты от вторжений с использованием искусственного интеллекта организациям необходимо применять многоуровневый подход к кибербезопасности. Это включает в себя внедрение надежных механизмов аутентификации, шифрование конфиденциальных данных и постоянный мониторинг сетевого

трафика на предмет подозрительных действий. Кроме того, организациям следует инвестировать в средства безопасности, основанные на ИИ, которые могут адаптироваться к возникающим угрозам и обнаруживать атаки, генерируемые ИИ, в режиме реального времени. Использование злоумышленниками технологий ИИ представляет серьезную проблему для специалистов в области кибербезопасности. По мере дальнейшего развития ИИ злоумышленники, вероятно, будут становиться все более изощренными в своих атаках. Для организаций крайне важно опережать эти угрозы, инвестируя в решения для обеспечения безопасности, основанные на ИИ, проводя регулярные аудиты безопасности и обучая сотрудников передовым методам обнаружения и предотвращения вторжений с использованием ИИ. Принимая упреждающие меры, организации могут защитить свои данные, системы и репутацию от рисков, связанных со злоумышленниками, использующими технологии искусственного интеллекта.

Список источников

1. Консалтинговая компания «McKinsey & Company» [Электронный ресурс]: – Режим доступа: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year (Дата обращения 21.04.24).

2. Известия – новости политики, экономики, спорта, культуры | IZ.RU [Электронный ресурс]: – Режим доступа: https://iz.ru/1540294/dmitrii-bulgakov/chuzhim-umom-kak-khakery-ispolzuiut-iskusstvennyi-intellekt-dlia-kiberprestuplenii (Дата обращения 21.04.24).

3. Телеканал «CNN» [Электронный ресурс]: – Режим доступа: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html (Дата обращения 21.04.24).

4. Информационный портал «SecurityLab.ru» [Электронный ресурс]: – Режим доступа: https://www.securitylab.ru/analytics/536551.php (Дата обращения 22.04.24).

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Короткова К. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

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

Вклад авторов

Короткова К. В. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Лысов Д. А. – написание статьи, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Анализ актуальных угроз безопасности персональных данных в организациях сферы здравоохранения

Карина Владимировна Короткова[1]✉, Кирилл Андреевич Седаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] marus.korotkova@yandex.ru✉, https://orcid.org/0009-0007-2396-4469
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624

Аннотация. Рассмотрены основные проблемы определения актуальных угроз безопасности персональных данных в сфере здравоохранения.

Ключевые слова: информационная безопасность, персональные данные, сфера здравоохранения, актуальные угрозы.

Для цитирования: Короткова К. В., Седаков К. А. Анализ актуальных угроз безопасности персональных данных в организациях сферы здравоохранения // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 140–142.

Интеграция информационных технологий (ИТ) в различные аспекты жизни человека, в частности в здравоохранение, стремительно растет. ИТ упрощают процессы, повышают доступность медицинской информации и оптимизируют административные задачи. Тем не менее, этот прогресс сопряжен с рисками, особенно в отношении безопасности персональных данных (ПДн). По данным исследовательской группы «Positive Technologies» медицинские учреждения находятся на втором месте по количеству совершаемых атак с целью похищения личных данных [1]. Информационно-аналитический портал «TAdviser» предоставил статью по основным утечкам данных в медицинских учреждениях за 2023, из которых можно сделать вывод о том, что защита ПДн в медицинских учреждениях остается одним из важнейших вопросов в области информационной безопасности [2].

Каждый человек имеет право на защиту его прав и свобод при обработке персональных данных, закрепленное статьей 23 Конституции РФ [3]. Помимо этого, сектор здравоохранения относится к объектам критической информационной инфраструктуры (КИИ) в соответствии с Федеральный законом 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации» [4]. Это подчеркивает важность безопасности и защиты информации, связанной с медицинскими данными, так как любое нарушение безопасности может иметь серьезные последствия для здоровья и безопасности граждан. Тем не менее, утечки ПДн продолжают происходить.

Так, например, 18 мая 2022 российская медицинская компания «Гемотест» подтвердила взлом базы данных своих клиентов, что повлекло утечку более, чем 30 млн строк с персональными данными [5].

Одной из ключевых проблем при выявлении текущих угроз безопасности ПДн в здравоохранении является динамичный характер киберугроз, который создает серьезную проблему для безопасности персональных данных в здравоохранении. Хакеры постоянно разрабатывают новые методы использования уязвимостей. Это создает необходимость проявлять повышенную бдительность — от систем мониторинга подозрительных действий до борьбы с программами-вымогателями и фишинговыми атаками, не забывая про регулярное обучение сотрудников.

Внутренние угрозы, связанные с ненадлежащим поведением сотрудников, также ставят под угрозу безопасность данных. По данным сервиса «SearchInform» с утечками информации в 2023 году столкнулось около 27 % организаций из сферы здравоохранения, при этом 64 % напрямую связано с действиями сотрудников [6]. Подобные действия могут нести как умышленный характер, так и быть вызваны недостаточной осведомленностью по вопросам обработки персональных данных или низким уровнем квалификации в области информационной безопасности.

Внешние угрозы являются не менее актуальными для медицинских организаций. Действия хакеров приводят к утечкам личной информации, нарушению нормального функционирования учреждения и даже изменению содержащихся в нем медицинских данных. Злоумышленники постоянно сканируют системы и сети здравоохранения в поисках уязвимостей, чтобы найти способы их эксплуатации и получить доступ к персональным данным. По данным газеты «The Daily Telegraph» от 1 июля 2023 года хакерской групировкой «BlackCat» (также известной как «ALPHV») была взломана база данных системы здравоохранения Британии и в общей сложности похитили 7 Тбайт личной информации пациентов, включая информацию о банковских счетах [7].

Таким образом, персональные данные в сфере здравоохранения имеют первостепенное значение, являясь чувствительной, наиболее достоверной и актуальной информацией, тем самым представляя наибольший интерес для хакеров. Дополнительно стоит отметить, что безопасность персональных данных в секторе здравоохранения находится на недостаточном уровне. Организациям этой области необходимо проявлять повышенную бдительность при обработке конфиденциальной информации — от внешних киберугроз до внутренних рисков. Важно основываться на законодательстве Российской Федерации, учитывать требования регуляторов и качественно обслуживать информационные системы, занимающиеся обработкой персональных данных, используя современное оборудования, актуальные настройки и надежные политики безопасности. Организациям здравоохранения важно быть в курсе текущих угроз безопасности персональных данных и своевременно устранять эти риски. Осведомленность о текущих угрозах имеет первостепенное значение для упреждающего реагирования на риски и защиты конфиденциальности пациентов и репутации

учреждения. Надежная политика в области информационной безопасности, инвестиции в кибербезопасность и постоянное обучение персонала также имеют решающее значение.

Список источников

1. Газета «Деловой Петербург» [Электронный ресурс]: – Режим доступа: https://www.dp.ru/a/2023/01/20/Tabletka_ot_utechki (Дата обращения 13.04.24).
2. TAdviser – портал выбора технологий и поставщиков: [Электронный ресурс]: – Режим доступа: https://www.tadviser.ru/index.php/Статья:Утечки_данных_в_медицинских_учреждениях (Дата обращения 13.04.24).
3. Статья 23 Конституции Российской Федерации [Электронный ресурс]: – Режим доступа: https://www.consultant.ru/document/ cons_doc_LAW_28399/ (Дата обращения 13.04.24).
4. Федеральный закон от 26.06.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»: [Электронный ресурс]: – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_220885/ (Дата обращения 14.04.24).
5. Правозащитный проект «Юраптека» [Электронный ресурс]: – Режим доступа: https://t.me/apteka_lawyer/35 (Дата обращения 13.04.24).
6. Searchinfrom [Электронный ресурс]: – Режим доступа: https://searchinform.ru/news/company-news/2023/03/02/v-2022-iz- edorganizacij-chasche-vsego-utekali-pdn-i-kommercheskaya-informaciya/ (Дата обращения 14.04.24).
7. Ежедневная британская газета The Daily Telegraph [Электронный ресурс]: – Режим доступа: https://www.telegraph.co.uk/ (Дата обращения 14.04.24).

Статья поступила в редакцию 19.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Короткова К. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Короткова К. В. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – написание статьи, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004

Применение методов машинного обучения для определения вредоносного трафика в шифрованном сетевом трафике

Алексей Дмитриевич Лавриенко[1]✉, Вячеслав Вячеславович Каштанов[2], Юрий Вадимович Алферов[3]
[1, 2, 3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1] nauchnajarota@yandex.ru✉, https://orcid.org/0009-0007-5540-2719
[2] slavakashtanov302@gmail.com, https://orcid.org/0009-0007-5540-2719
[3]alf-1996.alferov@ya.ru, https://orcid.org/0009-0007-5540-2719

Аннотация. В настоящее время большую часть сетевого трафика составляет шифрованный трафик. Доминирующим протоколом, обеспечивающим шифрование сетевого трафика, является протокол Transport Layer Security (TLS). В некоторых исследованиях сообщается, что до 60 % сетевого трафика использует TLS [1]. Вредоносные программные средства также используют шифрование для обеспечения конфиденциальности передаваемых данных. Эта тенденция усложняет обнаружение угроз, поскольку делает неэффективным использование глубокой проверки пакетов. Около 64 % компаний не могут обнаружить вредоносное содержимое в шифрованном трафике [2].

Ключевые слова: сетевой трафик, обнаружение вредоносного трафика, классификация.

Для цитирования: Лавриенко А. Д., Каштанов В. В., Алферов Ю. В. Применение методов машинного обучения для определения вредоносного трафика в шифрованном сетевом трафике // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 143–146.

Вступление

Подход, связанный с обнаружением вредоносных данных в сетевом трафике за счёт сопоставления с сигнатурами в современных системах обнаружения вторжений, является крайне неэффективным, когда речь идёт про зашифрованный трафик. На момент написания в популярной системе обнаружения вторжений Snort насчитывалось 3437 правил [3], из которых 3307 проверяют открытое содержимое пакетов. Только 48 правил системы Snort специфичны для шифрованного трафика, и из них только шесть служат для выявления вредоносных данных за счёт обнаружения самозаверенных сертификатов. Из оставшихся правил 19 обнаруживают атаки на уязвимость Heartbleed и другие атаки, направленные на конкретные программные реализации протокола TLS, а

23 обнаруживают открытый данные, передающиеся через порты, специфичные для трафика TLS. Эти цифры доказывают, что традиционные методы, основанные на сигнатурах, не способные выявлять вредоносные сессии в зашифрованном TLS-трафике. В связи с этим проблема обнаружения вредоносных сессий без необходимости дешифрования данных является актуальной. Для решения этой проблемы используют методы классификации.

Под классификацией трафика будем понимать процесс сопоставления трафика с приложениями, которые его создают. Классификация шифрованного трафика не предполагает его дешифрацию, информация, содержащаяся внутри пакетов, остаётся конфиденциальной и видна только пользователю и удалённому узлу. Из-за большого использования шифрованного сетевого трафика, возникла проблема обнаружения в нём вредоносного трафика. Для решения этой проблемы используют задачи классификации. Формально задачу классификации можно сформулировать следующим образом — необходимо определить отображение, при котором каждый поток шифрованного трафика, характеризующийся множеством признаков, соответствует только одному классу трафика: «вредоносному» или «не вредоносному». Для классификации трафика используют следующие подходы:

- на основе номеров портов;
- на основе полезной нагрузки;
- на основе IP-адреса источника.

Подходы на основе номеров портов и IP-адреса источника просты в реализации, однако обладают низкой точностью классификации. Поэтому предлагается использовать подход на основе статистики потоков, который основан на поиске отличительных характеристик потока трафика, таких как среднее значение пакета или статистика интервалов между пакетами в потоке.

Для реализации классификации трафика при помощи алгоритмов машинного обучения в данной статье предлагается использовать модель, представленную на рисунке 1.

Первым этапом решения задачи классификации сетевого зашифрованного трафика является его сбор. На этом этапе получаем исходные данные для обучения и тестирования модели. Для сбора трафика можно использовать программные или аппаратные средства — «снифферы». Они собирают весь трафик, проходящий через интерфейс, сохраняя полную структуру пакетов. Примерами таких снифферов могут быть Wireshark или tcpdump.

На этапе сбора трафика необходимо сформировать как не вредоносный трафик, так и вредоносный. Сбор можно осуществлять одновременно или последовательно, то есть сначала собрать не вредоносный трафик, а затем вредоносный, после чего собранный трафик объединить. Однако необходимо обеспечить возможность отличить вредоносный трафик от не вредоносного, например по IP-адресу источника.

Разбиение трафика на сессии необходимо для выделения признаков. Один пакет сам по себе не содержит много информативных сведений. На основе его параметров нельзя обнаружить классификационные признаки. С этой точки

зрения имеет значение несколько связанных пакетов — сессии. Сессия — совокупность пакетов, имеющих одинаковые значения полей «адрес назначения», «порт назначения», «адрес источника», «порт источника», либо со сменой адресов источника и назначения в некоторых ситуациях.

Рис. 1. Модель обнаружения вредоносных данных

В сессии можно выделить следующий набор признаков:

- средний размер пакета;
- среднеквадратичное отклонения размера пакета;
- средний размер полезной нагрузки;
- среднеквадратичное отклонение полезной нагрузки;
- количество пакетов;
- общий размер полезной нагрузки;
- общий размер пакетов;
- КПД — отношение общего размера полезной нагрузки к общему размеру пакетов и т. д.

Разметка трафика имеет важное значение для обучения. На этом этапе каждому классу трафика присваиваем идентификатор, который будет использоваться при обучении.

Далее необходимо заняться конструированием классификационных признаков. На их основе будет происходить классификация. Примером классификационных признаков могут быть размер в байтах всех пакетов в сессии или средний размер полезной нагрузки протокола транспортного уровня в потоке.

На следующем этапе необходимо произвести расчёт значений признаков и перейти к предварительной обработке данных. На этапе предварительной обработки данных происходит выделение значимых признаков, их нормирование или уменьшение размерности. Использование нормировки или уменьшения размерности необходимо для приведения всех признаков к одной размерности. Далее необходимо произвести машинное обучение с использованием одного из алгоритмов (Алгоритм k-ближайшего соседа, алгоритм решающие деревья, алгоритм случайного леса) после чего провести тестирование полученного классификатора на нескольких тестовых выборках. После проведения оценки делается вывод о том, можно ли полученный классификатор использовать для построения системы обнаружения вредоносных сессий в сетевом зашифрованном трафике или нет. Если его использовать нельзя, то необходимо пройти все шаги предлагаемой модели заново, увеличив объём выборки, изменив алгоритмы выбора значимых признаков или машинного обучения.

Список источников

1. Most Internet Traffic will be Encrypted by Year End. Here’s Why. [Электронный ресурс]. Режим доступа: http://fortune.com/2015/04/30/netflix-internet-traffic-encrypted.

2. Ponemon Report. [Электронный ресурс]. Режим доступа: https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018.

3. Snort: Community Rules. [Электронный ресурс]. Режим доступа: https://www.snort.org/downloads/community/ community-rules.tar.gz.

Статья поступила в редакцию 26.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Лавриенко А. Д. – оператор научной роты, Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Каштанов В. В.– заместитель начальника отдела опытной эксплуатации средств специальных воздействий, Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Алферов Ю. В. – инженер отдела опытной эксплуатации средств специальных воздействий, Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Лавриенко А. Д. – сбор материала, обработка материала (33 %).

Каштанов В. В. – идея, частичное написание статьи (34 %).

Алферов Ю. В. – написание статьи, научное редактирование текста (33 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Обзор организационных и технических решений защиты информации в медицинских учреждениях

Станислав Алексеевич Лосев[1]✉, Кирилл Андреевич Седаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] losef.vk@mail.ru✉, https://orcid.org/0010-0222-3244-5674
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624

Аннотация. Анализ организационных и технических мер в защите информации в медицинских учреждениях, обосновывающих актуальность и научную значимость этой проблемы в усовершенствовании безопасности хранения медицинских данных.

Ключевые слова: Информационная безопасность, контроль доступа к медицинским данным, анализ методов защиты персональных данных, угроза персональным данным, шифрование конфиденциальных данных.

Для цитирования: Лосев С. А., Седаков К. А. Обзор организационных и технических решений защиты информации в медицинских учреждениях // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 147–150.

Общую тенденцию защиты персональных данных определяет доктрина информационной безопасности Российской Федерации. Она определяет национальные интересы, включающие обеспечение прав человека и гражданина в использовании информации, сохранение культурных ценностей, и обеспечение информационной безопасности.

Рассмотрим набор организационных мер по защите информации, в частности нормативно-правовая база, направленная на решение этой задачи.

Реализация прав гражданина в медицинской сфере начинается с врачебной тайны, которую нельзя распространять третьим лицам, осуществляется с помощью создания, развития и эксплуатация федеральных государственных информационных систем в здравоохранении. Создается, развивается единая государственная система с обработкой персональных данных [1].

Необходимо принять меры, соответствующие третьему уровню защищенности, для защиты информации такие как:

- Обеспечить безопасность помещений, где хранится информационная система, чтобы предотвратить несанкционированный доступ.

- Гарантировать сохранность данных.

- Утвердить документ руководителем, определяющий лиц, имеющих доступ к данным, обрабатываемым в системе, для исполнения своих обязанностей.

- Использовать средства защиты информации, прошедшие проверку соответствия законодательству России, если требуется для снижения рисков.

- Назначить специалиста, ответственного за обеспечение безопасности данных в системе.

Добавление некоторых средств защиты, чтобы уровень защищенности соответствовал второму уровню:

- Предоставление разрешения к содержимому журнала событий, но только для уполномоченных лиц

Третий уровень защиты включает в себя:

- Регистрацию в электронном журнале событий.

- Структурная часть создается и внедряется в производство [2].

Для всех уровней защиты характерны некоторые принципы в рамках правовых методов защиты информации:

1) Соблюдение законности;

2) Комплексное обеспечение безопасности критической информационной инфраструктуры с участием органов исполнительной власти и субъектов критической информационной инфраструктуры;

3) Приоритет предотвращения компьютерных атак [3];

4) Защита информации от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, передачи и распространения;

5) Соблюдение конфиденциальности информации с ограниченным доступом.

Важность анализа угроз безопасности информации подтверждается информационным банком данных угроз безопасности информации на сайте bdu.fstec.ru.

Необходимо отметить, что анализ организационных и технических мер в защите информации в медицинских учреждениях имеет большое значение для обеспечения конфиденциальности медицинских данных. Важно быть в курсе последних тенденций в области информационной безопасности и соблюдать законодательство Российской Федерации, только таким образом можно эффективно защитить данные пациентов от угроз и несанкционированного доступа. Развитие и внедрение современных методов защиты информации необходимы для обеспечения безопасности в медицинской сфере. Примеры таких методов включают:

- Проверка личности и подлинности пользователей и объектов доступа;

- Использование биометрической аутентификации для доступа к компьютерным системам;

- Управление разрешениями пользователей на доступ к объектам;

- Установка различных уровней доступа к файлам и папкам в сети компании;

- Ограничение использования программного обеспечения;

- Блокировка доступа к определенным программам или веб-сайтам на рабочих компьютерах;

- Защита физических носителей информации с персональными данными;

- Хранение важных документов в сейфе или защита USB-накопителей паролем;

- Фиксация событий в области безопасности. Ведение журнала учета входов и выходов пользователей из системы.

В процессе обработки персональных данных в информационных системах важно проводить аутентификацию пользователей и объектов доступа. Доступ должен быть разделён на разные уровни для изоляции программной среды. Чтобы получить доступ к данным на машинных носителях, необходимо выполнить определённые меры безопасности. Если количество ошибок превысит допустимый порог, пользователю будет отказано в доступе, а информация о попытках входа будет передана администратору для анализа. Пользователи должны быть осведомлены обо всех действиях в информационной системе. Защита информации на носителях обеспечивается благодаря антивирусным мерам, направленным на обнаружение и предотвращение несанкционированного доступа [4].

Для эффективной реализации мер по защите персональных данных применяются следующие шаги:

- Анализ предыдущих ошибок информационной системы и выявление текущих уязвимостей для общей оценки результатов;

- Установка необходимого программного обеспечения;

- Регулярное изменение паролей и применение строгих правил их генерации;

- Мониторинг актуальности используемых технических средств.

Законодательно выделяются некоторые типы угроз по используемой уязвимости:

- Угрозы, которые выискивают лазейки и просчеты в защите системного программного обеспечения;

- Угрозы, анализирующие сетевые протоколы и существующими лазейками в них;

- Угрозы, направленные на уязвимости в организации технической защиты информации от несанкционированного доступа;

- Угрозы, передающиеся по каналам связи;

- Угрозы, которые могут быть осуществлены через уязвимости, обусловленные наличием технических каналов для утечки информации [5].

Список источников

1. Закон Российской Федерации "Федеральный закон "Об основах охраны здоровья граждан в Российской Федерации"" от 1.11.2011 № 323 // Собрание законодательства Российской Федерации. -2011 г. -с изм. и допол. в ред. от 21.11.2011.

2. Защита персональных данных. Новое в законодательстве: тенденции, вопросы практического применения в медицинских информационных системах // cyberleninka URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-novoe-v-zakonodatelstve-tendentsii-voprosy-prakticheskogo-primeneniya-v-meditsinskih-informatsionnyh (дата обращения: 14.03.2024).

3. Закон Российской Федерации "О безопасности критической информационной инфраструктуры Российской Федерации" от 12.07.2017 № 187 // Российская газета. - 2017 г. - с изм. и допол. в ред. от 02.06.2013.

4. Приказ ФСТЭК России "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 18.02.2013 № 21 // Официальный интернет-портал правовой информации. - 2013 г. - с изм. и допол. в ред. от 14.05.2020.

5. " Закон Российской Федерации "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15.02.2008 // Официальный интернет-портал правовой информации. – 2008.

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Лосев С. А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Лосев С. А. – сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – идея, научное редактирование текста, оформление (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.051

Исследование системы оценки ущерба от кибератак

Ирина Владимировна Марченко[1]✉, Анна Александровна Горлова[2]✉, Дмитрий Андреевич Лысов[3]✉
[1, 2, 3] Брянский государственный технический университет, Брянск, Россия
[1] snake2001@mail.ru✉, https://orcid.org/0009-0001-2023-3923
[2] anuytka32@gmail.com✉, https://orcid.org/0009-0000-1944-6588
[3] lysovdmitriia@gmail.com✉, https://orcid.org/0009-0003-9666-7191

Аннотация. Расширение киберпространства привело к переходу от обычной формы войны к кибервойне. Кибервойна, происходящая в современном мире, включает в себя многочисленные кибератаки, которые совершаются путем использования уязвимостей киберактивов. Это в первую очередь связано с увеличением числа активов и информации, хранящейся в этих активах. Такой ресурс, как «информация», является важным звеном, который в силах регулировать исход войны. Поэтому оценка ущерба играет важную роль в киберпространстве, а также может повлиять на провал или избежать его. В статье предлагается структура оценки ущерба от кибератак в период между физическими операциями. Рассматриваемая структура позволяет определить потенциальный или уже наступивший ущерб от кибернападений.

Ключевые слова: оценка ущерба, кибербезопасность, предотвращение кибернападения, кибератака, влияние угроз, метод анализа вреда.

Для цитирования: Марченко И. В., Горлова А. А., Лысов Д. А. Исследование системы оценки ущерба от кибератак // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 151–156.

В современном мире киберпространство развивается в потоке с информационным и коммуникационными технологиями. Такой вид развития предполагает преобразование в военной сфере, которое выражается кибервойной. Увеличение частоты осуществления кибератак напрямую зависит от увеличения числа активов и информации, которой владеют эти активы. Таким образом, в ходе военных действий информация может играть решающую роль. Отсюда можно сделать вывод, что, если кибератака происходит между физическими операциями, она может иметь непосредственное влияние на успешность выполнения операции. Таким образом важно оценивать потенциальный ущерб от кибернападений, случающихся между физическими операциями.

Предлагаемые в данной статье показатели системы оценки ущерба от кибератак в основном состоят из показателей эффективности и импактора (ударного элемента).

Ниже приводится метод, используемый для получения показателей деятельности активов и воздействия на них, которые являются показателями уровня активов.

В данной исследовательской работе эффективность активов зависит от оптимизации стоимости (Value Engineering). VE представляет собой метод проектирования, который внимательно исследует и проводит анализ структуры компонентов, учитывая их функциональные ценности и играя ключевую роль в управлении активами. Чтобы рассчитать существующую VE необходимо воспользоваться уравнением (1).

(1),

где V — цена;
F — функция;
C — затраты.

Если говорить иначе, Value Engineering оценивает, насколько эффективно достигается желаемая функция относительно затрат, рассматривая это как цену. В данной работе VE терпит изменения в том смысле, что чем больше активов будет использовано для выполнения различных функций по сравнению с числом уязвимых мест, тем более ценным оно будет является для миссий. Эффективность использования активов определяется значением стоимости имущества для выполнения миссии, и метод ее нахождения аналогичен формуле (2).

(2),

где A — стоимость эффективности активов;
V — фактор уязвимости;
F — количество ресурсов, используемых в функции;
α — экспертный оценочный балл.

Добавляя в формулу α, можно более четко оценить стоимость актива. Экспертный оценочный балл дает значение от 1 до 5, когда эксперт, выполняющий фактическую миссию, оценивает важность актива.

Метод, используемый для получения производительности и ударного элемента функции, которые являются показателями функционального уровня, заключается в следующем. Под выполнением функций понимается та степень, в которой функция используется для выполнения своей миссии.

Функциональный импактор (I_F) имеет два случая, которые влияют на миссию в качестве меры. Ударный элемент функционального времени (I_{FT}) — шкала для случая неисполнения в течение указанного времени, а ударный элемент функциональной точности (I_{FA}) — для случая, когда в результате выпол-

нения происходит ошибка. Метод получения функционального ударного элемента аналогичен уравнению (3).

(3)

Метод вычисления коэффициента влияния времени функции вычисляет время выполнения функции по сравнению со временем выполнения задачи. В случае если во время выполнения задачи совершается задержка, она может быть вычислена путём умножения времени отложенной функции на время отложенной задачи в импакторе функционального времени. Образец ударного элемента функционального времени можно наблюдать на рис. 1.

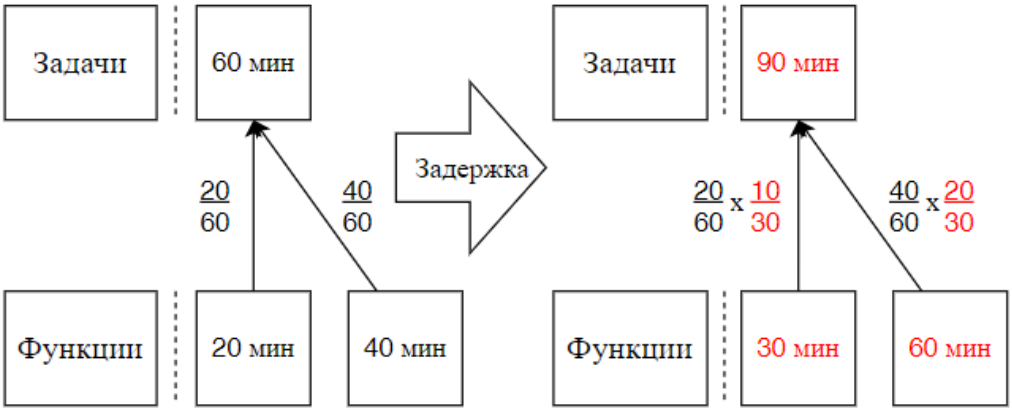


Рис. 1. Пример импактора функционального времени

Ударный элемент с функциональной точностью является мерилом для определения правильности выполнения той или иной функции. Когда активы, необходимые для выполнения этой функции, могут быть использованы в полном объеме, выполняется правильная миссия и начальный ударный элемент точности функции инициализируется до 1.

Выполнение миссии вычисляется перед получением кибератаки. Когда происходит кибератака, поврежденное имущество идентифицируется, а его эффективность снижается. Результаты деятельности миссии вновь рассчитываются путем расчета верхнего уровня, затронутого сокращением объема активов. Оценка ущерба выполняется путем сравнения значений производительности миссии до и после кибератаки.

Эксперимент

При выполнении данной работы был проведен эксперимент с использованием системы оценки ущерба от кибератак, предложенной в этой статье. В эксперименте были настроены сценарии миссий и атак, а результаты моделирования были проверены с использованием OMNeT++ \.

Во время проведения эксперимента был подготовлен сценарий полета для запроса непосредственной авиационной поддержки (далее по тексту — НАП). Операция НАП заключается в нападении на противника с самолетом, а также в надлежащем образе запроса операции НАП у армейского полка и, наконец, распространения приказа о воздушной миссии.

В целях разработки предложенной системы оценки киберущерба были проанализированы элементы сценария миссии. Задачи и функции были определены на основе проанализированных элементов, а имущество и сети были сконфигурированы. В таблице 1 определяются задачи сценариев миссии.

Таблица 1

Задачи сценариев миссии

Задача	**Информация**
1	Командир полка заполняет форму запроса на рассмотрение дела
2	Запрос НАП от полка к дивизии
3	Запрос НАП от дивизии в управление процессами безопасности (УПБ)
4	Запрос НАП от (УПБ) к центру воздушных операций (ЦВО)
5	Планирование работы НАП в ЦВО
6	Утверждение НАП и публикация приказа о воздушной миссии

В таблице 2 определяются функции сценариев миссии.

Таблица 2

Определение функций сценариев миссии

Номер	**Задача**	**Функция**
1	1	Анализ операционной среды
2	1	Идентификация цели
3	1	Определение режима работы НАП
4	1	Форма запроса на операцию НАП
5	2,3,4	Отправить запрос на операцию НАП
6	2,3,4	Анализ запроса на выполнение операции НАП
7	2,3,4,5	Доступный анализ мощности
8	5	Выбор реактивных истребителей
9	5	Написать приказ о воздушной миссии
10	6	Разработать приказ о воздушной миссии
11	6	Эксплуатация НАП с одобрением

Конфигурация активов, используемых в сценарии миссии, показана на рис. 2.

Рис. 2. Определение актива сценария миссии

На основе задач, функций и активов, полученных в результате анализа сценария миссии, результаты моделирования с использованием OMNeT++ были внесены в систему оценки ущерба от кибератак. В результате, производительность миссии до кибератаки составила 26372.

Вывод

Мероприятия по оценки ущерба от кибератак рекомендуется для компаний с особой настойчивостью. Подобные действия выполняются с целью понимания последствий атаки, улучшения безопасности и минимизации потенциальных убытков.

В статье была предложена структура оценки ущерба, причиненного миссии кибератакой. Если рассматривать кибератаку как поврежденный актив, в этом случае она является частью иерархической структуры. Система оценки ущерба, которая была исследована, включает в себя сравнение результатов до и после возникновения повреждений.

Предлагаемая система оценки позволяет быстро и количественно определить степень ущерба, произошедшего в ходе миссии. Это позволяет наглядно донести до командира причиненный ущерб, что поможет ему принять решение.

Список источников

1. D. Kim, D. Kim, D. Shin, D. Shin, and Y. Kim. Cyber battle damage assessment framework and detection of unauthorized wireless access point using machine learning – in Proc. Int. Conf. Frontier Comput. Singapore: Springer, 2018. – pp. 510–519.

2. S. Im, C. Lee, S. Hong, and S. Jeon. A method of defense scoring on trainee in cyber mock battle – in Proc. KICS, Jeju, South Korea, 2019. – pp. 833 –834.

3. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. – Москва, Вологда: Инфра-Инженерия, 2020. – 692 с. – ISBN 978-5-9729-0486-0.

4. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. – Москва: Техносфера, 2021. – 482 с. – ISBN 978-5-94836-612-8.

5. Менисов, А. Б. Технологии искусственного интеллекта и кибербезопасность: монография / А. Б. Менисов. – Москва: Ай Пи Ар Медиа, 2022. – 133 с. – ISBN 978-5-4497-1788-7.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Марченко И. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Горлова А. А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

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

Вклад авторов

Марченко И. В. – сбор материала, частичное написание статьи (34 %).

Горлова А. А. – идея, написание статьи (33 %).

Лысов Д. А. – обработка материала, научное редактирование текста (33 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.054

Оценка рисков для безопасности киберфизических систем на основе зависимости

Ирина Владимировна Марченко[1]✉, Анна Александровна Горлова[2], Дмитрий Андреевич Лысов[3]
[1, 2, 3] Брянский государственный технический университет, Брянск, Россия
[1] snake2001@mail.ru✉, https://orcid.org/0009-0001-2023-3923
[2] anuytka32@gmail.com, https://orcid.org/ 0009-0000-1944-6588
[3] lysovdmitriia@gmail.com, https://orcid.org/ 0009-0003-9666-7191

Аннотация. Нарушения безопасности в киберпространстве влияют на физическую среду. Число и разнообразие таких нападений на киберфизические системы (КФС) растет впечатляющими темпами. Во времена Индустрии 4.0 и киберфизических систем обеспечение безопасности от киберфизических атак является серьезной задачей, которая требует применения методов оценки рисков кибербезопасности, способных исследовать тесные взаимодействия и взаимозависимости между киберфизическими и физическими компонентами в таких системах. Однако существующие методы оценки рисков не учитывают эту специфическую характеристику КФС. В статье предлагается основанный на зависимостях, не зависящий от предметной области метод оценки рисков кибербезопасности, который использует исследуемую модель КФС, отражающую зависимости между компонентами системы. Предложенный метод определяет возможные пути атаки на критические компоненты КФС с точки зрения злоумышленника и определяет приоритетность этих путей в соответствии с риском их реализации, что позволяет защитникам определять эффективные средства контроля безопасности.

Ключевые слова: киберфизические системы, анализ пути атаки, оценка риска, безопасность, системы промышленного контроля, индустрия 4.0.

Для цитирования: Марченко И. В., Горлова А. А., Лысов Д. А. Оценка рисков для безопасности киберфизических систем на основе зависимости // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 157–172.

Объединение информационных и коммуникационных технологий (ИКТ) с операционными технологиями (ОТ) привело к созданию киберфизических систем. Несмотря на преимущества такого слияния в области мониторинга и контроля традиционных промышленных систем управления, взаимозависимости между кибер-элементами и физическими компонентами КФС создают новые виды рисков

для кибербезопасности, поскольку киберкомпоненты могут оказывать негативное воздействие на физическую среду, повышая тем самым риски для безопасности.

В КФС неожиданные события происходят главным образом из-за слишком запутанных связей и взаимозависимостей между ее неоднородными компонентами.

Разнообразие активов и взаимодействий между ними в КФС является дополнительной причиной, по которой традиционные методы оценки рисков не могут идентифицировать киберфизические атаки, поскольку сфера охвата анализа этих методов ограничивается ИТ-системами. Традиционные КФС создавались как физически и логически изолированные системы, без каких-либо механизмов безопасности, за исключением мер физической безопасности. Позднее эти системы были постепенно расширены за счет сетевой функциональности и могли подключаться к Интернету и обеспечивать дистанционный мониторинг и контроль [5].

Стандарт IEC TS 62351-1:2007 гласит, что обеспечение 100 % безопасности для каждого компонента системы не только считается дорогостоящим и непрактичным решением, но и может препятствовать предприятиям, пытающимся использовать механизмы безопасности. Поэтому методы оценки рисков для КФС должны уделять особое внимание повышению эффективности и недопущению ненужного анализа, который не имеет никакого значения для повышения безопасности системы.

Каждое нападение состоит из различных этапов, которые должны проходить шаг за шагом, чтобы достичь своей конечной цели, известной как «цепь уничтожения» [6]. Другими словами, каждое нападение можно рассматривать как цепь зависимостей. Поэтому для того, чтобы помешать злоумышленнику достичь своей цели и повлиять на систему, достаточно разорвать звенья этой цепи. Только одно нарушение пути атаки может защитить систему. Соответственно, можно определить новое понятие «сквозной» защиты, в котором «сквозная» защита и безопасность подразумевают отсутствие цепочки зависимости между двумя соответствующими компонентами.

Киберфизические системы различны по своему характеру; это следует учитывать при разработке метода, основанного на анализе путей атаки. В отличие от ИТ-систем, в КФС наиболее часто объектом сложных кибератак является воздействие на функциональность промышленных систем управления.

Признавая преимущества использования анализа путей атаки для получения четкой картины возможных атак против КФС и учитывая ее специфические атрибуты, в статье предлагается новый, основанный на зависимости, метод оценки риска. Этот метод сначала выявляет важнейшие активы системы, а затем обнаруживает цепочки зависимостей между соответствующими активами, которые могут быть использованы злоумышленниками для совершения нападения на каждую из целей. Предлагаемый метод представляет собой комплексную методику, которая рассматривает как топологические, так и функциональные взаимосвязи между компонентами системы как прямые, так и скрытые зависимости в рамках КФС, чтобы обеспечить целостную оценку риска. Он использует моделирование для визуализации рисков безопасности, чтобы облегчить сотрудничество между экспер-

тами по ИТ и ОТ в КФС. Это помогает защитникам понять намерения злоумышленников, тем самым направляя их использовать соответствующие подходы для уменьшения рисков. Предлагаемый метод не зависит от предметной области и был разработан для охвата всех КФС в различных областях, таких, как судоходство, авиация и энергетика. В этой статье продемонстрирована работа предложенного метода на примере КФС в области энергетики.

Основной вклад данной работы заключается в следующем: предлагается основанный на зависимости метод оценки риска для определения путей целенаправленных атак в КФС, который учитывает киберфизическую и физико-кибернетическую взаимозависимости внутри систем. Предлагаемый метод:

- облегчает сотрудничество между экспертами по ИТ и ОП для выявления нежелательных событий с точки зрения безопасности;
- раскрывает сложные киберфизические атаки, используя обратнный анализ, чтобы понять намерения злоумышленников;
- повышает эффективность анализа пути атаки, заменяя слепой анализ целенаправленным обратным анализом;
- является реалистичным методом расчета риска и оценки вероятности и воздействия на основе показателей, которые охватывают требования как ИТ, так и ОТ.

Методы оценки киберрисков для КФС чаще всего зависят от конкретной области, поскольку они должны учитывать безопасность как фактор воздействия, дополняющий «традиционные» факторы воздействия — конфиденциальность, целостность и доступность. Именно поэтому вопросы охраны и безопасности КФС изучаются совместно.

Существующие методы оценки рисков для КФС учитывают только кибер-часть или физическую часть по отдельности. Как упоминалось в [4], необходим целостный подход к изучению киберфизических систем, который мог бы регулировать сложную связь между физическим процессом и инфраструктурой ИТ.

Методология оценки рисков

Предлагаемая методология оценки рисков разделена на четыре этапа. Для проведения целостной оценки рисков КФС прежде всего необходимо смоделировать систему, найти связи и зависимости между компонентами системы (1 этап). Это облегчит идентификацию цепочек зависимостей и использование методологии «галстука-бабочки», которая будет описана позднее, на 3 этапе. После того как система смоделирована, определяется и ранжируется критичность компонентов системы (2 этап). На 3 этапе по каждому целевому компоненту, выбранному в соответствии с результатами второго этапа, проводится первый глубокий поиск для извлечения цепочек зависимостей. Затем определяются все нежелательные события для целевых компонентов и выясняется, сможет ли каждая выделенная цепочка зависимостей действительно привести к этому нежелательному событию. Для расчета риска собираются соответствующие показатели для оценки вероятности и воздействия, как с точки зрения безопасности, так и охраны (3 этап). После

расчета риска каждой выявленной цепочки зависимостей оцениваются результаты.

Первый этап: моделирование системы

Для представления комплексной модели КФС, пригодной для оценки рисков кибербезопасности, необходимо учитывать как топологические, так и функциональные аспекты системы. Таким образом, первым шагом является выявление связей в рамках системы и выявление кибер- и физических взаимодействий в системе, которые обозначают соответственно потоки данных и материальные потоки в системе. Используемый метод — теория графов [3]. Здесь КФС моделируется как ориентированный граф G(V, E), в котором V является множеством вершин (узлов), представляющих компоненты системы, а E — это множество граней (связей), представляющих взаимосвязи между компонентами системы.

Второй этап: определение и ранжирование важнейших компонентов системы

Цель этого шага заключается в том, чтобы классифицировать критичность компонентов системы как потенциальную цель кибератак как с системной, так и с организационной точки зрения.

Согласно [2] методу оценивается вклад компонентов системы, как звеньев, так и узлов, в сохранение функциональности системы и возможности подключения.

На системном уровне основное внимание уделяется исключительно характеристикам и роли компонентов, в то время как на организационном уровне следует рассматривать различные аспекты. Для определения важности каждого компонента на организационном уровне заинтересованные стороны используют одну из следующих ценностей:

- 1 — низкая важность;
- 2 — средняя важность;
- 3 — высокая важность.

Поскольку критичность организационного уровня измеряется в качественном отношении, ее следует надлежащим образом масштабировать до агрегирования с учетом критического уровня системы. Общая критичность компонента Xi вычисляется на основе формулы (1), в которой COrg и CSys ссылаются на критичность организационного и системного уровней, соответственно.

$$C_{Total}(X_i) = \frac{C_{Org}(X_i)}{\max(C_{Org})} \times \max \quad (1)$$

Третий этап: оценка рисков, связанных с зависимостью

Данный шаг направлен на выявление возможных цепочек зависимостей между компонентами системы, которые могут быть использованы злоумышленниками для достижения своей цели. В идеальной ситуации оценка рисков, начинается с наиболее важных компонентов, ранжированных на втором этапе, и продолжается до уровня критичности, который удовлетворяет владельцев систем.

Третий этап начинается с выбора одного из важнейших компонентов системы в качестве целевого узла Xi. Далее, все нежелательные события UE(Xi), которые могут повлиять на узел Xi определены.

Затем выбирается одно из нежелательных событий, которое может повлиять на узел X_i (например, $UE_{j(Xi)}$). При выполнении поиска в глубину обнаруживаются все некруговые цепочки зависимостей, которые заканчиваются на X_i.

Для проведения анализа рисков кибербезопасности вместе с цепочкой зависимостей применяется концепция галстука-бабочки. Такая концепция широко используется в управлении рисками безопасности для выявления коренных причин и последствий опасностей. Как показано на рис. 1, правая сторона галстука-бабочки в работе соответствует нежелательным событиям ($UE_{j(xi)}$), которые могут произойти, левая сторона указывает причины (F_{UEj}), которые могут привести к этим нежелательным событиям, а центральный узел отмечает изучаемый объект (X_i).

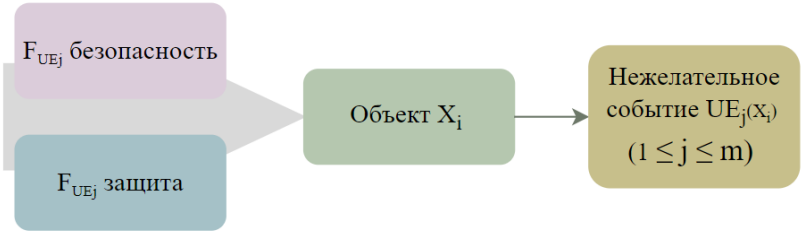


Рис. 1. Галстук-бабочка

Предположим, что для критического узла X_i, $UE_{(Xi)} = \{UE_{1(Xi)},\ldots, UE_{m(Xi)}\}$ – есть m возможных нежелательных событий. Чтобы обнаружить пути атаки, нацеленные на узел X_i, необходимо начать с узла X_i и выбрать первое нежелательное событие ($UE_{1(Xi)}$). Затем проверяются потенциальные опасности и угрозы, которые могут привести к этому событию, рассматривая узел X_i, узел X_{i-1} и связь (X_{i-1}, X_i) как соответствующую поверхность атаки X_i.

Если найдена причина $UE_{1(Xi)}$ (F_{UE1}), происходит перемещение на один шаг влево от цепи и повторяем тот же процесс для следующего узла (X_{i-1}). F_{UE1} — режим уязвимости или отказа, который может вызвать $UE_{1(Xi)}$. (рис. 2).

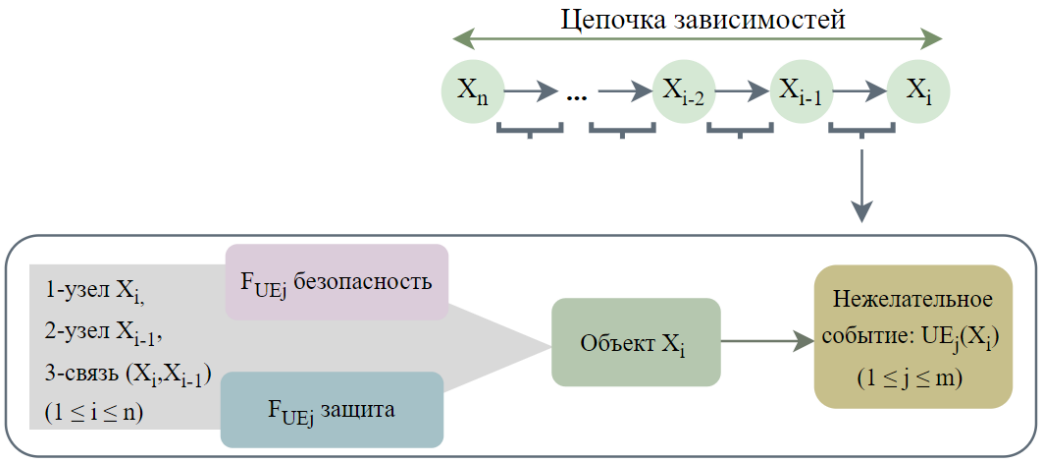


Рис. 2. Цепочка зависимостей и совместный анализ рисков для безопасности

Принимая во внимание актив X_i, F_{UEj} указывает на предварительное условие j, которое, если выполнится, позволит осуществить постусловие $UE_{j(Xi)}$. С точки зрения безопасности, предварительное условие определяет режимы отказа и рассматривает повреждение имущества, включая X_i, X_{i-1} и связь (X_{i-1}, X_i), в то время как постусловие показывает окончательные эффекты и последствия материализации каждого предварительного условия.

Из-за того, что цель оценки риска ясна с самого начала, здесь пути атаки и впоследствии риск для каждого целевого компонента X_i можно рассчитать отдельно без необходимости исследовать все взаимодействия и зависимости внутри системы.

Для ясности приведен пример простого графа (рис. 3). Здесь предполагается заинтересованность в обнаружении путей атаки, которые заканчиваются на X_1 и вызывают $UE_{1(x1)}$.

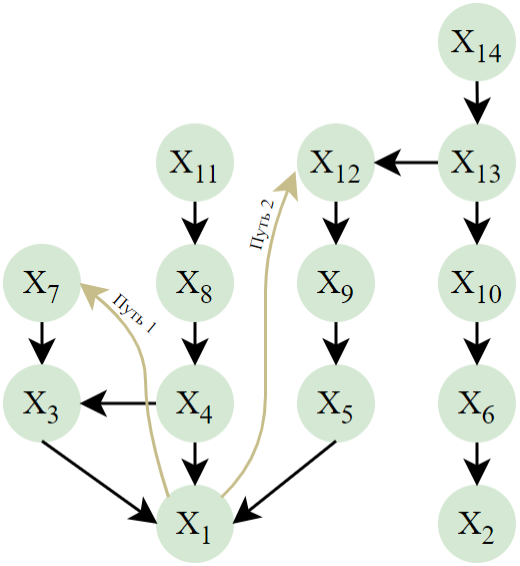


Рис. 3. Простой пример обнаружения путей атаки

Предположительно уязвимости и режимы отказов существуют между $X_7 \rightarrow X_3 \rightarrow X_1$ и $X_{12} \rightarrow X_9 \rightarrow X_5 \rightarrow X_1$, которые могут быть использованы злоумышленниками и, следовательно, привести к $UE_{1(Xi)}$. Ссылаясь на предположение, которое может привести к $UE_{1(Xi)}$ из X_5, исследование из узла X_5 будет прекращено и этот узел будет удален из списка. Расследование продолжается до тех пор, пока не будут найдены пути 1 и 2.

Последний пункт третьего этапа заключается в расчете риска. Для вычисления риска каждого пути атаки, который может привести к $UE_{j(Xi)}$, следует рассчитать вероятность материализации этого пути. Для критического узла X_0, риск материализации пути атаки $X_n \rightarrow \ldots \rightarrow X_1 \rightarrow X_0$ с длиной n вычисляется следующим образом:

$$R_{Path} = L_{X_n,\ldots,X_0} \times I_{X_1,X_0} = \prod_{i=} \quad (2)$$

где R_{Path} — риск этого пути атаки;
L_i и I_i — вероятность и влияние нацеливания X_0, соответственно.

Однако, может быть несколько путей атаки к критическому узлу X_i [1]. Чтобы отразить это при вычислении риска каждого целевого узла X_i, используется формула (3):

R (3)

где $P(X_i)$ — вероятность доступа к узлу X_i, который отображает число путей атаки; $Impact(X_i)$ — результат воздействия, возникающий при $UE_{j(Xi)}$.

Из-за того, что пути атак для каждого целевого узла X_i взаимно независимы, вероятность доступа к X_i через хотя бы один из доступных путей атаки вычисляется на основе формулы (4):

$$P(X) = 1 - \prod_{i=1}^{k}\left(1 - p(path_i)\right) = 1 - \prod_{i=1}^{k}(1 \quad (4)$$

где $p(path_i)$ — вероятность пути атаки i.

После этого остается определить вероятность и воздействие. Как упоминалось выше, основная цель предлагаемого метода заключается в содействии одновременному анализу рисков в области безопасности и охраны в КФС. Для этого необходимо рассчитать вероятность и воздействие нежелательного события на основе показателей, которые способствуют как безопасности, так и защищенности. Для проведения комплексной оценки рисков для КФС, которая охватывает как компоненты ИТ, так и компоненты ОТ, необходимо оценивать воздействие на основе обоих подходов.

Принимая во внимание как кибер-, так и физические аспекты КФС, для определения вероятности оцениваются 3 показателя, а именно: вектор доступа, необходимые знания/навыки и внешние факторы. Метрика вектора доступа показывает, как злоумышленник может получить доступ к целевому компоненту и насколько это будет сложно. Метрика необходимых знаний/навыков отражает сложность атаки. В метрике внешних факторов показана атака на загрузку ложных данных, в которой злоумышленникам необходимо отправлять ложные данные в определенный промежуток времени, чтобы иметь возможность поставить систему в нестабильную ситуацию. В таблицах 1 и 2 содержатся подробные указания в отношении присвоения значений элементам риска.

Таблица 1

Вероятность

Метрика	**Категория**	**Описание**	**Значение**
Вектор доступа	Удаленный	Удаленный доступ к уязвимому компоненту или ссылке извне системы (интернет)	Высокая
	Соседний	Доступ к уязвимому компоненту или ссылке из соседней подсистемы/подсети в рамках той же системы	Средняя

Метрика	Категория	Описание	Значение
	Локально-физический	Физический доступ к уязвимому компоненту или ссылке из той же подсистемы/подсети в той же системе	Низкая
	Локально-кибернетический	Кибер-доступ к уязвимому компоненту или ссылке из той же подсистемы/подсети в той же системе	Средняя
Необходимые знания/навыки	Высокие	Успешная атака требует высокого уровня знаний и мастерства	Высокая
	Средние	Злоумышленник со средним уровнем знаний/навыков может успешно атаковать уязвимый компонент или ссылку	Средняя
	Отсутствуют	Случайные сбои или атаки вслепую влияют на уязвимый компонент или ссылку	Высокая
Внешние факторы	Требуемые	Для успешной атаки требуются внешние факторы (определенные возможности, привилегии)	Высокая
	Отсутствуют	Атака может быть проведена в любое время без каких-либо предварительных требований	Высокая

Таблица 2

Влияние на изменение

Метрика	Описание
Экономический эффект	Значимость экономических потерь и/или ухудшения качества продукции или услуг
Общественный эффект	Гибель людей, болезни, серьезные травмы, эвакуация
Воздействие на окружающую среду	Воздействие на население и окружающую среду
Конфиденциальность	Кибернетический домен (ИТ-ресурсы в киберфизической системе)
	Физический домен (другие ресурсы в киберфизической системе)
Доступность	Кибернетический домен (ИТ-ресурсы в киберфизической системе)
	Физический домен (другие ресурсы в киберфизической системе)
Целостность	Кибернетический домен (ИТ-ресурсы в киберфизической системе)
	Физический домен (другие ресурсы в киберфизической системе)

Авторы в [7] пояснили, что баллы вероятности и воздействия равны средним показателям их составляющих. Поэтому вероятность и последствия использования уязвимости или опасности в цепочке зависимости рассчитываются на основе сред-

них соответствующих показателей, определенных в таблицах 1 и 2, следующим образом:

(5)

. (6)

Количество баллов от 0 до 1.

Оценка важности выявленных путей атаки

Для каждого выбранного узла X_i в третьем этапе все нежелательные события $UE_{(Xi)}$ извлекаются, а затем шаги, повторяются, чтобы найти все связанные пути атаки и вычислить соответствующий риск. После завершения процесса третьего этапа необходимо оценить результаты и расставить приоритеты компонентов с более высокой степенью риска, с тем чтобы были приняты надлежащие меры по уменьшению или регулированию риска.

Помимо риска, связанного с каждым целевым компонентом Xi, еще одним фактором является воздействие на периметр. Согласно таблице 2, удар по периметру указывает на то, в какой степени сбой/неисправность одного узла может повлиять на систему. Удар по периметру каждого пути атаки можно вычислить на основе следующего уравнения:

$$P \cdot Impact_p \quad (7)$$

Анализируя результат третьей фазы, можно определить общие предварительные условия и компоненты, которые появляются в различных путях атаки. Это поможет разбить максимальное количество путей атаки с меньшими усилиями, и, следовательно, это повышает безопасность систем.

Описание

Эта система представляет собой простое приближение энергосистемы, которая состоит из четырех сетевых зон: корпоративной сети, демилитаризованной зоны (ДМЗ), полевой сети и сети управления для контроля критическими инфраструктурными компонентами в энергосистеме. Сеть управления соединяет контрольный уровень с модулями управления более низкого уровня. Корпоративная сеть с сетью управления позволяет операторам мониторить и контролировать операции за пределами полевой сети. ДМЗ является отдельным сегментом сети, который соединяется непосредственно с брандмауэром. Физический процесс системы осуществляется в полевой сети. Полевая сеть в исследовании представляет собой трехшинную двухлинейную систему передачи. Это модифицированная версия системы IEEE с девятью шинами и тремя генераторами, которая представляет собой процесс генерации и передачи энергии конечным пользователям и включает в себя несколько компонентов.

Анализ рисков

Основываясь на описании системы и графическом рассмотрении тематического исследования, был предоставлен дираф системы, как показано на рис. 4.

Затем следует определить критичность компонентов системы. С этой целью метод [2] применяется для измерения значения каждого компонента с точки зрения системного уровня (например, C_{sys}). Результат этого шага показан во втором столбце таблицы 3. В третьем столбце этой же таблицы указывается организационный уровень критичности каждого компонента, который определяется знаниями экспертов в данном разделе. Наконец, используя C_{sys} и C_{Org}, вычисляется общая критичность компонентов на основе формулы (1).

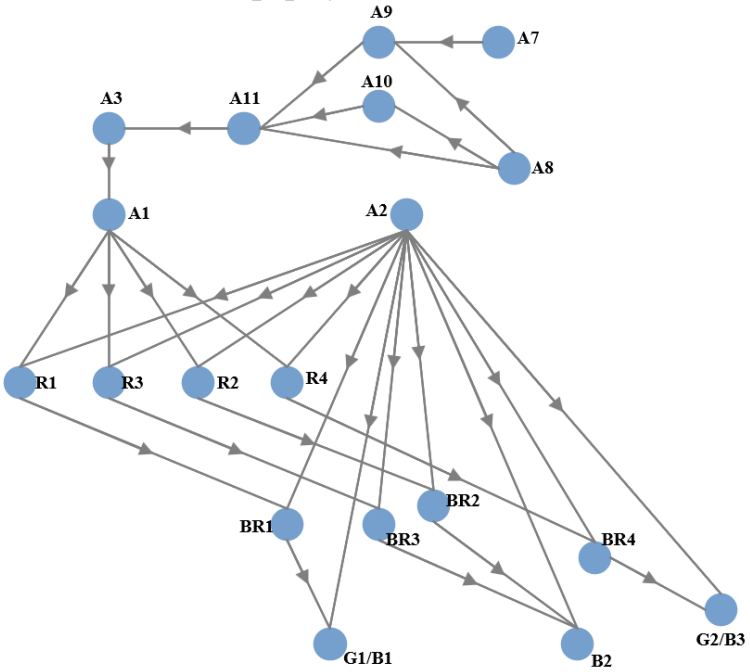


Рис. 4. Дираф системы

Таблица 3

Значение критичности компонентов системы

Идентификатор узла	**C_{sys}**	**C_{org}**	**C_{total}**
B1/G1	0.1693	3	2.1484
BR1	0.357	2	1.6764
R1	0.4916	2	1.811
B2	0.2829	2	1.6023
BR2	0.3423	2	1.6617
R2	0.4761	2	1.7955
BR3	0.3423	2	1.6617
R3	0.4761	2	1.7955

Идентификатор узла	C_{sys}	C_{org}	C_{total}
B3/G2	0.1693	3	2.1484
BR4	0.357	2	1.6764
R4	0.4916	2	1.811
A1	1.959	3	3.9381
A2	0.7322	3	2.7113
A3	1.9791	3	3.9582
A7	0.7977	1	1.4574
A8	1.1544	1	1.8141
A9	1.1584	2	2.4778
A10	0.9474	2	2.2668
A11	1.9228	2	3.2422

Согласно таблице, узлы {G1, G2, A1, A2, A3, A9, A10, A11} имеют более высокий уровень критичности по сравнению с другими компонентами системы. G1 был выбран как компонент для запуска третьей фазы и вычисления риска.

Отключение генератора и его повреждение можно рассматривать как два нежелательных события. Предполагается, что противники не имеют физического доступа к G1. Одной из существенных причин, приводящих к повреждению генератора в энергосистеме, является неправильная синхронизация ($UE_{(G1)}$).

После этого должны быть извлечены цепочки зависимостей, которые заканчиваются на G1 и проверены, могут ли отношения между узлами в каждой цепочке зависимостей формировать пути атаки.

Далее была рассмотрена поверхность атаки BR1, чтобы найти возможные причины изменения состояния BR1. R1 рассматривается только как соседний узел. В этом случае злоумышленник (I4) может ввести ложные данные в BR1, используя ссылку (R1, BR1). Путь 2 в таблице 4 относится к ручному доступу I4. Используя уязвимости, извлекаются соответствующие пути атаки, которые приводят к нежелательному событию $UE_{(G1)}$. Результаты перечислены в табл. 4.

Таблица 4

Пути атаки на G1

№	Путь
1	I4→BR1→G1
2	I4→R1→BR1→G1
3	A6→A7→A9→A11→A3→A1→R1→BR1→G1
4	A6→A8→A10→A11→A3→A1→R1→BR1→G1

№	Путь
5	A6→A8→A11→A3→A1→R1→BR1→G1
6	A6→A8→A9→A11→A3→A1→R1→BR1→G1
7	I2→A7→A9→A11→A3→A1→R1→BR1→G1
8	I2→A8→A10→A11→A3→A1→R1→BR1→G1
9	I2→A8→A10→A11→A3→A1→R1→BR1→G1
10	I2→A8→A9→A11→A3→A1→R1→BR1→G1
11	I3→A9→A11→A3→A1→R1→BR1→G1
12	I3→A10→A11→A3→A1→R1→BR1→G1
13	I3→A11→A3→A1→R1→BR1→G1
14	I1→A1→R1→BR1→G1
15	I1→HMI→R1→BR1→G1
16	I1→HMI→BR1→G1
17	I4→R3→A1→R1→BR1→G1

Путь 17 подчеркивает необходимость учета как топологических, так и функциональных зависимостей при оценке рисков. После определения соответствующих путей атаки, можно определить вероятность и воздействие, связанные с каждым шагом обозначенных путей атаки, на основе руководства в таблицах 1 и 2 соответственно.

Затем можно вычислить риск и воздействие по периметру каждого пути атаки (табл. 5) на основе уравнений (2) и (7).

Таблица 5

Риск и влияние на периметр выявленных путей атаки

Путь	Вероятность	Влияние на периметр	Риск на пути атаки
1	0.0012	0.0723	0.0032
2	0.0013	0.0718	0.0035
3	0.134	0.0659	0.3485
4	0.134	0.0723	0.3485
5	0.0583	0.0723	0.1515
6	0.134	0.0718	0.3485
7	0.1142	0.0659	0.2968
8	0.1142	0.0723	0.2968
9	0.0496	0.0649	0.1291

Путь	Вероятность	Влияние на периметр	Риск на пути атаки
10	0.1142	0.0645	0.2968
11	0.0496	0.0586	0.1291
12	0.0496	0.0449	0.1291
13	0.0292	0.0488	0.0759
14	0.0055	0.0381	0.0144
15	0.0035	0.0352	0.0092
16	0.0021	0.0244	0.0054
17	0.0053	0.0562	0.0138

Риск $UE_{(G1)}$ для компонента G1 рассчитывается на основе формулы (3) следующим образом:

$$R(G1) = P(G1) \times Impact(G1) = \left(1 - \prod_{i=1}^{k}\left(1 - p(path_i)\right)\right) \times Impact(G1) =$$

$$= \left(1 - \left((1 - 0.0012) \times \ldots \times (1 - 0.0053)\right)\right) \times 2.6 = 0.6524 \times 2.6 = 1.6962 \quad (8)$$

На рис. 5 также показан риск каждого пути атаки.

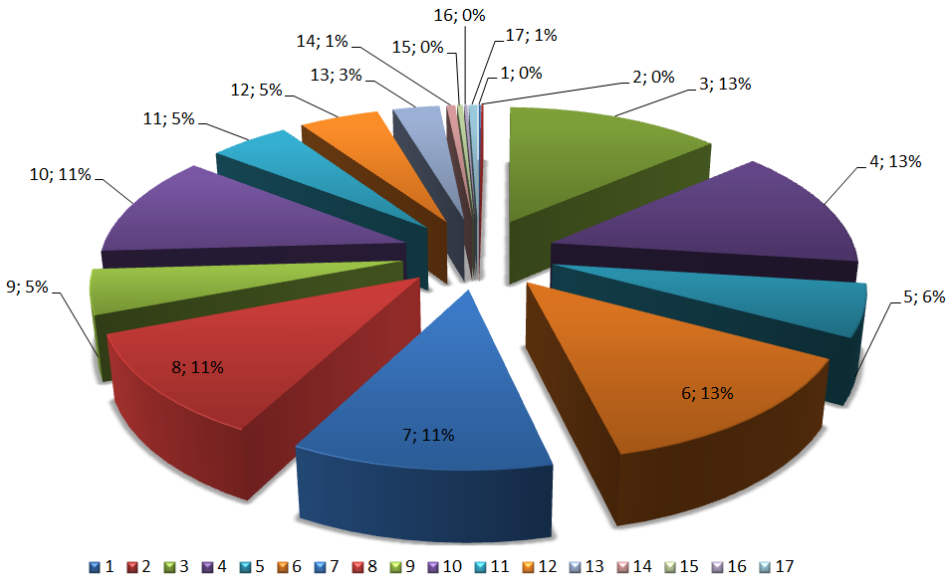


Рис. 5. Риск, связанный с каждым способом атаки

Сравнение выявленных путей атаки на основе вероятности облегчает определение наиболее вероятной точки проникновения и значительных путей атаки, которые могут привести к $UE_{(G1)}$. Вероятность нацеливания G1 через A6 и I2 выше, чем у остальных потенциальных точек входа. Эта информация имеет огромное значение для управления рисками в системе.

Преимущества предложенного метода станут более очевидными, когда он будет применяться для оценки риска нескольких компонентов системы. Поэтому реле R1 будет считаться и другим критическим компонентом в системе. Чтобы рас-

считать риск R1, предполагается, что злоумышленники хотят изменить настройки реле R1. Следуя тому же подходу, который описан ранее, были извлечены соответствующие пути атаки к R1 (табл. 6).

Таблица 6

Пути атаки на R1

№	Путь
1	A6→A7→A9→A11→A3→A1→ A2→R1
2	A6→A8→A10→A11→A3→A1→ A2→R1
3	A6→A8→A11→A3→A1→ A2→R1
4	A6→A8→A9→A11→A3→A1→ A2→R1
5	I2→A7→A9→A11→A3→A1→ A2→R1
6	I2→A8→A10→A11→A3→A1→ A2→R1
7	I2→A8→A11→A3→A1→ A2→R1
8	I2→A8→A9→A11→A3→A1→ A2→R1
9	I3→A9→A11→A3→A1→ A2→R1
10	I3→A10→A11→A3→A1→ A2→R1
11	I3→A11→A3→A1→ A2→R1
12	I1→ A2→R1
13	I4→R1

Затем рассчитывается вероятность каждого пути и влияние нацеливания на R1, результат показан в табл. 7.

Таблица 7

Риск и периметр вероятности атаки пути на R1

Путь	Вероятность	Влияние на периметр	Риск на пути атаки
1	0.1362	12.6	0.2996
2	0.1362	12.5	0.2996
3	0.0592	1.3	0.1302
4	0.1362	12.6	0.2996
5	0.116	12.6	0.2552
6	0.116	12.5	0.2552
7	0.0504	11.3	0.1109
8	0.116	12.6	0.2552

Путь	Вероятность	Влияние на периметр	Риск на пути атаки
9	0.0504	11.1	0.1109
10	0.0504	11.1	0.1109
11	0.0297	9.8	0.0653
12	0.0021	5	0.0046
13	0.0008	2.2	0.0018

Принимая во внимание выявленные пути атаки, вероятность и влияние нацеливания на R1, можно вычислить риск нацеливания на R1 на основе уравнения (3) следующим способом:

$$R(R1) = P(R1) \times \text{Impact}(R1) = \Big(1 - \big((1 - 0.1362) \times \ldots \times (1 - 0.0008)\big)\Big) \times \times$$

$$2.2 = 0.653 \times 2.2 = 1.4366 \quad (9)$$

Теперь, сравнивая риск G1 с риском R1, можно понять, что в этой системе G1 требует большего внимания, чем R1, что разумно, поскольку G1 должен поставлять электроэнергию в систему. Этот результат также соответствует уровню критичности G1 по сравнению с R1.

Заключение

В статье рассматриваются кибер- и физические аспекты КФС для оценки рисков кибербезопасности. Предложенный метод облегчает сотрудничество между операторами ИТ и ОТ и, следовательно, облегчает идентификацию трудноопределимых и сложных путей атаки на КФС. Это стало возможным благодаря оценке риска того, что пути нападения, ведущие к целевому компоненту КФС, материализуются. Для каждого критического компонента системы извлекаются все связанные цепочки зависимостей и изучаются возможные сценарии атаки для каждого пути. Для всех критических компонентов в цепочке зависимостей исследуются сам критический компонент, его соседний узел и входящее звено, чтобы обнаружить все возможные дефекты. Для повышения эффективности анализа пути атаки выбирается метод обратного отслеживания. Была продемонстрирована работа предложенного метода с использованием, в качестве примера КФС, реалистичной энергосистемы.

Предложенный метод помогает владельцам систем и операторам устанавливать свою цель с самого начала анализа и выводить только те пути, которые могут привести к нежелательным событиям, затрагивающим целевой компонент. Информация, полученная с помощью предлагаемого метода оценки рисков, может быть дополнительно использована для разработки комплексного метода управления рисками для КФС.

Список источников

1. Akbarzadeh A., Katsikas S. Identifying and analyzing dependencies in and among complex cyber physical systems – Sensors 21(5), 2021.

2. Akbarzadeh A., Katsikas S. Identifying critical components in large scale cyber physical systems – Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, 2020. – pp. 230–236.

3. Akbarzadeh A., Pandey P., Katsikas S. Cyber-physical interdependencies in power plant systems: a review of cyber security risks – 2019 IEEE Conference on Information and Communication Technology, 2019. – pp. 1–6.

4. Skopik F., Smith P. D. Smart grid security: Innovative solutions for a modernized grid – Syngress, 2015.

5. Stellios I., Kotzanikolaou P., Psarakis M., Alcaraz C. Risk assessment for IoT-enabled cyber-physical systems – Advances in Core Computer Science-Based Technologies: Springer, 2021 – pp. 157–173.

6. Wolf M., Serpanos D.N. Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems – Springer, Berlin, 2020.

7. Zinsmaier S., Langweg H., Waldvogel M. A practical approach to stakeholder-driven determination of security requirements based on theGDPR and common criteria – 6th International Conference on Information Systems Security and Privacy, 2020. – pp. 473–480.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Марченко И. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Горлова А. А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

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

Вклад авторов

Марченко И. В. – сбор материала, частичное написание статьи (33 %).

Горлова А. А. – идея, написание статьи (33 %).

Лысов Д. А. – обработка материала, научное редактирование текста (34 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.52

Защита информации в интересах войск радиоэлектронной борьбы

Даниил Александрович Матвеев[1]✉, Егор Дмитриевич Колосов[2], Артем Сергеевич Ткачёв[3], Виктор Васильевич Шатских[4]
[1, 2, 3, 4] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1, 2, 3, 4] nauchnajarota@yandex.ru, https://orcid.org/0009-0007-5540-2719

Аннотация. Защита информации является одним из самых важных и главных направлений в современном мире и её участие в обществе становится всё более заметным. Защита информации позволяет сохранить необходимые данные от случайной потери, защитить от несанкционированного доступа, сберечь от кражи злоумышленников и это лишь некоторые примеры, которые особенно актуальны на сегодняшний день.

Ключевые слова: Защита информации, радиоэлектронная борьба, система защиты.

Для цитирования: Матвеев Д. А., Колосов Е. Д., Ткачёв А. С., Шатских В. В. Защита информации в интересах войск радиоэлектронной борьбы // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 173–175.

Современное общество развивается с космической скоростью, и наука не стоит на месте. С каждым днем существует все больше и больше способов обхода защиты информации. Но также и выстроенная система защиты информации не стоит на месте и развивается с каждым днем. Появляется альтернативная защита на основе развивающихся вариантов атаки хакеров.

В Российской армии существуют очень много информации, требующей полной и комплексной защиты. Самая главная информация в Российской армии, подлежащая защите — это государственная тайна. Понятие государственной тайны определено согласно статье 2 Закона Российской Федерации от 21 июля 1993г. № 5485 – I «О государственной тайне» [1]. Государственная тайна — информация, имеющая особенную важность для государства, доступ к которой строго ограничен и за разглашение которой предусмотрена уголовная ответственность. Информация, относящаяся к государственной тайне [22]:

- о вооружённых силах;
- военной промышленности;
- научной деятельности, имеющей военной значение;
- спецслужбах;

• непубличной внешнеполитической деятельности.

Рассмотрим процесс защиты информации с точки зрения интереса войск радиоэлектронной борьбы (РЭБ). Для начала разберемся, что же такое РЭБ и какие цели она выполняет.

Радиоэлектронная борьбы предполагает использование войсками радиопомех для нарушения работы вражеских систем связи и управления беспилотными летательными аппаратами (БПЛА), а также радаров, систем наведения, подавления и так далее. Как в прошлом, так и в настоящем времени войска радиоэлектронной борьбы являются неотъемлемой частью военных операций, они всегда были и будут востребованы. Наша армия известна всему миру своими передовыми возможностями в области радиоэлектронной борьбы, которое имеет значительное преимущество в борьбе со врагом.

РЭБ помогает нашим войскам достичь тактического преимущества при решении оборонительных и наступательных задач. РЭБ, как и защита информации имеют одну общую цель — минимизировать и обнулить возможность противника собирать информацию с помощью разведки [3].

Основные цели радиоэлектронной борьбы:

• контроль (контроль над ведением действий противника, отслеживание передвижения войск, передвижения техники и т. д., получение преимущества для контроля каналов связи и лишение возможности врага действовать эффективно);

• обман (введение в заблуждение электронных систем подавления противника и нарушение связи);

• лишение возможности координировать действия противника;

• нарушение работы (прерывание работы электронных систем и инфраструктуры противника;

• уничтожение (физическое повреждение или уничтожение электронных систем подавления противника).

Исходя из выделенных целей войск радиоэлектронной борьбы можно сделать выводы о том, что ценность информации и степень ее защиты от злоумышленников становится все больше. Умение правильно владеть информацией становится важнейшим качеством каждого военнослужащего.

Чтобы нейтрализовать угрозы, необходимо выявить и распределить их на классы, специалисты по защите информации подразделяют их на два вида:

• внутренние (конфликты личного состава, создание искусственно накаленной атмосферы);

• внешние (действия противника, находящихся за пределами Российской Федерации).

Для эффективной защиты можно выделить следующие мероприятия по обеспечению информационной безопасности:

1. Защита информации от повреждения, утечки, перехвата;

2. Психологическая защита личного состава, психологическая помощь военнослужащим.

Эти меры необходимо принять во внимание ввиду того, что устойчивая система защиты информации должна стать причиной снижения боеспособности войск противника, снижение их мотивации вести военные действия.

Таким образом, информация, циркулирующая в войсках радиоэлектронной борьбы, имеет высокое значение и большую важность для врага, особенно в настоящее время. Противник всеми способами пытается завладеть информацией для получения тактического преимущества. Для того, чтобы этого не допустить защита информации должна носить комплексный характер.

Список источников

1. Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.03.2015) «О государственной тайне»/КонсультантПлюс. www.consultant.ru.

2. Ворошилин И.А. Политика государства в сфере охраны тайн (опыт России): дис. … конд. полит. наук. Москва, 2013.

3. Болкунов А. Радиоэлектронной борьбе 100 лет [Текст]/А.Болкунов, В. Коровин, С. Косенко//Радио. – 2004. №4 – С. 119-124.

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Матвеев Д. А. – старший оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Колосов Е. Д. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Ткачёв А. С. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Шатских В. В. – старший научный сотрудник роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Матвеев Д. А. – идея, сбор материала, обработка материала, частичное написание статьи (45 %).

Колосов Е. Д. – написание статьи, научное редактирование текста (20 %).

Ткачёв А. С. – написание статьи, научное редактирование текста (20 %).

Шатских В. В. – научное редактирование текста, подбор литературных источников (15 %).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Анализ традиционных методов защиты информации от киберугроз

Галина Дмитриевна Матюхина[1]✉, Владимир Александрович Воронин[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] galinochka2303@gmail.com✉,https://orcid.org/0009-0001-1295-2944
[2] voroni.vladimir.ozi@gmail.com, https://orcid.org/0009-0009-5380-2465

Аннотация. В данной статье рассматриваются традиционные методы защиты информации от основных видов киберугроз.

Ключевые слова: киберугроза, иформационная безопасность, спам, вирус, фишинг, бранмауэры, шифрование.

Для цитирования: Матюхина Г. Д., Воронин В. А. Анализ традиционных методов защиты информации от киберугроз // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 176–179.

Каждый день в мире совершаются тысячи цифровых атак, угрожающих безопасности и конфиденциальности информации. На защиту конфеденциальным данным становится информационная безопасность.

Информационная безопасность — важнейшая задача современного общества, так как зависимость от цифровых систем и Интернета постоянно растет. Практика кражи личных конфидециальных и общественных «секретов» в современном мире быстро развивается, растут возможности отъема информации, следовательно растет и спрос на системы защиты, которым мешают киберугрозы.

Киберугрозы становятся все более опасными, проникая в различные сферы жизни. Понимание и борьба с этими угрозами становятся неотъемлемой частью современного общества, требующей постоянного внимания и обновления соответствующих мер защиты. Киберугроза является распространением вредоносной информации и спама в Сети, ставящая под угрозу персональную информационную безопасность человека, компании или государства [2].

Основными видами внешних киберугроз являются вирусы, спам, фишинг, DoS/DDoS-атаки, удаленный доступ и т. д.

Вирус — это программный код, который самовоспроизводится и может самопроизвольно присоединяться к файлам, заражать их и создавать свои копии [3].

Спам — это массовая рассылка сообщений получателям без их согласия и размещение опасных вредоносных программ [4].

Фишинг — массовая рассылка сообщений получателям без их согласия, нацеленнная на узкие группы пользователей и содержащая сообщения с социальным контекстом, призывающие потенциальную жертву открыть исполняемый файл или перейти на сайт, содержащий вредоносный код [1, с. 5].

DoS-атака — атака на вычислительную систему, доводящая её до отказа, то есть создание таких условий, при которых легитимные пользователи системы не могли получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднён. DDoS-атаки в отличие от DoS-атаки имеют цель сделать сетевые ресурсы или каналы связи недоступными для легитимных пользователей [5].

Удаленный доступ — атака со стороны злоумышленников, с помощью которой они получают возможность читать и редактировать документы, хранящиеся на файл-серверах и в компьютерах, по собственному желанию уничтожать их, внедрять собственные программы и т. д. [1, с. 5].

Обращаясь к традиционным мерам защиты основных киберугроз, выделяют брнмаэры, системы обнаружения вторжений (IDS) и шифрование. Брандмауэры — это защитный экран между глобальным интернетом и локальной компьютерной сетью организации [5]. Он выполняет функцию проверки и фильтрации данных, поступающих из интернета. В зависимости от настроек брандмауэр может пропустить их или заблокировать, различают сетевой брандмауэр (или, по-другому, сетевой экран) и брандмауэр, встроенный в операционную систему Windows. На основе их функциональности бранмауэры защищают от фишинга и DDoS-атак.

Системы обнаружения вторжений (IDS) — система обнаружения вторжений, предназначенная для регистрации подозрительных действий в сети, уведомляющая о них ответственного за информационную безопасность сотрудника с помощью передачи сообщения на консоль управления [6]. Данный способ защиты способствует устранению вирусов, устраняет попытки несанкционированного доступа к системе или сети (удалённого доступа) и защищает DoS-атаки, направленные на отключение системы или сети.

Шифрование — метод защиты данных, который преобразовывает их таким образом, что сообщения способны прочитать только авторизованные пользователи [7]. Для обратного преобразования (дешифрования) и доступа к передаваемым сообщениям такие пользователи используют специальный ключ. Данный метод защищает пользователя от перехвата данных, несанкционированного доступа к системе, вирусов и вредоносныхх ПО.

В заключении следует отметить, что все вышеперечисленные методы очень малоэффективны по отдельности, так как каждый из них имеют свои ограничения. Данные меры безопасности полагаются на правила и набор операций, которых может быть недостаточно для обнаружения и дезактивации новых неизвестных атак. Так же они могут ложно срабатывать и неспособны адаптироваться к меняющемуся уровню угроз. Поэтому необходимо использовать совокупность данных методов для эффективной защиты и конфеденциальности данных пользователя.

Список источников

1. Вангородский, С. Н.Основы кибербезопасности : учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019. — с. 240.

2. Киберугрозы и методы борьбы с ними [Электронный ресурс]. — URL:https://silino.mos.ru/presscenter/news/detail/9197858.html(Дата обращения 22.04.2024).

3. Компьютерные вирусы и защита от них — урок. Информатика, 7 класс. [Электронный ресурс]. — URL:https://www.yaklass.ru/p/informatika/7-klass/tcifrovaia-gramotnost-7279385/vredonosnoe-programmnoe-obespechenie-6749705/re-0597d9eb-7a45-41df-8563-b68f5549eef6(Дата обращения 21.04.2024).

4. Спам: что это такое, его виды и как с ним бороться. | Unisender [Электронный ресурс]. — URL:https://www.unisender.com/ru/glossary/chto-takoe-spam-i-ego-vidy/(Дата обращения 21.04.2024).

5. Что такое брандмауэр и как его отключить, настройка windows firewall, правила для входящих подключений [Электронный ресурс]. – URL:https://www.nic.ru/help/chto-takoe-brandmauer-i-kak-ego-otklyuchit6_11119.html?ysclid=luq018lckd586770905(Дата обращения 20.04.2024)

6. Системы обнаружения и предотвращения вторжений – IPS/IDS | Блог Timeweb Cloud [Электронный ресурс]. – URL:https://timeweb.cloud/blog/ips-ids?ysclid=lupzyvo5x0266732855(Дата обращения 20.04.2024).

7. Что такое шифрование и как оно работает? - Kingston Technology [Электронный ресурс]. – URL:https://www.kingston.com/ru/blog/data-security/what-is encryption#:~:text=%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%20%E2%80%94%20%D1%8D%D1%82%D0%BE%20%D1%81%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%20%D0%BF%D1%80%D0%B5%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F,%D0%B8%20%D1%81%D0%BE%D0%B3%D0%BB%D0%B0%D1%81%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D1%85%20%D0%BE%D1%82%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D0%B5%D0%BB%D0%B5%D0%BC%20%D0%B8%20%D0%BF%D0%BE%D0%BB%D1%83%D1%87%D0%B0%D1%82%D0%B5%D0%BB%D0%B5%D0%BC (Дата обращения 20.04.2024).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Матюхина Г. Д. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Воронин В. А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Матюхина Г. Д.– идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Воронин В. А. – написание статьи, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Основные виды угроз информационной безопасности в организациях сферы здравоохранения

Галина Дмитриевна Матюхина[1]✉, Максим Валерьевич Ковалев[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] galinochka2303@gmail.com✉, https://orcid.org/0009-0001-1295-2944
[2] makskovalew@mail.ru, https://orcid.org/0009-0000-2312-2279

Аннотация. В данной статье проанализированы виды конфиденциальной информации, обрабатываемой и хранимой в организациях сферы здравоохранения и рассмотрены основные виды угроз информационной безопасности таких организаций.

Ключевые слова: информационная безопасность, здравоохранение, персональные данные пациентов, коммерческая тайна, медицинская (врачебная) тайна, виды угроз информационной безопасности.

Для цитирования: Матюхина Г. Д., Ковалев М. В. Основные виды угроз информационной безопасности в организациях сферы здравоохранения // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 180–183.

В организациях сферы здравоохранения обрабатывается и хранится несколько видов конфиденциальной информации, требующей защиты от различных видов угроз во избежание возникновения ущерба.

Система здравоохранения России, функционирующая для поддержания и улучшения качества жизни населения, играет роль в социально-экономическом развитии как страны в целом, так и отдельных её регионов. Внедрение информационных технологий в учреждениях сферы здравоохранения необходимо для повышения качества медицинской помощи граждан. При использовании информационных технологий многие данные находятся под угрозой кибератак со стороны злоумышленников, поэтому для защиты информационных технологий применяются средства по обеспечению информационной безопасности. Однако, уровень зрелости информационной безопасности в медицинских учреждениях России, согласно исследованию BI.ZONE, по состоянию на 2020 год находился на невысоком уровне по сравнению с другими отраслями (2.2 балла по пятибалльной шкале) [5. Кроме этого за первые шесть месяцев 2020 года было зафиксировано 25 утечек конфиденциальной информации, связанной с подтверждёнными анализами на короновирусную инфекцию COVID-19 [5].

К видам конфиденциальной информации в сфере здравоохранения относятся: персональные данные пациентов (ПДп), медицинская (врачебная) тайна, коммерческая тайна, статистические сведения и иная служебная информация [2].

Персональными данными пациента является ФИО, место рождения и проживания, контактная информация, номер медицинского полиса и прочее.

Медицинская (врачебная) тайна включает сведения, описывающие состояние пациента: его здоровье, наличие каких-либо заболеваний, диагнозы, результаты лечения, в соответствие с п. 1 ст.13 и п.2 ст. 22 N-323 ФЗ «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 [4].

Коммерческая тайна включает следующие сведения: сведения клиентской базы, планы развития организации, методология лечения болезней, способы проведения качественных исследований и проверок.

Статистическими сведениями является информация из карт пациентов, сведения о работниках медицинских учреждений (например, зарплаты), их работе с бюджетными средствами.

Иной служебной информацией являются такие результаты служебных проверок по исполнению требований по работе и служебным обязанностям.

Такая информация из организаций нередко подвергается хакерским атакам, ведущим к утечкам данных из медицинских учреждений. Из всех существующих видов угроз ИБ для медучреждений наиболее часто встречаются следующие: имитация (подделка личности) другого лица сотрудником организации (включая имитацию другого лица медицинскими работниками и вспомогательным персоналом), имитация другого лица поставщиками услуг, имитация другого лица посторонними лицами, попадание вредоносного или разрушительного программного обеспечения (вирусы, черви и другое вредоносное ПО), злоупотребление системными ресурсами и т. д. [3].

Имитация другого лица сотрудниками организации заключается в использовании системы теми, кто извлекает выгоду из учетных записей, не принадлежащих им [1]. Примером подобного может являться работа одного медицинского работника и замена его другим на рабочей станции с продолжением работать по уже открытой карте объекта оказания медицинской помощи без выхода первого пользователя и входа второго пользователя. Такая имитация другого лица сотрудниками организации является источником нарушений конфиденциальности.

Имитация другого лица поставщиками услуг заключается в использовании сотрудниками, работающими на договорной основе, привилегированного доступа к системам для получения несанкционированного доступа к данным [2]. Данная угроза информационной безопасности медицинского учреждения является нарушением безопасного обеспечения использования внешних источников, что ведёт к утечке конфиденциальности персональной медицинской информации.

Имитация другого лица посторонними лицами заключается в получение доступа к данным или ресурсам системы, выдав себя за уполномоченного поль-

зователя или обманным путем став уполномоченным пользователем [2]. Третьими лицами могут быть: хакеры, журналисты, частные детективы и «хактивисты» (хакеры, которые работают от имени или в поддержку политических группировок). При такой угрозе отказывает одна или несколько мер безопасности: идентификация пользователя, аутентификация пользователя, аутентификация источника, контроль доступа и управление полномочиями.

В заключении следует отметить, что основные угрозы информационной безопасности, рассмотренные выше, представляют основные риски для обеспечения информационной безопасности в медицинских организациях. Эти угрозы могут привести к утечкам данных и нарушению конфиденциальности персональных данных граждан, что противоречит законам Российской Федерации.

Список источников

1. ГОСТ Р ИСО 27799-2015 Информатизация здоровья. Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002 [Электронный ресурс]. — URL: https://ohranatruda.ru/upload/iblock/11f/4293755562.pdf?ysclid=luedtjcfz5510433452 (Дата обращения 22.04.2024).

2. Защита медицинских данных: как защитить ПДн пациентов от разглашения? [Электронный ресурс]. — URL:https://rt-solar.ru/products/solar_dozor/blog/3205/?ysclid=luedoj5o1d104231087 (Дата обращения 21.04.2024).

3. Приложение А (справочное). Угрозы защиты медицинской информации | ГАРАНТ [Электронный ресурс]. — URL: https://base.garant.ru/71742172/53f89421bbdaf741eb2d1ecc4ddb4c33(Дата обращения 21.04.2024).

4. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 N 323-ФЗ (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. — URL: https://www.consultant.ru/document/cons_doc_LAW_121895 (Дата обращения 22.04.2024).

5. Чем опасны кибератаки на медицинские учреждения [Электронный ресурс]. — URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Cyberattacks-on-healthcare-system (Дата обращения 19.04.2024).

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Матюхина Г. Д. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Ковалев М. В. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Матюхина Г. Д. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Ковалев М. В. – написание статьи, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

Научная статья
УДК 004.8

Основные критерии в оценке ущерба от утечки персональных данных

Галина Дмитриевна Матюхина[1]✉, Кирилл Андреевич Седаков[2], Сергей Алексеевич Ермаков[3]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[1] galinochka2303@gmail.com✉, https://orcid.org/0009-0001-1295-2944
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624
[3] ermar_87@mail.ru

Аннотация. Рассмотрены основные критерии оценки финансового ущерба при утечки персональных данных в организации.

Ключевые слова: количественный анализ, качественный анализ, метод суда.

Для цитирования: Матюхина Г. Д., Седаков К. А., Ермаков С. А. Основные критерии в оценке ущерба от утечки персональных данных // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 184–187.

В современной эпохе цифровизации, когда информационные технологии становятся все более важными в различных областях жизни, вопросы безопасности персональных данных становятся все более актуальными. Для уменьшения риска утечки информации, компаниям нужно сначала оценить возможный ущерб. Способы оценки ущерба, основанные на количественном анализе рисков, пользуются наибольшей популярностью.

Один из важных аспектов таких методов, как метод Дельфи, метод комиссии, метод суда и т. д., — это качественный анализ. Он основывается на оценке рисков и их возможных последствий с использованием различных критериев, таких как затраты, официальные требования, социально-экономические аспекты, внешняя среда, интересы заказчика и другие исходные данные [4].

Количественный анализ — это анализ потенциального воздействия идентифицированных рисков на общие цели проекта. Он используется для оценки рисков, полученных в результате качественного анализа. При нём оцениваются вероятности возникновения рисков и размеры ущерба/выгоды. Для того чтобы выбрать тот или иной способ анализа финансового ущерба, необходимо определить бюджет проекта и затраченное время.

Обращаясь к критериям, по которым производится тот или иной анализ рисков, рассматриваются следующие критерии анализа:

1. Описание самого проекта.
2. Активы организационного процесса.
3. Реестр рисков.
4. План управления данными рисками.
5. Оценка срочности риска.

Активами организационного процесса являются:

- базы данных, накопленных в процессе подготовки и реализации проекта;
- использование некоторых данных рисков предыдущих проектов,
- коллектив, занимающийся разработкой данного проекта.

Под описанием самого проекта понимается описание именно конкретной цели достижения поставленного результата. Оно служит для определения степени неопределённости.

Для плана управления данными рисков существуют категории рисков, распределение ролей и ответственности в управлении рисками, определение вероятности возникновения последствий, уточнение толерантности к риску участников проекта.

Реестр рисков подразумевает под собой список идентифицированных рисков, который включает в себя сами риски и их причины возникновения.

Оценка срочности риска — определение важности риска и моментальное реагирование его возникновение. На оценку срочности влияет ранг риска и симптомы самого риска.

Одним из способов оценки финансового ущерба является метод суда. Метод суда — это способ проведения коллективной оценки идей и вариантов решения. Он заключается в том, чтобы три категории людей: «прокурор», «адвокат», «судья» провели совещание, на котором «прокурор» критикует предложение, а «адвокат» защищает, а «судья» выносит своё решение, выслушав все стороны. Кроме этого существует функция модератора, заключающаяся в мирном урегулирование конфликтов во время проведения данного мероприятия. Эту функцию может взять на себя «судья». Данный метод используется в полуигровой форме, что за частую является одним из его недостатков, так как не всегда все способны работать на серьёзный результат в игровой форме и в процессе соответствовать своей роли [1].

Этот метод предлагает несколько вариантов решения проблемы, исходя из критериев финансового ущерба, которые обсуждаются коллективно без анонимности, что может вызывать разногласия между специалистами. Однако метод неэффективен из-за субъективного мнения каждого специалиста и требует много времени.

Проанализировав выше сказанное, можно сделать вывод, что определение конечного ущерба для организации в случае утечки персональных данных представляет собой сложную задачу. Основными критериями определения ущерба являются: размер штрафа в соответствии с законодательством РФ, ко-

личество исков от потерпевших, а также стоимость компенсации ущерба для субъектов данных. Значение минимального/максимального штрафа на юридическое лицо, согласно законодательству РФ, составляет от ста тысяч до восемнадцати миллионов рублей в соответствие с КоАП РФ Статья 13.11 [2].

Количество исков от субъектов персональных данных означает количество людей, пострадавших от утечки информации о клиентах или сотрудниках. Чем больше пострадавших, тем больший финансовый ущерб наносится организации.

Стоимость возмещения ущерба субъектам персональных данных ограничивается ч. 2 ст. 24 Закона 152 ФЗ. Моральный вред, причиненный субъекту, вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим ФЗ, а также требований к защите, установленных в соответствии с настоящим ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации [3].

Таким образом, текущий способ оценки конечного ущерба для организации на основе количественного анализа в случае утечки персональных данных представляет собой сложную задачу и не может быть задействован, поскольку отсутствуют основные критерии определения ущерба: размер штрафа в соответствии с законодательством РФ, количество исков от потерпевших, а также стоимость компенсации ущерба для субъектов данных.

Список источников

1. Солодов, А.К. Основы финансового риск-менеджмента: учебник и учебное пособие / А.К. Солодов; Финуниверситет. Москва: Издание Александра К. Солодова, 2018. 286 с.

2. КоАП РФ Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных \ Консультант Плюс [Электронный ресурс]. – URL:https://www.consultant.ru/document/cons_doc_LAW_34661/1f421640c6775ff67079ebde06a7d2f6d17b96db/?ysclid=luebg8eu4l314620819 (Дата обращения 17.04.2024).

3. Статья 24. Ответственность за нарушение требований настоящего Федерального закона \ КонсультантПлюс [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/741d689fd8f2aaf6a0a81af1cba20b45e78c2849/?ysclid=luecig90oh811196188 (Дата обращения 16.04.2024).

4. НОУ ИНТУИТ | Методические основы управления ИТ-проектами. Лекция 10: Идентификация рисков проекта [Электронный ресурс]. – URL:https://intuit.ru/studies/courses/964/502/lecture/11402?ysclid=luearv1crg295786629 (Дата обращения 12.04.2024).

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Матюхина Г. Д. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Ермаков С. А. – к. т. н., доцент кафедры иностранных языков ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Матюхина Г. Д. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – написание статьи, научное редактирование текста (40 %).

Ермаков С. А. – сбор материала, обработка материала, частичное написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 056

Анализ веб-сайта с помощью инструментов сканирования сети

Дмитрий Владимирович Мышляков[1], Оксана Михайловна Голембиовская[2], Сафаа Кхалид Бреесам Рабееах[3]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[3] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[1] mrteadragon@gmail.com https://orcid.org/0009-0009-9461-2887
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133
[3] ra_skb@mikron.ru

Аннотация. В статье представлен анализ использования инструментов сканирования сети для изучения веб-сайта. В статье рассматривается процесс сканирования портов и выявления потенциальных уязвимостей, а также методика проведения анализа с целью повышения безопасности сайта.

Ключевые слова: анализ, веб-сайт, инструменты сканирования сети, сканирование портов, безопасность, уязвимости.

Для цитирования: Мышляков Д. В., Голембиовская О. М., Рабееах С. К. Б. Анализ веб-сайта с помощью инструментов сканирования сети // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 188–191.

В современном информационном мире веб-сайты становятся все более важным и фундаментальным элементом успешного функционирования, как для бизнеса, так и для личных целей. Однако, наряду с возрастающей значимостью веб-ресурсов, возрастает и уровень угроз для их безопасности. В связи с этим, проведение анализа веб-сайта с использованием инструментов сканирования сети становится необходимым шагом для обеспечения безопасности и надежности сайта.

Анализ веб-сайта с помощью таких инструментов позволяет выявить потенциальные уязвимости, ошибки конфигурации, утечки данных и другие проблемы, которые могут стать причиной угрозы для сайта и его пользователей. Кроме того, данный тип анализа помогает обнаружить скрытые угрозы, которые могут оставаться незамеченными без специализированных инструментов.

Таким образом, важность проведения анализа веб-сайта с использованием инструментов сканирования сети не может быть недооценена. Этот процесс помогает обеспечить безопасность сайта, защитить информацию на нем и повысить уровень доверия пользователей. В данной статье рассматриваются ос-

новные принципы анализа веб-сайтов и роль инструментов сканирования сети в этом процессе.

Два основных инструмента сканирования сети, которые широко используются — это Nmap и DiG.

Nmap — это мощный инструмент сканирования портов и сетей, который позволяет анализировать устройства в сети, идентифицировать открытые порты, определять службы, работающие на этих портах, и даже выявлять потенциальные уязвимости в системах. Nmap предоставляет обширные возможности для сканирования сетей различных типов и размеров, а также для проведения тестов на проникновение [1].

DiG (Domain Information Groper) — это утилита, используемая для выполнения DNS-запросов и получения информации о доменах, IP-адресах, именах хостов и других связанных данных. DiG позволяет анализировать DNS-запросы, проверять состояние доменных записей, идентифицировать возможные проблемы с настройками DNS и т. д. Этот инструмент является важным компонентом в анализе безопасности веб-сайтов.

Nmap и DiG обладают различными функциональностями, которые позволяют проводить комплексный анализ веб-сайтов. Nmap способен сканировать отдельные узлы, целые сети, определять хосты и порты, исследовать уязвимости и многое другое. DiG, в свою очередь, предоставляет информацию о DNS-запросах, резолвинге доменных имен, проверке конфигурации DNS и другую полезную информацию об инфраструктуре сайта.

При проведении сканирования веб-сайта X с помощью инструмента Nmap были получены следующие результаты:

IP-адрес хоста: 84.42.79.98

Сканирование выполнено за 4,14 секунды

По результатам сканирования были обнаружены следующие порты и их статусы:

- 21/TCP: Фильтрованный FTP;
- 22/TCP: С фильтрацией SSH;
- 23/tcp: Фильтрует Telnet;
- 80/tcp: HTTP с фильтрацией;
- 110/TCP: С фильтрацией POP3;
- 143/TCP: Отфильтрованное изображение;
- 443/TCP: Фильтруется HTTPS;
- 3389/TCP: Фильтруется MS-WBT-сервер.

Из результатов сканирования видно, что большинство портов сайта X.ru защищены фильтрами или брандмауэром, что может создавать препятствия для доступа к соответствующим службам. Это говорит о хорошем уровне безопасности, так как доступ к сервисам ограничен.

В целом, анализ результатов сканирования сети для веб-сайта X.ru дает представление о степени безопасности и конфигурации сервера, а также помогает выявить потенциальные уязвимости и проблемы безопасности.

Проведено сканирование сайтов через сервис dig для подтверждения полученных данных. Результаты показали информацию о домене X.ru, что дополняет обнаруженные данные с Nmap. Это подтверждает наличие соответствующих записей и связей между IP-адресами и доменными именами.

Проведенный анализ веб-сайта X с использованием инструментов сканирования сети Nmap и DiG позволил получить ценные данные о его безопасности и конфигурации. Открытые порты и фильтрация служб говорят о наличии хорошей защиты и контроля доступа к сайту. Результаты сканирования позволяют лучше понять степень безопасности сайта и выявить потенциальные уязвимости.

Использование инструмента Nmap позволило идентифицировать открытые порты на сервере, а также выявить фильтрацию трафика на некоторых службах, что свидетельствует о хорошей настройке брандмауэра или других защитных механизмов. Это важно для предотвращения возможных атак или несанкционированного доступа.

DiG дополнил результаты сканирования, предоставив дополнительную информацию о DNS-запросах и доменных данных. Этот инструмент является неотъемлемой частью комплексного анализа безопасности веб-сайтов, позволяя проверить корректность настроек DNS и подтвердить соответствие доменных записей.

Рекомендации по использованию инструментов сканирования сети для анализа безопасности веб-сайтов включают регулярное проведение сканирований, мониторинг защиты открытых портов и обновление защитных мероприятий для обеспечения стабильной безопасности сайта. Также стоит обращать внимание на исправление выявленных уязвимостей и улучшение общей конфигурации сервера.

Анализ веб-сайта с помощью инструментов сканирования сети является важным шагом для обеспечения безопасности сайта и защиты информации. Правильно примененные инструменты позволяют выявить уязвимости и проблемы, которые могут быть устранены для повышения уровня безопасности и надежности веб-ресурса X.

В итоге, использование инструментов сканирования сети, таких как Nmap и DiG, представляет собой необходимую практику для оценки безопасности веб-сайтов и минимизации угроз. Путем анализа полученных данных мы можем улучшить защиту сайта, обеспечить сохранность данных и повысить доверие пользователей к ресурсу.

Проведение анализа веб-сайта с использованием инструментов сканирования сети имеет принципиальное значение для обеспечения безопасности и защиты информации на веб-ресурсах. В свете все возрастающих угроз и высокой значимости веб-сайтов, данный процесс становится обязательным шагом для предотвращения возможных атак и уязвимостей.

Проведенный анализ с использованием таких широко используемых инструментов, как Nmap и DiG, позволяет обнаружить потенциальные уязвимости, конфигурационные ошибки, утечки данных и другие проблемы, которые

могут представлять угрозу для безопасности веб-сайта и его пользователей. Это позволяет рано выявлять скрытые угрозы и проблемы, которые могли бы остаться незамеченными без специализированных инструментов сканирования.

Важность проведения анализа веб-сайта с использованием инструментов сканирования сети не может быть недооценена. Этот процесс способствует укреплению безопасности сайта, защите конфиденциальной информации и повышению уровня доверия пользователей к ресурсу. Результаты анализа помогают лучше понять степень безопасности сайта, выявить уязвимости и возможные проблемы безопасности, что важно для принятия необходимых мер по их устранению.

Таким образом, анализ веб-сайта с использованием инструментов сканирования сети является неотъемлемой частью обеспечения безопасности в виртуальной среде. Правильно примененные инструменты помогают создать надежную защиту от потенциальных угроз, минимизируя риски и обеспечивая сохранность информации на веб-ресурсе. Выводы, полученные в результате анализа веб-сайта X с использованием инструментов Nmap и DiG, подчеркивают важность регулярного проведения сканирований, мониторинга защиты портов и обновления защитных мероприятий. Благодаря этому процессу можно обеспечить стабильную безопасность сайта, предотвращая возможные атаки и несанкционированный доступ.

Список источников

1. Волхов В.Е., Шахов В.Г. Сравнительный анализ сетевых сканеров безопасности. 2006. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-setevyh-skanerov-bezopasnosti/viewer.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

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

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Рабееах С. К. Б. – к. т. н., доцент кафедры иностранных языков ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Мышляков Д. В. – идея, сбор материала, обработка материала, частичное написание статьи (80 %).

Голембиовская О. М. – научное руководство (10 %).

Рабееах С. К. Б. – обработка материала, частичное написание статьи (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Выявление основных особенностей в существующих методах оценки эффективности средств защиты персональных данных

Дмитрий Владимирович Мышляков[1]✉, Кирилл Андреевич Седаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] mrteadragon@gmail.com✉, https://orcid.org/0009-0009-9461-2887
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624

Аннотация. Рассматриваются существующие методы оценки эффективности средств защиты персональных данных с целью выявления основных особенностей и принципов их работы. Анализируются различные подходы к оценке безопасности и конфиденциальности данных, а также предлагаются рекомендации для повышения уровня защиты личной информации.

Ключевые слова: персональные данные, защита данных, информационная безопасность, методы оценки, квалификационный подход, технический подход, метрический подход, программные сканеры уязвимостей, методика OCTAVE, метрика MTTF, конфиденциальность данных, безопасность информации.

Для цитирования: Мышляков Д. В., Седаков К. А. Выявление основных особенностей в существующих методах оценки эффективности средств защиты персональных данных // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 192–195.

Количество цифровых данных, содержащих личную информацию, в нашем мире растет с каждым днем, вызывая необходимость обеспечения их адекватной защиты. В условиях постоянных угроз кибербезопасности становится все более актуальным вопрос эффективности средств защиты персональных данных. Для оценки эффективности таких средств на сегодняшний день существует множество методов и подходов. В данной статье мы пройдемся по основным особенностям существующих методов оценки эффективности средств защиты персональных данных, выявим их преимущества и недостатки, а также рассмотрим возможные пути улучшения данной методологии [2].

Цель данной работы заключается в изучении и анализе разнообразных подходов к оценке эффективности средств защиты персональных данных, применяемых в современном информационном обществе. Основное внимание будет уделено выявлению основных принципов и методов, используемых для оценки уровня безопасности персональных данных, а также анализу их достоинств и недостатков. На основе этого анализа будет составлен обзор наиболее

результативных методов оценки защиты личных данных, что позволит выделить оптимальные практики в данной области и предложить рекомендации для улучшения уровня безопасности и конфиденциальности информации. Уровень угроз для персональных данных постоянно возрастает, что требует постоянного контроля и совершенствования методов и средств их защиты. Рассмотрение существующих методов оценки эффективности средств защиты личных данных позволит определить их сильные и слабые стороны, а также выявить потенциальные области улучшения. Критическое осмысление проблемы обеспечения безопасности данных сегодня является ключевым элементом современной информационной безопасности, и исследование различных подходов к оценке эффективности защиты персональных данных способствует развитию этой области.

Существует несколько основных подходов к оценке эффективности средств защиты персональных данных, каждый из которых имеет свои особенности и области применения в практике информационной безопасности [1]. Среди них выделяются следующие типы методов:

1. Квалификационный подход: основан на оценке квалификации и опыта специалистов по информационной безопасности, которые анализируют системы защиты и выявляют их уязвимости.

- преимущества:
  - основан на экспертной оценке специалистов по информационной безопасности;
  - позволяет выявить уязвимости, которые могут быть не замечены другими методами.
- недостатки:
  - требует высокой квалификации экспертов;
  - подвержен субъективному восприятию.

2. Технический подход: включает в себя использование специализированных инструментов и программного обеспечения для сканирования уровня безопасности систем и сетей.

- преимущества:
  - использует специализированные инструменты для точного сканирования уровня безопасности;
  - может автоматизировать процессы оценки.
- недостатки:
  - может быть ограничен в области применения;
  - требует постоянного обновления инструментов.

3. Метрический подход: основан на количественной оценке показателей эффективности средств защиты, таких как время обнаружения угрозы, время реакции на инциденты безопасности и другие параметры.

- преимущества:
  - обеспечивает количественные оценки эффективности защиты данных;

– позволяет проводить сравнительный анализ различных методов.

- недостатки:
  – требует определения показателей для измерения;
  – может быть сложен в применении для некоторых организаций.

Подходы к оценке эффективности средств защиты персональных данных могут быть различны в зависимости от конкретных требований организации и характеристик информационной инфраструктуры. Некоторые из основных подходов включают в себя:

- анализ уязвимостей: оценка уровня уязвимости систем и приложений для выявления возможных точек атаки со стороны злоумышленников;
- оценка соответствия стандартам безопасности: проверка соответствия системы защиты персональных данных стандартам и правилам безопасности, установленным в отрасли или государственными органами;
- проверка уровня шифрования: анализ методов шифрования, используемых для защиты персональных данных, и оценка их надежности и эффективности [3].

Для проведения оценки эффективности средств защиты персональных данных существует ряд специализированных инструментов и метрик, которые помогают определить уровень защиты информационной системы. Некоторые из наиболее популярных примеров включают:

- программные сканеры уязвимостей: специализированные программы для автоматического обнаружения уязвимостей в сети или приложениях;
- методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): методика оценки уязвимостей и угроз информационной безопасности организации;
- метрика MTTF (Mean Time To Failure): среднее время до возникновения отказа в системе защиты данных, используемое для оценки надежности и стабильности средств защиты.

Каждый из рассмотренных методов имеет свои преимущества и ограничения, и выбор метода должен ориентироваться на контекст и особенности организации. Необходимо постоянно совершенствовать методы оценки эффективности средств защиты, учитывая изменяющиеся угрозы и требования по защите персональных данных. Интегрированные и автоматизированные подходы, использование искусственного интеллекта и машинного обучения помогут улучшить оценку и реагирование на угрозы в информационной сфере.

Таким образом, оценка эффективности средств защиты персональных данных в организации является важным этапом информационной безопасности. Данная оценка позволит укрепить систему защиты конфиденциальной информации и обеспечить конфиденциальность персональных данных.

Список источников

1. Куракин А.С. Методы и алгоритмы построения информационных систем персональных данных в защищенном исполнении URL: https://www.dissercat.com/content/metody-i-algoritmy-postroeniya-informatsionnykh-sistem-personalnykh-dannykh-v-zashchishchenn.

2. Федеральный закон «О персональных данных» №152-ФЗ от 27.07.2006. URL: http://www.consultant.ru/document/cons_doc_LAW_61801.

3. Давыдова О.Б. Защита персональных данных URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-1.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

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

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Мышляков Д. В. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Порядок реагирования на наиболее популярные способы реализации кибератак в соответствии с техниками матрицы MITRE ATT&CK

Никита Алексеевич Николаев[1]✉, Анна Николаевна Вишнякова[2], Иван Владимирович Горбачев[3], Оксана Михайловна Голембиовская[4]

[1, 2, 3, 4] Брянский государственный технический университет, Брянск, Россия
[1, 3] bryansk-tu@yandex.ru✉
[2] vshnv.a@yandex.ru
[4] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133

Аннотация. Порядок реагирования на наиболее популярные способы реализации кибератак в соответствии с техниками матрицы MITRE ATT&CK в настоящее время крайне актуален, учитывая все шире распространение киберугроз и увеличение сложности кибератак. Проактивная защита информационных систем по методике MITRE ATT&CK позволяет организациям быть готовыми к разнообразным угрозам, эффективно обнаруживать и предотвращать атаки, а также оперативно восстанавливаться после инцидентов.

Ключевые слова: информационная безопасность, кибератака, матрица MITRE ATT&CK.

Для цитирования: Николаев Н. А., Вишнякова А. Н., Горбачев И. В., Голембиовская О. М. Порядок реагирования на наиболее популярные способы реализации кибератак в соответствии с техниками матрицы MITRE ATT&CK // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 196–201.

Проблема роста количества кибератак с каждым годом набирает обороты. Под удар попадают организации различной направленности и сфер деятельности. Причем растет не только общее количество, но и сложность исполняемых техник.

Эксперты компании Positive Technologies представили подробный анализ ситуации в сфере кибербезопасности за 2023 год и дали прогноз на 2024 год. По статистике компании, 73 % всех кибератак в России за первые 9 месяцев носили целевой характер. Это на 5 процентных пунктов больше, чем за аналогичный период 2022 года (68 %). 58 % успешных атак привели к краже конфиденциальных данных. Еще в 41 % случаев произошло нарушение основной деятельности атакованных организаций [1].

В таблице 1 представлен пример обнаружения наиболее популярных способов реализации кибератак, проведено соответствие с техниками матрицы MITRE ATT&CK, а также подробно описан порядок реагирования на эксплуатацию техники. Помимо этого, описан порядок превентивного реагирования, работа с которым позволит значительно снизить вероятность эксплуатации рассматриваемых техник.

Таблица 1

Пример реагирования и обнаружения для некоторых видов техник матрицы MITRE ATT&CK

Техника MITRE ATT&CK	Пример обнаружения индикатора компрометации который может свидетельствовать о выполнении данной техники	ПО для автоматического реагирования	Порядок реагирования если инцидент произошел	Порядок превентивного реагирования
Способ реализации кибератаки: Маскарадинг (masquerading) ОС: Linux, Windows, macOS Маскарадинг происходит, когда имя или местоположение исполняемого файла, законного или вредоносного, подвергаются различным манипуляциям и злоупотреблениям с целью обхода защиты. Наиболее распространённый вариант маскарадинга заключается в том, чтобы исполняемый файл был помещен в общепринятый каталог или получил имя законной, доверенной программы. Имя файла может быть похоже на название законной программы. Такой способ маскировки применяется для обхода инструментов, которые доверяют файлам полагаясь на имя или путь к файлу, а также для обмана системных администраторов.				
T1036	Атакующие часто переименовывают свои утилиты под легитимное ПО, можно сравнить хеши запускаемого ПО (Sysmon event_id 1или события EDR) с оригинальными. Маскарадингом также могут являться файлы с двойным расширением (пример docx.exe или pdf.exe), помимо этого можно найти файлы	Антивирусное ПО (например, Kaspersky Endpoint Security), Межсетевые экраны (Например, межсетевой экран ESR-20, версия программного обеспечения 1.5).	Проверить выполняемые команды и аргументы, которые могут пытаться манипулировать функциями своих артефактов, чтобы они выглядели легитимными для пользователей и средств безопасности. Собрать хэши файлов: имена файлов, которые не соответствуют ожидаемому хэшу, являются подозрительными. Выполнить мониторинг файлов: подозрительными являются файлы с известными именами, но в необычных местах. Отследить изменения, внесенные в файлы вне обновлений или исправлений, контекстуальные данные о	Создавая различные правила безопасности избегать исключений на основе имени и пути к файлу. Требовать подписания двоичных файлов (подписание подтверждает две вещи - что файл не был подделан, и личность подписавшего). Использовать средства контроля доступа к файловой системе для защиты доверенных директорий. Не использовать инструменты ограничения выполнения программ на основе

	которые недавно скомпилировались.		запланированном задании, которые могут включать в себя такую информацию, как название, время выполнения, команды и т.д. изменения в данных заданиях. Отследить вызовы API, такие как fork(), которыми можно злоупотреблять для маскировки метаданных процесса или манипулирования ими. Следить за вновь выполняемыми процессами, которые могут пытаться манипулировать функциями своих артефактов, несоответствием имен файлов на диске и метаданных PE двоичного файла, вновь созданными сервисами. Зафиксировать индикаторы компрометации. Удалить вредоносные файлы.	имени или пути к файлу. Идентифицировать и блокировать потенциально-опасное и вредоносное ПО, которое может выглядеть как законная программа. Обучать пользователей не открывать вложения электронной почты и не переходить по неизвестным ссылкам (URL). Использовать сертифицированное Антивирусное ПО (например, Kaspersky Endpoint Security), а также средства контроля безопасности на конечной точке (HIPS) (например, Malware Defender) и средства автоматического мониторинга – SIEM, EDR, SOAR, XDR .
Способ реализации кибератаки: Обфускация файлов или информации (Obfuscated Files or Information) ОС: Linux, Windows, macOS Злоумышленники могут применять шифрование, кодирование и всевозможные методы обфускации файлов и их содержимого в системе или при их передаче. Чтобы скрыть строки простого текста закодированными могут быть и части файлов. Полезные нагрузки могут быть разделены на отдельные невредоносные файлы, которые при сборке в единое целое выполняют вредоносный функционал.				
T1027	Последствия запуска нелегитимного файла в системе, иными словами действия данного файла в системе (какие процессы и строки порождает, к каким файлам, ключам реестра и адресам обращается	IDS-системы (например межсетевой экран и система обнаружения вторжений «Рубикон», программный комплекс обнаружения	Отследить выполняемые команды и аргументы на предмет признаков запутывания и потенциально подозрительного синтаксиса, такого как не интерпретированные управляющие символы (например, ^). Запустить проверку на наличие вредоносной активности при помощи антивирусного ПО. Отследить контекстные	Использовать сертифицированное Антивирусное ПО (например, Kaspersky Endpoint Security), периодически проверять распространенные хранилища баз файлов (такие как Реестр или репозиторий WMI) для потенциального выявления ненормаль-

	и др.)	вторжений «Ребус-СОВ») , шлюзы безопасности электронной почты, также если есть такая возможность, можно запустить подозрительный файл в песочнице (Sandbox)и отправить вендору антивирусного ПО на анализ.	данные подозрительных файлов, которые могут включать такую информацию, как имя, содержимое (например, подпись, заголовки или данные / носители), пользователь / владелец, разрешения и т.д. Отследить и проанализировать вызовы таких функций, как GetProcAddress() которые связаны с обфускацией вредоносного кода. Следить за вновь выполняемыми процессами, которые могут пытаться затруднить обнаружение или анализ исполняемого файла путем шифрования, кодирования или иного запутывания его содержимого в системе или при передаче. Зафиксировать индикаторы компрометации. Удалить вредоносные файлы.	ных и вредоносных данных. Внедрить системы автоматического мониторинга – SIEM, EDR, SOAR, XDR
Способ реализации кибератаки: Инъекция кода в процесс (Process Injection), Ten Process Injection Techniques ОС: Windows, Linux, macOS Процессные инъекции – это метод выполнения произвольного кода в адресном пространстве отдельно живущего процесса. Запуск кода в контексте другого процесса позволяет получить доступ к памяти инъецируемого процесса, системным/сетевым ресурсам и, возможно, повышенные привилегии.				
T1055	Только оповещения систем мониторинга и антивирусного ПО.	Только самостоятельная проверка в рамках песочницы или запуск подозрительного файла в песочнице (Sandbox)и отправка вендору антивирусного ПО на анализ.	Мониторить контекстные данные о файле, которые могут включать такую информацию, как имя, содержимое (например, подпись, заголовки или данные / носители), пользователь / владелец, разрешения и т.д. Отслеживать изменения, внесенные в файлы, которые могут внедрять код в процессы, чтобы обойти защиту, а также, возможно, повысить привилегии. Отслеживать события файлов DLL / PE, в частности,	Методы инъецирования кода в процессы основаны на злоупотреблении штатными функциями ОС прямое воздействие на которые может привести к нестабильной работе законного ПО и продуктов безопасности. Усилия по предотвращению применения техник перехвата необходимо сосредоточить на более ранних этапах

			создание этих двоичных файлов, а также загрузку библиотек DLL в процессы. Искать библиотеки DLL, которые не распознаются или обычно не загружаются в процесс. Мониторить специфичные для Linux вызовы, например такие как системный вызов ptrace, который не должен генерировать большие объемы данных из-за их специализированной природы и может быть очень эффективным методом обнаружения некоторых инъекций. Контролировать несоответствия памяти процесса, например, сверять диапазоны памяти с известной копией допустимого модуля.	цепочки атаки, а именно применять инструменты блокировки потенциально-опасного ПО, такие как AppLocker. Применять Yama (модуль безопасности Linux) (например, /proc/sys/kernel/yama/ptrace_scope) в качестве превентивной меры от инъекций кода в ptrace, ограничив использование ptrace только привилегированными пользователями. Использовать WAF (например, Positive Technologies Application Firewall, F5 Networks Application Security Manager, NetScaler Application Firewall) Дополнительные меры защиты могут включать развертывание модулей безопасности ядра, обеспечивающих расширенный контроль доступа и ограничение процессов (SELinux, grsecurity, AppArmor). Внедрить системы автоматического мониторинга – SIEM, EDR, SOAR, XDR

Таким образом, применение описанных в рамках статьи рекомендаций позволит снизить вероятность эксплуатации наиболее популярных техник реализации кибератак на объекте, а также быстро и эффективно отреагировать на уже наступивший инцидент информационной безопасности, чтобы минимизировать возможные последствия.

Список источников

1. Шпионское ПО, уязвимости в системах передачи данных и нейросети в киберпреступности: аналитика Positive Technologies за 2023 год [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/news/544568.php (Дата обращения: 04.03.2024).

Статья поступила в редакцию 15.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Николаев Н. А. – выпускник кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Вишнякова А. Н. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Горбачев И. В. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Николаев Н. А. – обработка материала, написание статьи (50 %).
Вишнякова А. Н. – сбор материала, частичное написание статьи (17 %).
Горбачев И. В. – сбор материала, частичное написание статьи (17 %).
Голембиовская О. М – идея, научное редактирование (16 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Разработка алгоритма применения матрицы MITRE ATT&CK для реагирования на инциденты информационной безопасности

Никита Алексеевич Николаев[1]✉, Артем Андреевич Рябцев[2], Оксана Михайловна Голембиовская[3]
[1, 2, 3] Брянский государственный технический университет, Брянск, Россия
[1] bryansk-tu@yandex.ru✉
[2] ryabcev@yandex.ru
[3] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133

Аннотация. Разработка алгоритма применения матрицы MITRE ATT&CK для реагирования на инциденты информационной безопасности является важным этапом в обеспечении защиты информационных ресурсов организации. В разработке алгоритма необходимо учитывать специфику организации, ее инфраструктуру и угрозы, с которыми она сталкивается. Важно также регулярно обновлять алгоритм в соответствии с изменяющейся угрозовой ситуацией и новыми версиями матрицы MITRE ATT&CK.

Ключевые слова: информационная безопасность, реагирование на инциденты, матрица MITRE ATT&CK.

Для цитирования: Николаев Н. А., Рябцев А. А., Голембиовская О. М. Разработка алгоритма применения матрицы MITRE ATT&CK для реагирования на инциденты информационной безопасности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 202–206.

В условиях развивающихся технологий вопрос защиты информации и предотвращения инцидентов информационной безопасности становится все более актуальным, поскольку большинство значимых данных (коммерческая тайна, персональные данные и др.) начали полностью обрабатываться в электронном формате.

По данным отчета экспертного центра безопасности Positive Technologies [1] в последние два года количество проектов по расследованию инцидентов неуклонно растет. 40 % инцидентов связаны с деятельностью известных однозначно идентифицированных APT-группировок, оставшиеся 60 % связаны с деятельностью APT-группировок, которые на момент исследования не удалось однозначно идентифицировать, и других неустановленных злоумышленников, основным мотивом которых послужила финансовая выгода и (или) хактивизм, в том числе политической окраски.

Данные статистики подтверждают, что вопрос противодействия инцидентам информационной безопасности имеет высокую значимость для предприятий любого назначения, необходимо должное внимание уделять мониторингу и расследованию инцидентов для недопущения их в будущем.

Матрица MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) это общедоступная база знаний, разработанная корпорацией MITRE для того, чтобы помочь организациям оценить свою кибербезопасность. Применение матрицы MITRE ATT&CK необходимо в тех случаях, когда системы мониторинга сети на объекте отсутствуют, сработали некорректно или же не сработали по причине отсутствия отдельных правил реагирования, а также в тех ситуациях, когда средства сработали, но требуется дополнительная информация о действиях злоумышленника для расследования инцидента и (или) его предотвращения.

В MITRE ATT&CK можно получить информацию о том по каким признакам обнаружить реализацию той или иной техники реализации атаки, понять какая в данный момент у злоумышленника тактика (какова его цель в конкретный момент времени) и выделить перечень мер, которые следует применить для смягчения последствий того, что злоумышленник проник в инфраструктуру.

В случае если кибератака произошла на объекте, но применения автоматических средств для того чтобы обнаружить в чем причина недостаточно, действия группы реагирования должны быть следующие:

1. Обнаружить и изолировать (если это возможно) конечную точку куда идет соединение и от которой идет соединение до сервера управления злоумышленника, заблокировать адрес серверов атакующего на периметровых СЗИ или добавить в черный список у провайдера.
2. При наличии возможности перевести зараженные устройства в другой изолированный VLAN (виртуальная локальная компьютерная сеть) для изучения.
3. Выдвинуть версии того, какую тактику (техники) использует злоумышленник по имеющимся индикаторам компрометации и (или) составить приоритетный список техник, которые могут быть характерны для исследуемой системы, для того чтобы начать с ручную проверку с данных техник.

Также для выбора направления проверки можно использовать некоторые средства автоматического реагирования. Для диагностики подходят EDR-решения, поскольку в них встроены модули ретроспективы и специальные правила реагирования, а также XDR-решения внутри которых есть EDR с такой возможностью или возможностью отправлять команды и собирать артефакты для поиска индикаторов компрометации. При помощи подобных решений можно подключаться отдельно к каждому устройству системы и искать индикаторы компрометации.

4. После того как выбраны приоритетные тактики и техники, с которых следует начать ручной анализ, исследователь может подключить в работу матрицу MITRE ATT&CK. Выбрав тактику и технику, которую необходимо исследовать, он нажимает на технику и изучает ее описание, а также раздел «Обнаружение». И выполняет указания раздела на практике.

Например, по общей картине компрометации исследователь подозревает, что злоумышленник только получил первоначальный доступ в систему используя технику фишинг. В рамках матрицы он может изучить описание техники, а также информацию о том, как обнаружить в системе следы выполнения данной техники и источник ее реализации.

5. В случае получения подтверждения того, что на объекте была использована выбранная для исследования техника, специалистам объекта следует провести мероприятия, нейтрализующие влияние злоумышленника на систему (если данный пункт не был выполнен на этапе 1), с учетом того, что необходимо сохранить (зафиксировать) обнаруженные артефакты для дальнейшего расследования инцидента ИБ.

6. После того, как пройдена критическая стадия реагирования, специалистам необходимо смягчить возможные от инцидента ИБ последствия и сделать все возможное чтобы не допустить подобного инцидента в будущем, в чем тоже помогает матрица MITRE ATT&CK. В разделе «Меры по смягчению последствий» расположены указания к действию, позволяющие минимизировать последствия и вероятность повторения инцидента.

7. Если на объекте функционирует система мониторинга (например, SIEM-система) и при этом она сработала некорректно или не сработала вообще, следует провести процедуру по обогащению, в рамках которой разработать дополнительные правила корреляции, позволяющие обнаружить аномальные события инфраструктуры.

Общий алгоритм применения матрицы MITRE ATT&CK для реагирования на инциденты информационной безопасности представлен на рис. 1.

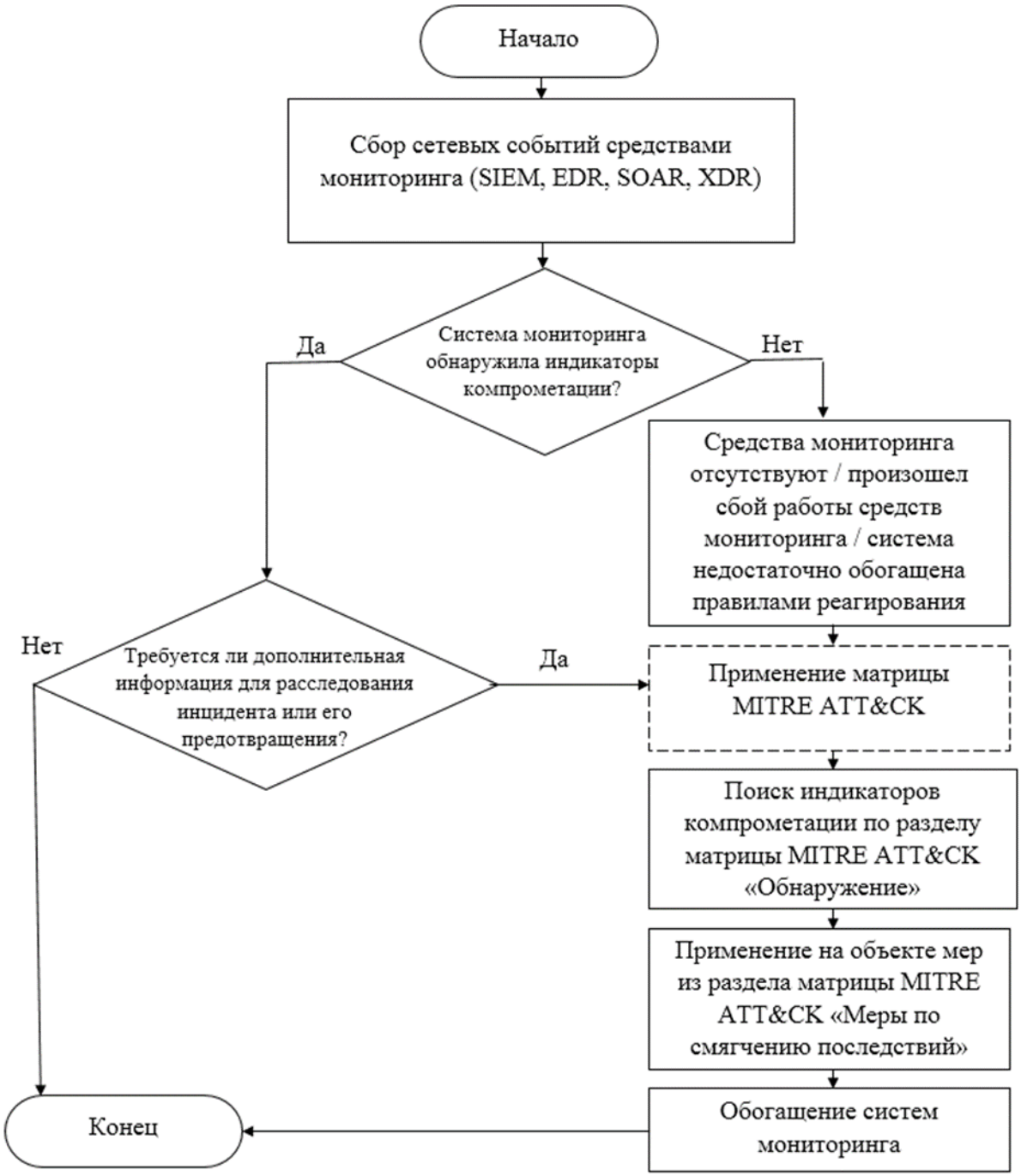


Рис. 1. Алгоритм применения матрицы MITRE ATT&CK для реагирования на инциденты информационной безопасности

Таким образом, представленный порядок действий, включающий в себя работу с матрицей MITRE ATT&CK позволяет обеспечить эффективное реагирование на инциденты информационной безопасности и попытку компрометации системы. Накопленный и собранный в рамках MITRE ATT&CK опыт исследователей помогает выстроить логику передвижения злоумышленника внутри инфраструктуры, остановить его продвижение вглубь сети и применить меры, смягчающие возможные последствия и уменьшающие вероятность наступления подобного инцидента ИБ вновь.

Список источников

1. Итоги расследований инцидентов ИБ в 2021–2023 годах [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/ (Дата обращения: 03.02.2024).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Николаев Н. А. – выпускник кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

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

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Николаев Н. А. – обработка материала, написание статьи (50 %).
Рябцев А. А. – сбор материала, частичное написание статьи (25 %).
Голембиовская О. М. – идея, научное редактирование (25 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 347.12

Правовой статус лица, разгласившего конфиденциальную информацию в киберсреде

Валерий Петрович Новиков
Брянский государственный технический университет, Брянск, Россия
asdf32a@yandex.ru, https://orcid.org/0009-0004-0686-8967

Аннотация. Отражены особенности прав и обязанностей нарушителя, допустившего разглашение конфиденциальной информации и тем самым допустившим административное правонарушение в информационно-телекоммуникационной сети «Интернет».

Ключевые слова: интернет, информационно-телекоммуникационная сеть, административная ответственность, участники производства по делу об административном правонарушении, субъект административной юрисдикции.

Для цитирования: Новиков В. П. Правовой статус лица, разгласившего конфиденциальную информацию в киберсреде // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 207–212.

Рассмотрение административно-процессуального положения участника производства по делам об административных правонарушениях в информационно-телекоммуникационных сетях "интернет" показало, что проблема реализации прав и законных интересов физических и юридических лиц в производстве по делам об административных правонарушениях требует определенных изменений. Появление современных средств вычислительной техники и телекоммуникаций привело не только к трансформации традиционных имущественных и неимущественных преступлений и административных правонарушений в новейшие формы, но и к появлению правонарушений, специфических для киберсреды [2, 37].

Одновременно права и обязанности потерпевшего от административных правонарушений в киберсреде и лица, в отношении которого осуществляют производство по делу об административном правонарушении, не всегда поддаются кореляции.

Необходимо иметь ввиду, что к лицам, совершившим административные правонарушения в киберсреде, нельзя применять административное наказание и меры обеспечения производства по делу об административном правонарушении иначе как это регламентировано КоАП РФ. Статья 25.1 указанного источника устанавливает совокупность прав лиц, которых

привлекают к административным наказаниям. Необходимость их обязательного разъяснения является очень важной гарантией соблюдения указанных прав.

Однако имеется проблема в реализации обязанности по разъяснению лицу, в отношении которого ведется производство по делу об административном правонарушении в киберсреде, а также потерпевшему указанных прав, поскольку их перечень довольно широк, а нормы, их содержащие, могут находиться в разных статьях Кодекса.

В связи с этим считаем что необходимо перечислить хотя бы приблизительно перечень прав лица, в отношении которого ведется производство по делу об административном правонарушении в киберсреде.

Итак, в самом общем виде лицо, в отношении которого ведется производство по делу об административном правонарушении в киберсреде (и физическое, и юридическое, включая и особых субъектов административной ответственности):

1) может быть подвергнутым административному наказанию и мерам обеспечения производства по делу об административном правонарушении только на основании регламентации, установленной КоАП РФ; быть наказанным только на основании полного и всестороннего изучения дела и рассмотрения доказательств, в т.ч. учитывая личность нарушителя, обстоятельств, смягчающих или отягчающих административную ответственность, его имущественного положения; рассчитывать на открытое рассмотрение дела об административных правонарушениях (если нет препятствующих этому обстоятельств); рассчитывать на использование норм, смягчающих ответственность, либо устраняющих ее; реализацию принципа равенства всех перед законом и требовать (для физических лиц) недопустимость дискриминации в зависимости от пола, расы, национальности, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям; (для юридических лиц) с учетом места расположения, организационно-правовых форм, соподчиненности и других обстоятельств; быть привлеченным к административной ответственности только за те административные правонарушения, в отношении которых установлена его вина, и, тогда, исходить из невозможности привлечения его к ответственности в других случаях; предполагать себя и считаться невиновным, пока его вина не будет доказана в порядке, предусмотренном КоАП РФ, и установлена вступившим в законную силу постановлением судьи, органа, должностного лица, рассмотревших материал; предполагать, что толкование всех неустраненных сомнений в виновности будет в его пользу; в случае применения мер административного принуждения предполагать недопустимость принятия решений и совершения действий (бездействия), унижающих человеческое достоинство; предполагать возможность освобождения от административной ответственности при совершении административного правонарушения в условиях крайней необходимости; предполагать возможность освобождения от административной

ответственности при совершении административного правонарушения в состоянии невменяемости; предполагать возможность освобождения от административной ответственности при совершении малозначительного административного правонарушения; предполагать возможность освобождения от административной ответственности при истечении срока привлечения к административной ответственности; считать себя более не подвергнутым административному наказанию, если истек один год со дня окончания исполнения постановления об административном наказании; предполагать возможность рассмотрения дела по месту, где совершено административное правонарушение; предполагать возможность рассмотрения (на основании ходатайства), дела по месту своего жительства; предполагать возможность получения извещения о времени и месте, где будет рассмотрено дело;

2) предполагать соблюдение запрета на привлечении к административной ответственности за одно и то же административное правонарушение дважды;

3) вправе: получить информацию о своих правах, получить комментарий своих прав; ознакомиться со всеми материалами; предъявлять объяснения как устно, так и письменно, требовать их закрепления в материале об административном правонарушении, материале о применении меры обеспечения производства по делу об административном правонарушении, протоколе рассмотрения дела об административном правонарушении; предъявлять доказательства; ходатайствовать об отводах для защитника, представителя, специалиста, эксперта либо переводчика; лицу, ведущему производство по делу об административном правонарушении; принимать помощь законных представителей а также юридическую помощь защитника с момента возбуждения дела об административном правонарушении; иметь в качестве защитника как адвоката так и иное лицо; не давать информацию против себя самого, супруга и близких родственников (среди которых родители, дети, усыновители, усыновленные, родные братья и сестры, дедушки, бабушки, внуки); давать показания, приносить ходатайства и отводы, подавать жалобы как на родном языке так и на другом языке общения; использовать услуги переводчика, ходатайствовать о замене переводчика; не настаивать на своей невиновности; письменно, либо с помощью средств аудиозаписи фиксировать процесс рассмотрения дела об административном правонарушении; получать информацию о поступивших внепроцессуальных обращениях в суд, в производстве которого находится материал об административном правонарушении; предъявлять ходатайства, настаивать на их рассмотрении с указанием о принятых мерах в определении; настаивать на возмещении расходов, возникших в связи с присутствием в суде в случае необоснованного привлечения к административной ответственности или безосновательного возбуждения производства по делу об административном правонарушении; настаивать на возмещении убытков, понесенных в результате незаконного и необоснованного привлечения к административной ответственности; получать информацию о времени и месте рассмотрения материала, для этого непосредственно либо в через своего законного

представителя быть уведомленным об этом факте; непосредственно либо в лице своего законного представителя быть извещенным обо всех происходящих при производстве по делу об административном правонарушении процессуальных действиях либо полученных результатах; предполагать возможность участия в рассмотрении материала и в случае невозможности присутствия в связи с уважительными причинами настаивать на отложении рассмотрения дела; предполагать возможность обязательного участия при рассмотрении в отношении него дела об административном правонарушении, если оно влечет административный арест, административное выдворение за пределы Российской Федерации лица без гражданства либо иностранного гражданина или обязательные работы; подавать жалобу на использование мер обеспечения производства по делу; подавать жалобу на постановление по делу об административном правонарушении; настаивать на присутствии понятых в тех случаях, которые установлены законом; получить информацию из заключения эксперта; наблюдать за отбором проб и образцов, вписывать в протокол об отборе образцов и проб свои замечания; настаивать на отборе арбитражной пробы; предъявлять свои доказательства; присутствовать при изъятии вещественных доказательств и документов, настаивать на составлении их описи; настаивать на оценке вещественных доказательств; настаивать на подтверждении исправности и поверки специализированных технических средств, с помощью которых выявлено правонарушение; присутствовать при проведении осмотра места совершения правонарушения; настаивать на разъяснении обязанностей и прав при осмотре места происшествия; при ознакомлении с протоколом о проведении осмотра места совершения правонарушения вписать туда свои замечания; настаивать на подтверждении полномочий лиц, осуществляющих производство по делу об административном правонарушении и производящих некоторые процессуальные действия; присутствовать при составлении протокола по делу об административном правонарушении, для чего быть поставленным в известность о времени и месте составления протокола непосредственно или с помощью своего законного представителя; прочитать протокол по делу об административном правонарушении, взять его копию; знать о возбуждении дела об административном правонарушении; получить непосредственно или с помощью своего законного представителя фотокопию определения о возбуждении дела об административном правонарушении и осуществления административного расследования; получить непосредственно либо с помощью своего законного представителя фотокопию определения о продлении срока административного расследования; получить постановление по делу об административном правонарушении; на пояснение в постановлении сроков и порядка обжалования постановления; на освобождение при подаче жалобы на постановление по делу об административном правонарушении от уплаты государственной пошлины; на пересмотр решения, вынесенного по жалобе на постановление по делу об административном правонарушении; на передачу постановления для исполнения только с даты вступления его в законную силу,

но не раньше, чем будут рассмотрены жалоба, протест на постановление по делу об административном правонарушении и (или) на последующее решение по жалобе, протесту, вступившее в законную силу постановление по делу об административном правонарушении.

Однако сформулировать все поименованные права в одной статье КоАП РФ довольно проблематично.

Так же следует отметить, что лица (как физические так и юридические) могут вступить в административно-процессуальные правоотношения как добровольно, так и быть вовлеченным в них в принудительном порядке (к примеру, в качестве лица, в отношении которого ведется производство по делу об административном правонарушении). В данной связи актуален вопрос о порядке вовлечения (принудительно или добровольно) в производство по делу об административном правонарушении потерпевшего.

Но как ранее я писал, возникают сложности с установлением личности потерпевшего, если тот не желает привлекать к ответственности лиц, в отношении которых имеется повод к возбуждению дела об административном правонарушении. Так как с одной стороны в производстве по делам об административных правонарушениях нет дефиниции «дела частного обвинения» (дела, которые возбуждают по заявлению потерпевших), а с другой — лицо, осуществляющее производство по делу, обязано установить размер и характер нанесенного административным правонарушением ущерба, потерпевший в производство по делу вовлекается принудительно. И здесь можно было бы предусмотреть освобождение физического лица, совершившего административное правонарушение, влекущее административную ответственность от ответственности, по требованию потерпевшего либо его законного представителя от административной ответственности, если оно примирилось с потерпевшим либо его законным представителем [3, 56].

Данные положения необходимо учитывать в процессе моделирования защиты данных в киберсреде [4, 51].

Список источников

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ // Собрание законодательства РФ. 07.01.2002, N 1 (ч. 1), ст. 1.

2. Гулак М.Л., Шпичак С.А. Некоторые криминалистически значимые признаках компьютерных преступлений // Информационная безопасность и защита персональных данных: Проблемы и пути их решения [Текст]+[Электронный ресурс]: материалы VI Межрегиональной научно-практической конференции / под ред. О.М. Голембиовской. – Брянск: БГТУ,2014. – 175 с.

3. Новиков В.П. Физические и юридические лица как потерпевшие по делам об административных правонарушениях: Дис. ... к.ю.н. М., 2004. С. 56.

4. Рытов М.Ю. Моделирование процессов защиты данных в информационных порталах региональных органов исполнительной власти / Рытов М.Ю, Еременко В.Т., Горлов А.П. // Вестник информационных технологий. 2016. - № 9 (97). - С. 48-53.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторе

Новиков В. П. – к. ю. н., доцент кафедры «Системы информационной безопасности ФГБОУ ВО «БГТУ».

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Анализ нормативно-правовой базы в области реагирования на инциденты информационной безопасности

Николай Иванович Нуждин[1]✉, Оксана Михайловна Голембиовская[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] kolya32.bryansk.ru@gmail.com✉, https://orcid.org/0009-0002-4852-6733
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133

Аннотация. В статье проводится анализ нормативно-правовых актов, регулирующих реагирование на инциденты информационной безопасности. Рассматривается подходы управления инцидентами информационной безопасности в организациях. Выявлена необходимость формализации в области реагирования на инциденты информационной безопасности.

Ключевые слова: реагирование на инциденты информационной безопасности, управление компьютерными инцидентами, минимизация потенциальных угроз, предупреждение вероятных угроз.

Для цитирования: Нуждин Н. И., Голембиовская О. М. Анализ нормативно-правовой базы в области реагирования на инциденты информационной безопасности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 213–217.

Защита информации одна из первостепенных задач современного общества. В условиях современной геополитической ситуации и уровня развития информационных технологий, информация является одним из самых ценных активов, а обладание отдельными данными может существенно влиять на ход общей ситуации.

На фоне данных условий стабильно растет статистика осуществляемых кибератак, более того, они становятся все изощреннее, точнее и направленнее. По данным экспертов ГК «Солар», за январь и февраль 2024 года доля атак высокой критичности уже выросла с 2 % до 6,3 % по сравнению с IV кварталом 2023 года. Кроме того, с 73 % до 80 % увеличилась доля инцидентов с применением вредоносного софта, и до 15 % выросла доля веб-атак. За 2023 год число событий информационной безопасности (далее ИБ) по сравнению с 2022 годом выросло на 64 % и составило 1,5 млн событий. Доля подтверждённых инцидентов оставалась стабильной. Однако эксплуатация уязвимостей показала рост в 2 раза год к году, до 11,5 % [9].

Данная статика подтверждает довод о том, что сфера защиты информации нуждается в развитии и отдельно отмечается важность борьбы с эксплуатацией уязвимостей, которые являются основным способом проникновения в систему.

Нормативно-правовая база закрепляет ключевые основы изучаемой области, которые имеют первоочередное значение в масштабах государства. Анализ нормативно-правовых актов в области реагирования на инциденты ИБ позволяет изучить основные требования и порядок реагирования на инциденты ИБ.

ГОСТ Р 59710-2022 Защита информации. Управление компьютерными инцидентами. Общие положения [1] устанавливает общие требования и принципы управления компьютерными инцидентами в организации. Содержит основные термины, связанных с управлением компьютерными инцидентами, а также принципы построения системы управления инцидентами и процедуры обработки инцидентов.

Также документ содержит рекомендации по организации процесса обработки инцидентов, включая этапы выявления, анализа, реагирования и восстановления после инцидента.

Раздел 5 ГОСТ Р 59712-2022 Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты [2] посвящен обнаружению и регистрации компьютерных инцидентов.

Раздел 6 данного стандарта посвящен реагированию на компьютерные инциденты. Он описывает основные этапы и процедуры, которые должны быть выполнены при возникновении инцидента, начиная с определения типа инцидента и его классификации, и заканчивая документированием и анализом произошедшего случая. Также описывается процедура уведомления ответственных лиц о произошедшем инциденте, организация работы по ликвидации уязвимостей, восстановлению систем и данных, а также мониторинг и анализ последствий инцидента.

Раздел 7 данного стандарта посвящен фиксации материалов, связанных с возникновением компьютерных инцидентов, и установлению причин и условий их возникновения.

В разделе 8 рассматривается процесс оценки эффективности мер по предотвращению и устранению компьютерных инцидентов, что позволяет выявить слабые места в системе управления компьютерными инцидентами.

В ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» [3] приведены цели, этапы, преимущества, а также примеры инцидентов ИБ и их причин.

Стандарт определяет процессы, процедуры и принципы, которые должны быть реализованы для эффективного управления инцидентами ИБ. Он помогает организациям разрабатывать планы и стратегии по предотвращению, обнаружению и реагированию на инциденты, связанные с ИБ.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 «Обеспечение информационной безопасности организаций банковской

системы Российской Федерации. Менеджмент инцидентов информационной безопасности» [4] представляет собой набор рекомендаций, направленных на защиту информационных ресурсов банков и обеспечение эффективного реагирования на инциденты ИБ.

На основе этого стандарта разрабатываются рекомендации по эффективному применению соответствующих методов и инструментов, а также по повышению квалификации специалистов в области ИБ.

Международный стандарт ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management [5] предоставляет рекомендации по управлению инцидентами ИБ. Стандарт описывает процесс управления инцидентами, начиная с их обнаружения и классификации до анализа, реагирования и восстановления, что позволяет организациям минимизировать их воздействие на бизнес-процессы и обеспечивать защиту конфиденциальности, целостности и доступности данных.

ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response [6] охватывает все аспекты управления инцидентами ИБ, включая детектирование, реагирование, расследование и управление инцидентами. Он также содержит рекомендации по управлению рисками и предотвращению инцидентов ИБ.

Основной целью стандарта является обеспечение адекватного управления инцидентами ИБ в организации, что помогает минимизировать потенциальные угрозы и ущерб от нарушений безопасности.

Стандарт выполнения испытаний на проникновение — The Penetration Testing Execution Standard (PTES) [7] является набором рекомендаций и процедур для проведения тестирования на проникновение в информационные системы. PTES также включает в себя разделение испытаний на различные фазы, включая фазу подготовки, исследования, анализа, эксплуатации и завершения. Каждая фаза имеет свои цели и задачи, которые помогают обеспечить полное и всестороннее тестирование системы. Его можно использовать как отдельный контрольный список или как часть более масштабной методологии тестирования.

Руководство NIST Special Publications 800 Series Подраздел SP 800-115 Technical Guide to Information Security Testing and Assessment [8] содержит практические рекомендации по разработке, внедрению и поддержанию процессов и процедур технического тестирования и экспертизы ИБ. Они могут использоваться для нескольких целей, таких как поиск уязвимостей в системе или сети и проверка соответствия политике или другим требованиям.

Документ представляет собой подробное руководство по методикам и инструментам, используемым при проведении испытаний ИБ, включая планирование тестирования, сбор данных, анализ результатов и разработку отчетов.

На основе проведенного анализа, можно сделать вывод, о том, что на данный момент наблюдается недостаток формализации в области реагирования

на инциденты ИБ, что может осложнять эффективное управление кибербезопасностью и обеспечение защиты информации в стране.

Таким образом, выявлена необходимость формализации в области реагирования на инциденты информационной безопасности. Рассмотрение этих аспектов в комплексе позволит усовершенствовать безопасность в информационной сфере и защите информационных ресурсов от угроз и атак.

Список источников

1. ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения», 02.12.2022.

2. ГОСТ Р 59712-2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты», 08.12.2022.

3. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», 16.06.2020.

4. Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности" (приняты и введены в действие распоряжением Банка России от 17 мая 2014 г. № Р-400)

5. ISO/IEC 27035-1:2023 «Information technology — Information security incident management — Part 1: Principles and process», 13.02.2023.

6. ISO/IEC 27035-2:2023 «Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response», 13.02.2023.

7. Стандарт выполнения испытаний на проникновение – The Penetration Testing Execution Standard (PTES).

8. NIST Special Publications 800 Series Подраздел SP 800-115 Technical Guide to Information Security Testing and Assessment.

9. ГК «Солар» рассказала, что с начала 2024 года число высококритичных атак выросло в три раза [Электронный ресурс] – Режим доступа: https://habr.com/ru/news/796305/ (Дата обращения: 20.03.2024).

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Нуждин Н. И. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Нуждин Н. И. – идея, сбор материала, обработка материала, написание статьи, научное редактирование текста (90 %).

Голембиовская О. М. – научное руководство (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Анализ нормативно-правовой базы и научной литературы в области противодействия нарушителям информационной безопасности и развития цифровой гигиены

Владислав Романович Попенко[1]✉, Оксана Михайловна Голембиовская[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] vladikpopenko@mail.ru✉, https://orcid.org/0009-0007-3152-8958
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133

Аннотация. В статье анализируются ключевые нормативно-правовые акты Российской Федерации в области противодействия нарушителям информационной безопасности и развития цифровой гигиены. Также обозревается Всероссийская программа кибергигиены и делается вывод о необходимости разработки методики «снижения потенциальной опасности внешнего нарушителя за счет повышения уровня цифровой гигиены сотрудников», которая позволит усовершенствовать систему защиты объекта от возможного внешнего воздействия.

Ключевые слова: Всероссийская программа кибергигиены, информационная безопасность, нормативно-правовые акты, противодействие нарушителям, цифровая гигиена.

Для цитирования: Попенко В. Р., Голембиовская О. М. Анализ нормативно-правовой базы и научной литературы в области противодействия нарушителям информационной безопасности и развития цифровой гигиены // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 218–221.

Информационная безопасность как сфера набирает все большие обороты. Усложнение геополитической обстановки поспособствовало резкому росту статистики в части реализации атак и осознанию как частными, так и государственными организациями необходимости применения мер и средств защиты.

По данным исследования Positive Technologies за 2023 год 74 % респондентов считают свои организации недостаточно защищенными от сложных и целевых атак. В IV квартале 2023 года доля целевых атак на организации увеличилась до 78 % от общего числа. Одной из причин такого роста стала неспособность традиционных средств защиты информации противодействовать таргетированным атакам. Применяемые в них шпионское ПО, шифровальщики, вайперы и другие зловреды могут проникать в контур компании, оставаясь незамеченными для антивирусов [3, 5].

Данные, приведенные в исследовании, свидетельствуют о том, что количество атак стремительно возрастает, большая часть из них это целевые APT-атаки, при этом организации не готовы к отражению данной угрозы.

В нормативно-правовой базе закрепляются ключевые основы изучаемой области, которые имеют первоочередное значение в масштабах государства. Анализ отечественных НПА позволяет понять основные требования и порядок противодействия нарушителям информационной безопасности и особенности развития цифровой гигиены.

Под данную тему подходят лишь четыре отечественных документа:

1. Методический документ «Методика оценки угроз безопасности информации» [2].

Документ закрепляет тринадцать типов нарушителей ИБ. Для каждого из них описаны возможные цели реализации угроз и уровень потенциальных возможностей. Кроме того, выделен перечень с тактиками и техниками, которые могут ими использоваться для реализации атак на систему.

2. Распоряжение Правительства РФ от 22 декабря 2022 г. № 4088-р «О Концепции формирования и развития культуры информационной безопасности граждан РФ» [3].

Документ утверждает концепцию формирования и развития культуры информационной безопасности граждан РФ, заключающуюся в комплексном подходе информирования населения по вопросам ИБ путем использования для каждой возрастной группы актуальных для них средств коммуникации.

3. Постановление Правительства РФ от 19.08.2015 N 857 «Об автоматизированной информационной системе «Реестр нарушителей прав субъектов персональных данных» (вместе с «Правилами создания, формирования и ведения автоматизированной информационной системы «Реестр нарушителей прав субъектов персональных данных») [4].

Постановление описывает правила создания, формирования и ведения специального реестра на базе автоматизированной информационной системы, а также критерии определения оператора автоматизированной информационной системы, в целях привлечения к формированию и ведению такого реестра.

4. Приказ Роскомнадзора от 22.07.2015 N 84 «Об утверждении Порядка взаимодействия оператора реестра нарушителей прав субъектов персональных данных с провайдером хостинга и Порядка получения доступа к информации, содержащейся в реестре нарушителей прав субъектов персональных данных, оператором связи» (Зарегистрировано в Минюсте России 14.08.2015 N 38532) [Кодекс] [5].

Данный документ устанавливает порядок взаимодействия оператора реестра с провайдером хостинга и порядок получения доступа к информации, содержащейся в реестре, оператором связи.

Несмотря на, скромную нормативно-правовую базу, связанную с цифровой гигиеной, государство обращает внимание на данную проблему и организует различные программы, например, существует Всероссийская программа кибергигиены.

Данная программа стартовала в 2022 году в рамках федерального проекта «Информационная безопасность» национального программы «Цифровая экономика».

Для реализации программы был запущен раздел на портале Госуслуг, который содержит несколько блоков, посвящённых различным типам угроз, а также набор памяток с важными советами по кибербезопасности.

Перечень затрагиваемых тем включает в себя:

- Фишинг;
- Кибербуллинг;
- взлом аккаунтов;
- телефонное мошенничество;
- мобильные угрозы.

В рамках проекта выделены следующие направления:

«КиберЗОЖ» — направлен на защиту данных, включает в себя информацию об основных правилах личной информационной безопасности, участниками являются пользователи сети «Интернет».

«Кибербуллинг или интернет-травля» — волна оскорблений или угроз в социальных сетях или мессенджерах в адрес конкретного человека. Именно детям и подросткам в программе уделяется особое внимание, так как они наиболее активная категория пользователей в Интернете и, чтобы общение в интернете не переросло в травлю, проект рассказывает, как определить агрессора, что ему ответить и как не стать жертвой травли в интернете.

«Выучи свою роль» — этот проект направлен на защиту от телефонных мошенников. На странице проекта представлена инструкция, как не стать жертвой мошенников, а также есть возможность поговорить с чат-ботом, который имитирует мошенническую схему, и закрепить полученную информацию. Данной атаке подвержены все обладатели телефонов.

«Прокачай скилл защиты» — этот проект направлен преимущественно на игроманов. Предлагает ряд правил, благодаря которым можно избежать потерю аккаунта, купленного в игре инвентаря, а также защите от вирусов.

Также в программу вошел всероссийский мониторинг уровня грамотности граждан по вопросам информационной безопасности. Он направлен на выявление аспектов личной информационной безопасности, в которых россиянам не хватает знаний. Это, в дальнейшем, позволит оптимизировать программу и сделать ее еще более эффективной.

На основе анализа всей вышеперечисленной информации, можно сделать выводы, о том, что на данный момент государство принимает шаги в развитии цифровой гигиены граждан и запускает для этого специальные программы в рамках концепцию формирования и развития культуры ИБ. Но в нормативно-правовых актах Российской федерации не определена зависимость между нарушителями информационной безопасности и уровнем цифровой гигиены сотрудников.

Отсутствие сформулированной зависимости между нарушителями информационной безопасности и уровнем цифровой гигиены сотрудников демон-

стрирует необходимость разработки методики «снижения потенциальной опасности внешнего нарушителя за счет повышения уровня цифровой гигиены сотрудников», для усовершенствования системы защиты объекта от возможного внешнего воздействия со стороны злоумышленников.

Список источников

1. Защищенность конечных точек российских компаний [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/zashchishchennost-konechnyh-tochek-rossijskih-kompanij/#id2 (Дата обращения: 20.03.2024).

2. «Методический документ. Методика оценки угроз безопасности информации», утв. ФСТЭК России 05.02.2021.

3. Распоряжение Правительства РФ от 22 декабря 2022 г. № 4088-р «О Концепции формирования и развития культуры информационной безопасности граждан РФ».

4. Постановление Правительства РФ от 19.08.2015 N 857 «Об автоматизированной информационной системе «Реестр нарушителей прав субъектов персональных данных» (вместе с «Правилами создания, формирования и ведения автоматизированной информационной системы «Реестр нарушителей прав субъектов персональных данных»).

5. Приказ Роскомнадзора от 22.07.2015 N 84 «Об утверждении Порядка взаимодействия оператора реестра нарушителей прав субъектов персональных данных с провайдером хостинга и Порядка получения доступа к информации, содержащейся в реестре нарушителей прав субъектов персональных данных, оператором связи» (Зарегистрировано в Минюсте России 14.08.2015 N 38532) [Кодекс].

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Попенко В. Р. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Попенко В. Р. – идея, сбор материала, обработка материала, написание статьи, научное редактирование текста (90 %).

Голембиовская О. М. – научное руководство (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Особенности атрибуции кибератак

Роман Игоревич Рукавичников[1]✉, Екатерина Владимировна Кондрашова[2], Елизавета Андреевна Музалевская[3], Кирилл Евгеньевич Шинаков[4]
[1, 2, 3, 4] Брянский государственный технический университет, Брянск, Россия
[1] bryansk-tu@yandex.ru✉
[2] kondrashova_katerina@bk.ru
[3] lizamuz2002@yandex.ru
[4] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. Атрибуция кибератак — это процесс определения и идентификации лиц, стоящих за совершением кибернарушений. Этот процесс представляет собой одну из ключевых задач в области кибербезопасности, так как правильная и точная атрибуция позволяет не только наказывать злоумышленников, но и принимать меры для предотвращения будущих атак.

Ключевые слова: кибератака, информационная безопасность, атрибуция кибератак.

Для цитирования: Рукавичников Р. И., Кондрашова Е. В., Музалевская Е. А., Шинаков К. Е. Особенности атрибуции кибератак // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 222–226.

Ситуация относительно количества кибератак в России нестабильная, показатели с каждым годом ухудшаются. По данным НКЦКИ ежедневно более 170 кибератак направлено на российские компании. В первом полугодии 2023 года участились координированные целевые атаки одновременно с «фоновым шумом» в виде массовых поверхностных атак, с целью отвлечения внимания. С середины года хакеры действуют «точечно», используя данные, полученные в результате утечек [1].

Развитие набирают APT-атаки. Это целевые атаки на отдельную инфраструктуру, как правило они хорошо спланированы, сильно распределены во времени (от нескольких дней до нескольких лет) и включают несколько этапов, сочетая в себе комбинацию различных методов реализации (социальная инженерия, эксплуатация уязвимостей, вредоносное ПО и т. д.). Знание или предположение того, какая группировка стоит за проводимой атакой может помочь подобрать более точечные меры противодействия.

Процесс установления злоумышленника или преступной группировки, стоящей за кибератакой или вредоносной кампанией при помощи организационных мероприятий и технических средств, называют атрибуцией.

Основной особенностью атрибуции в России является отсутствие ее веса в правовом поле. Как правило, доказать правдивость выводов аналитика, проводящего атрибуцию кибератаки невозможно, потому что вывод делается на основе косвенных признаков. Исключением являются три случая:

- злоумышленник пойман с поличным;
- злоумышленник признался в совершении кибератаки сам (однако важно учитывать наличие ситуаций, когда кто-то один берет на себя всю вину);
- произошла утечка информации (если это не направленная дезинформация).

Таким образом, в настоящий момент целью атрибуции является вынесение предположения о том, кто стоит за реализацией атаки, какие цели он преследует и какими инструментами пользуется, для того чтобы минимизировать возможные последствия от продвижения злоумышленника вглубь инфраструктуры не допустить повторной реализации подобной атаки.

Исследователь должен быть ориентирован на поиск ляпов, ошибок, отличительных особенностей, которые в дальнейшем могут быть полезны в вопросах противодействия. В таблице 1 представлены примеры классификации и атрибуции кибератак.

Таблица 1

Примеры классификации и атрибуции кибератак

Пример атаки	Уязвимость	Программы	Цели	Источник	Технические приемы	Группа
Атака на посетителей форумов, посвященных исламскому джихаду [2]	Уязвимость в Firefox 17 (TOR Browser)	Неизвестный эксплойт	В список целей не были включены IPадреса Иордании, Турции и Египта, но были включены пользователи определенного провайдера спутникового интернета в Афганистане	Серверы, используемые Equation Group	Атаке подвергались только авторизованные пользователи, которые зашли с определенных IP-адресов	Equation Group
Атака на правительственные организации с использованием уязвимости CVE2017-11882 [2]	Уязвимость в Microsoft Office CVE-2017-	Backdoor, написанный на PowerShellPOWRUNER	Правительственные организации в странах Ближнего Востока	Не установлен	Массовые рассылки сообщений с использованием скомпрометированных учетных записей.	APT 34

Пример атаки	Уязвимость	Программы	Цели	Источник	Технические приемы	Группа
	11882				Социальная инженерия.	
Атака на энергетическую компанию госсектора [3]	-	Модификации трояна Decoy Dog	Организации на территории Российской Федерации	Аккаунт с юзернеймом @lahat	Предварительный доступ к хосту, помещение файла в загрузчик	Hellhounds
Атаки на организации различных сфер и масштабов в России и Сербии [4]	Не установлена	ВПО ShadowPad, бэкдор Deed RAT, ВПО Voidoor, публично доступные утилиты для продвижения по сети	Шпионаж и кража конфиденциальной информации	Не установлен	Переиспользование старых адресов сайтов, с помощью создания на них доменов более высокого уровня, внедрение ВПО, использование уязвимостей, разведка при помощи Acunetix и использование слабых мест	Space Pirates
Атаки на правительственный сектор России, Белоруссии, Азербайджана, Турции, Словении [5]	Уязвимость в редакторе уравнений из пакета Microsoft Office CVE-2017-11882	Полезная нагрузка ВПО	Шпионаж и кража конфиденциальной информации	Фишинговое письмо с вредоносным вложением - документ (как формата .doc, так и .docx), реализующий атаку типа Template Injection.	Целенаправленные рассылки, основанные на профессиональной сфере атакуемых	Cloud Atlas

Основой для проведения процедуры атрибуции также могут быть данные, полученные из публичных исследований. Например, отчеты Лаборатории Касперского об аналитике APT-атак [6], отчеты PT ESC Threat Intelligence [7].

Таким образом, атрибуция, выполненная квалифицированными специалистами-аналитиками, позволяет на основе применяемых технических приёмов определить группировку, стоящую за реализацией инцидента, предпринять наиболее эффективные меры противодействия и максимально сократить вероятность реализации инцидента со стороны данной и подобных группировок в будущем.

Список источников

1. Positive Technologies: какие уязвимости будут главными угрозами в 2023 году [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/apt-cloud-atlas-unbroken-threat/ (Дата обращения: 30.01.2024).

2. Атрибуция кибератак [Электронный ресурс] – Режим доступа:https://www.imemo.ru/files/File/ru/conf/2021/22062021/22062021-Markov-Prez.pdf (Дата обращения: 30.01.2024).

3. Hellhounds: операция Lahat [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/hellhounds-operaciya-lahat/ (Дата обращения: 30.01.2024).

4. Space Pirates [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/space-pirates-exploring-non-standard-techniques-new-attack-vectors-and-grouping-tools/ (Дата обращения: 30.01.2024).

5. APT Cloud Atlas: Unbroken Threat [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/apt-cloud-atlas-unbroken-threat/ (Дата обращения: 30.01.2024).

6. Отчеты APT[Электронный ресурс] – Режим доступа: https://securelist.com/category/apt-reports/ (Дата обращения: 30.01.2024).

7. PT ESC Threat Intelligence [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/ (Дата обращения: 30.01.2024).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Рукавичников Р. И. – выпускник кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Кондрашова Е. В. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Музалевская Е. А. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Рукавичников Р. И. – обработка материала, написание статьи (50 %).
Кондрашова Е. В. – сбор материала, частичное написание статьи (17 %).
Музалевская Е. А. – сбор материала, частичное написание статьи (17 %).
Шинаков К. Е. – идея, научное редактирование (16 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004

Методика оценки защищенности критической информационной инфраструктуры

Михаил Юрьевич Самков
Брянский государственный технический университет, Брянск, Россия
samkov.misha@mail.ru, https://orcid.org/0009-0004-2694-6766

Аннотация. В статье представлена методика оценки защищенности критической информационной инфраструктуры на основании анализа организационно-технической документации, технической защиты и мониторинга информационной безопасности.

Ключевые слова: критическая информационная инфраструктура (КИИ); оценка защищенности; информационная безопасность.

Для цитирования: Самков М. Ю. Методика оценки защищенности критической информационной инфраструктуры // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 227–232.

В рамках данной статьи приведена методика оценки защищенности объектов КИИ, которую можно применить к любой сфере функционирования.

В общем виде процесс оценки защищенности (Z) объектов КИИ состоит из следующих этапов:

1. Оценка организационно-технической документации (D).
2. Оценка технической защиты (T).
3. Оценка реализации мониторинга (M).

Методика оценки сформирована на основе подхода, представленного Отраслевым Стандартом Банка России СТО БР ИББС-1.2-2014 [1]. По каждому направлению оценки определяются общие показатели, подробно разъясняющие, насколько объект критической информационной инфраструктуры соответствует требованиям законодательства. Групповой показатель, который является обобщенным показателем, формируется из нескольких частных показателей, включающих критерии соответствия. Оценка группового показателя осуществляется путем вычисления отношения суммы частных показателей, входящих в него, к общему числу критериев частных показателей. В итоге определяется уровень соответствия объекта критической информационной инфраструктуры законодательным требованиям по данному направлению оценки. Чтобы стандартизировать оценку по общим показателям, улучшить точность и надежность оценки, предусматривается использование дополнительной характеристики — весовой коэффициент.

Рассмотрим каждый этап оценки защищенности объектов КИИ подробнее.

Оценка организационно-технической документации.

Основные законодательные акты, действующие на территории Российской Федерации и определяющие требования по защите критической информационной инфраструктуры, которые служат основой для проведения оценки соответствия, включают следующие документы:

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [2];
- Постановление Правительства РФ от 08.02.2018 № 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» [3];
- Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [4];
- Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [5];
- Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [6];

На основе представленных документов, была составлена группа показателей, приведенная в табл. 1.

Таблица 1

Группа показателей организационно-технической документации

№	Наименование показателя	Значение при соответствии требованиям	Весовой коэффициент
1	Приказ о создании комиссии по категорированию	0,033	0,3
2	Положение о комиссии по категорированию	0,033	
3	Заключение о наличии процессов и объектов	0,033	
4	Перечень объектов КИИ	0,033	
5	Модель угроз	0.033	
6	Акт категорирования объектов КИИ	0,033	
7	Сведение о результатах категорирование объектов КИИ	0,033	

№	Наименование показателя	Значение при соответствии требованиям	Весовой коэффициент
8	Политика безопасности КИИ	0,033	
9	Приказ о распределении ответственности в области КИИ	0,033	
10	Должностные инструкции лиц, ответственных за обеспечение безопасности КИИ	0,033	
11	Положение о подразделении, ответственном за обеспечение безопасности КИИ	0,033	
12	Политика планирования мероприятий по обеспечению защиты информации	0,033	
13	План мероприятий по обеспечению безопасности КИИ	0,033	
14	Политика аудита безопасности	0,033	
15	Приказ о создании комиссии по контролю уровня безопасности КИИ	0,033	
16	Политика идентификации и аутентификации	0,033	
17	Политика управления доступом	0,033	
18	Политика ограничения программной среды	0,033	
19	Политика защиты машинных носителей	0,033	
20	Инструкция по учету машинных носителей	0,033	
21	Политика антивирусной защиты	0,033	
22	Политика предотвращения вторжений	0,033	
23	Политика защиты технических средств	0,033	
24	Приказ об установлении контролируемой зоны	0,033	
25	Политика реагирования на компьютерные инциденты	0,033	
26	Порядок действий в нештатных ситуациях	0,033	
27	Порядок взаимодействия с ГосСОПКА	0,033	
28	Политика информирования и обучения работников	0,033	
29	Журнал ознакомления с организационно-распорядительной документацией по КИИ	0,033	
30	Журнал инструктажа работников по вопросам обеспечения безопасности КИИ	0,033	

Оценка технической защиты.

На основании приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» п. 22 на объекте КИИ должны быть реализованы следующие технические меры: идентификация и аутентификация (ИАФ), управление доступом (УПД), ограничение программной среды (ОПС), защита машинных носителей информации (ЗНИ), аудит безопасности (АУД), антивирусная защита (АВЗ), предотвращение вторжений (компьютерных атак) (СОВ), обеспечение целостности (ОЦЛ), обеспечение доступности (ОДТ), защита технических средств и систем (ЗТС), защита информационной (автоматизированной) системы и ее компонентов (ЗИС), реагирование на инциденты информационной безопасности (ИНЦ), управление конфигурацией (УКФ), управление обновлениями программного обеспечения (ОПО), защита среды виртуализации (ЗСВ).

На основе анализа технических мер, была составлена группа показателей, приведенная в табл. 2.

Таблица 2

Группа показателей технических мер

№	Наименование показателя	Значение при соответствии требованиям	Весовой коэффициент (W_T)
1	ИАФ	0,066	0,45
2	УПД	0,066	
3	ОПС	0,066	
4	ЗНИ	0,066	
5	АУД	0.066	
6	АВЗ	0,066	
7	СОВ	0,066	
8	ОЦЛ	0,066	
9	ОДТ	0,066	
10	ЗТС	0,066	
11	ЗИС	0,066	
12	ИНЦ	0,066	
13	УКФ	0,066	
14	ОПО	0,066	
15	ЗСВ	0,066	

Оценка реализации мониторинга информационной безопасности.

Мониторинг информационной безопасности и реагирование — это важные аспекты в обеспечении безопасности информационных систем и данных. Мониторинг информационной безопасности включает в себя непрерывное отслеживание и анализ всех аспектов работы информационной системы с целью выявления угроз, аномалий и инцидентов, которые могут нарушить ее защищенность и нормальное функционирование.

Реагирование в области информационной безопасности представляет собой набор мер, которые применяются для предотвращения или минимизации ущерба, возникшего в результате угроз или инцидентов в информационной системе. План реагирования обычно включает в себя определенные шаги, процедуры и полномочия для быстрого и эффективного реагирования на инциденты, а также восстановления нормального функционирования системы.

Важно, чтобы мониторинг и реагирование в области информационной безопасности были организованы системно, а также регулярно обновлялись и улучшались в соответствии с изменяющимся угрозами и технологическим окружением. Надежная система мониторинга и оперативное реагирование помогают своевременно выявлять, анализировать и реагировать на возможные угрозы, обеспечивая безопасность информационных ресурсов и защищая их от потенциальных атак и нарушений (табл. 3).

Таблица 3

Группа показателей мониторинг

№	Наименование показателя	Значение при соответствии требованиям	Весовой коэффициент (W_M)
1	На объекте реализован централизованный сбор событий безопасности	0,4	0,25
2	На объекте реализован централизованный сбор событий безопасности на всех устройствах, имеющих доступ в «Интернет»	0,4	
3	Разработаны документация, определяющая порядок реагирования на инциденты	0,2	

На основе показателей выше, оценка защищенности рассчитывается по формуле:

$$Z = (D_1 + D_2 + D_n) * W_D + (T_1 + T_2 + T_k) * W_T + (M_1 + M_2 + M_l) *. \quad (1)$$

По итогам оценки формируются значение, отражающее уровень соответствия объекта критической информационной инфраструктуры требованиям законодательства по каждому из направлений оценки. Предлагается ввести 3 уровня соответствия:

Z = 0, 3 и менее — защищенность объектов КИИ низкая.

Z = 0,4 – 0,7 — защищенность объектов КИИ средняя.

Z = 0,8 и более — защищенность объектов КИИ высокая.

Итак, путем изучения нормативных требований, применения математических методов оценки и определения набора показателей для одного из направлений, была описана методика оценки уровня защищенности объектов критической информационной инфраструктуры.

Список источников

1. Стандарт Банка России СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014»;

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

3. Постановление Правительства РФ от 08.02.2018 № 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»;

4. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

5. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

6. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Статья поступила в редакцию 29.04.2024; принята к публикации 15.05.2024.

Информация об авторе

Самков М. Ю. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Анализ основных показателей защищенности при проведении оценки эффективности системы защиты персональных данных

Кирилл Андреевич Седаков[1]✉, Михаил Юрьевич Рытов[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] sekira98@mail.ru✉, https://orcid.org/0009-0002-9284-4624
[2] rmy@tu-bryansk.ru, https://orcid.org/0234-0023-2435-5763

Аннотация. Рассмотрены основные критерии в проведении оценки эффективности принятых мер и средств в обеспечении защиты персональных данных.

Ключевые слова: оценка эффективности защиты персональных данных, алгоритм проведения аудита информационной безопасности.

Для цитирования: Седаков К. А., Рытов М. Ю. Анализ основных показателей защищенности при проведении оценки эффективности системы защиты персональных данных // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 233–236.

В современном информационном обществе важно обеспечить защиту информации от различных угроз и рисков. Каждый день мы сталкиваемся с новыми угрозами, связанными с хакерскими атаками, вирусами, кражей данных и другими событиями, которые могут нанести серьезный ущерб деловой репутации и потерю конфиденциальной информации. Поэтому актуальность разработки и применения эффективных методов оценки информационной безопасности никогда не была такой высокой. Основная цель заключается в создании эффективного способа оценки эффективности средств и методов защиты персональных данных.

Главным критерием в оценке эффективности средств защиты персональных данных должен являться такой показатель, как оценка уровня остаточного риска от организационной и практической реализации набора контрмер, который используется в определенной организации сферы здравоохранения, и расчета степени влияния конкретных средств и методов защиты на общую защищенность организации. Для определения оценки риска сформированный алгоритм оценки ущерба от нарушения свойств защищенности должен базироваться на экспертно-статистической оценке, особенностью которой является использование метода прогнозного графа.

Однако, не стоит забывать о других показателях, с помощью которых можно и определить уровень оценки эффективности. Одним из таких показате-

лей можно считать оценку персональных данных. Для расчета такого показателя необходимо выполнить начальный аудит организации сферы здравоохранения, а затем, на основе полученных данных, нужно провести анализ максимального финансового ущерба от реализации угроз целостности, доступности и конфиденциальности. Критерием определения такого показателя можно считать размер штрафов, вызванных нарушением требований, действующих нормативно-правовых актов, а также стоимость восстановления информации при появлении деструктивных последствий. В результате данной работы должны быть сформированы расчетные показатели, стоимости утечки персональных данных не только клиентов (пациентов), но и сотрудников данного учреждения. Данные показатели должны обрабатываться на объекте с учетом суммы наносимого ущерба, стоимости их восстановления и ряда других показателей.

Следующим показателем, который нужно определить, это анализ актуальных угроз и выявление вероятности реализации угрозы. Помимо этого, в рамках определения данного показателя должны быть сформированы группы угроз, чтобы определить степень вариативности реализации угроз. При анализе угроз из состава Банка данных угроз (БДУ) ФСТЭК необходимо производить систематизацию перечисленных угроз [4]. Так же стоит определить параметры риска для каждой группы угроз. Определение критичной группы угроз на основании параметров коэффициента важности, должно основываться на экспертном методе. Исходя из этого, можно определить, что анализ определения данного показателя должен проводиться только высококвалифицированными специалистами в области защиты информации, а такой критерии, как коэффициент важности должен определяться в формате аддитивной свертки. На основе определенного показателя коэффициента важности можно определить значения возможности реализации угроз. Оценка вероятности реализации выявленных угроз проводится экспертным методом. Для его определения можно использовать данные, полученные раннее, а именно коэффициент важности и общее количество угроз, выявленных для данной организации. В заключение данного работы для простоты понимания данных необходимо перевести количественный показатель возможности реализации угрозы в качественный. Критерии можно классифицировать следующим образом:

1. Показатель вероятности реализации угрозы «Низкий». Данное значение получается, когда при проведении анализа было выявлено, что используемые меры и средства, которые необходимы для защиты персональных данных, достаточны или нуждаются в небольшом дополнении организационных и технических мер.

2. Показатель вероятности реализации угрозы «Средний». Данное значение получается, когда при проведении анализа было выявлено, что используемые меры и средства, которые необходимы для защиты персональных данных, недостаточны и нуждаются в дополнении организационных и технических мер.

3. Показатель вероятности реализации угрозы «Высокий». Данное значение получается, когда при проведении анализа было выявлено, что используемые меры и средства, которые необходимы для защиты персональных данных,

недостаточны и нуждаются в изменении всех системе информационной безопасности в организации.

Приведенное преобразование от количественного показателя к качественному продиктовано необходимостью расчета риска. Таким образом, это позволяет определить необходимые контрмеры для минимизации этого риска. Далее должна оцениваться степень критичности групп угроз. Этот показатель можно рассчитать с помощью значений коэффициента риска, последствия от реализации угрозы (ценность актива), количество определенных угроз.

Исходя из полученных данных, можно провести оценку уровня риска информационной безопасности. Показатель уровня риска информационной безопасности определяет, будет ли реализована угроза с учетом вероятности реализации угрозы и уровня коэффициента риска информационной безопасности. Уровень риска можно будет определить с помощью таких данных как возможность реализации угрозы и коэффициент риска. После расчета будут получены количественные оценки. Чтобы лучше понять их значения, можно будет перенести данный результат в качественные с помощью шкалы оценок.

В завершении всей работы, зная все необходимые показатели, можно определить итоговую оценку эффективности защиты персональных данных. Оценка эффективности формируется благодаря сравнительному анализу, который был получен в результате расчета таких показателей, как уровень риска и вероятности реализации угроз.

Таким образом, выбранные показатели можно использовать для оценки эффективности защиты персональных данных в различных организациях. Разработка алгоритма оценки эффективности на основе данных критериев позволит минимизировать финансовые и технические затраты на определение уровня защищенности организации. Если разработать данный алгоритм, то это приведет к повышению уровня анализа эффективности, используемых мер защиты информации в определенной организации.

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.Вячеслав Харченко Безопасность информационно-управляющих систем и инфраструктур / Харченко Вячеслав, Владимир Скляр, Евгений Брежнев. - М.: PalmariumAcademicPublishing, 2019. - 528с. — URL: http://www.iprbookshop.ru/4678997530.html.

3. 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;

4. Electronic resource: https://www.omgtu.ru/general_information/media_omgtu/journal_of_omsk_research_journal/files/arhiv/2021/№%205%20(179)%20(ОНВ)/7479%20Майстренко%20В.%20А.,%20Безродных%20О.%20А.,%20Дорохин%20Р.%20А..pdf

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Рытов М. Ю. – к. т. н., заведующий кафедрой «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Седаков К. А. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Рытов М. Ю. – научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.53

Малые беспилотные летательные аппараты как угроза объектам информатизации

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/0234-0023-2435-5763

Аннотация. В статье указывается необходимость и актуальность рассмотрения малых беспилотных летательных аппаратов как угрозы. Приводятся причины массовости применения беспилотных летательных аппаратов. Рассматриваются нормативно-правовой аспект использования таких аппаратов. Приводятся примеры сценариев применения беспилотных летательных аппаратов злоумышленником. Указываются возможные пути решения данной проблемы.

Ключевые слова: информационная безопасность, нарушитель безопасности информации, беспилотный летательный аппарат.

Для цитирования: Седачев О. С., Рытов М. Ю. Малые беспилотные летательные аппараты как угроза объектам информатизации // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 237–240.

В последние годы, а особенно с начала специальной военной операции, начавшейся 24 февраля 2022 года, применение беспилотных летательных аппаратов (БПЛА) становится всё более массовым. Особенно это относится к малым БПЛА вертолетного типа — так называемым «мультикоптерам», «квадрокоптерам» или «дронам». Для таких летательных аппаратов характерно использование установки на основе использования 4, 6 или большего количества двигателей [1].

Это обусловлено в первую очередь относительно низкой стоимостью как готовых изделий, так и самостоятельно собранных из различных комплектующих. Во втором случае человек может сам подобрать необходимые ему детали исходя из потребностей и целей применения. Кроме этого, подготовка оператора БПЛА не требует слишком много времени, а обслуживание не требует высокой квалификации. Также, малые БПЛА ввиду своих размеров обладают низкой заметностью.

Малые беспилотные летательные аппараты активно применяются как на поле боя в различных вооруженных конфликтах по всему миру, так и в мирных целях, например, для картографирования местности.

В Российской Федерации все БПЛА классифицируются как беспилотные воздушные судна и подлежат регистрации при массе от 150 г до 30 кг согласно Правилам государственного учета БВС, утвержденным постановлением Правительства Российской Федерации от 25.05.2019 № 658 вне зависимости от того ввезены они или произведены в России [2].

Однако в случае, если БПЛА будет ввезен или собран для совершения противозаконных действий, он вряд ли будет должным образом зарегистрирован. Злоумышленник может использовать в своих целях как штатное оборудование серийных изделий, так и модификации, либо полностью самостоятельно собранный аппарат.

Современные БПЛА, как правило, имеют встроенные камеры, позволяющие делать фото и записывать видео высокого разрешения. Это может позволить злоумышленнику проводить сбор сведений об объекте, визуальное наблюдение и запись конфиденциальной информации с большого расстояния, которое значительно уменьшает шансы его обнаружения.

Опыт специальной военной операции показал, что на БПЛА довольно легко изготовить и применять самодельные дополнительные устройства. Особенно широкое распространение получили модули для сброса с высоты различных взрывных устройств, гранат, мин и т. п. БПЛА с такими модификациями может быть применены террористическими группировками, либо отдельными лицами при участии таких группировок или спецслужб иностранных государств. Целью подобных атак, как правило, становятся следующие объекты информатизации:

- промышленные предприятия;
- аграрно-промышленные комплексы;
- административные здания;
- транспортные узлы и пути сообщения;
- электростанции и линии электропередач;
- магистральные трубопроводы;
- тепловые магистрали.

Такие атаки могут проводиться с целью:

- нанесения вреда жизни и здоровью людей;
- остановки работы или сокращения производства предприятия;
- вызова техногенных аварий и экологических катастроф;
- затраты времени и ресурсов на ликвидацию последствий;
- деморализации общества и оказание психологического давления;
- нанесения репутационного ущерба объекту атаки и государству [3].

Также атаки на могут производиться с помощью т.н. «дронов-камикадзе», представляющих собой недорогой БПЛА, взрывное устройство которого имеет контактный взрыватель, срабатывающий при столкновении летательного аппа-

рата с целью на большой скорости. Эта особенность вместе с небольшими размерами значительно затрудняет предотвращение атаки.

Кроме этого, БПЛА позволяет установить на него различное оборудование для проведения удаленных компьютерных атак на сети и системы. Это могут быть различные подавители беспроводных сетей или WiFi оборудование для получения несанкционированного доступа к сети жертвы, который далее будет использован для получения конфиденциальной информации или выведения из строя информационной системы.

Угрозы атак с применением БПЛА в последние годы стали заметны, в связи с чем начался активный процесс разработки и производства средств обнаружения, нейтрализации и уничтожения таких летательных аппаратов не только предприятиями военно-промышленного комплекса, но и частными компаниями. На рынке широко представлены различные радиолокационные, оптические и иные средства обнаружения, а также т. н. «антидроновые ружья». К сожалению, некоторые из подобных изделий них не справляются с поставленной задачей должным образом, независимо от стоимости. В будущем число атак с применением БПЛА на производственные, транспортные, топливно-энергетические и другие объекты, а также на их информационные системы будет расти. Кроме этого, возможно будет расти и спектр средств и методов воздействия ввиду возможности использования различных самодельных модулей, прикрепляемых к БПЛА. Для предотвращения этого необходимо развитие и поддержка отечественных средств обнаружения, нейтрализации и уничтожения беспилотных летательных аппаратов. Необходимо введение единой объективной и комплексной методики оценки коммерческих средств противодействия БПЛА. Также необходимо увеличить число квалифицированных специалистов в данной области.

Список источников

1. Макаренко С. И. Противодействие беспилотным летательным аппаратам. Монография. // Санкт-Петербург.: Наукоемкие технологии. 2020. 204 с.

2. Постановление Правительства РФ от 25 мая 2019 г. N 658 "Об утверждении Правил государственного учета беспилотных гражданских воздушных судов с максимальной взлетной массой от 0,15 килограмма до 30 килограммов, ввезенных в Российскую Федерацию или произведенных в Российской Федерации"

3. Темная сторона технологий: развивающаяся угроза атак с использованием дронов // SecurityLab. URL: https://www.securitylab.ru/blog/company/cloudnetworks/352846.php.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Седачев О. С. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Рытов М. Ю. – к. т. н., заведующий кафедрой «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Седачев О. С. – сбор материала, написание статьи (50 %).
Рытов М. Ю. – идея, научное редактирование (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.53

Анализ уязвимостей в системах управления беспилотных летательных аппаратов

Олег Сергеевич Седачев[1]✉, Сергей Александрович Шпичак [2]
[1, 2]Брянский государственный технический университет, Брянск, Россия
[1] sedachev57@mail.ru✉, https://orcid.org/0009-0004-7688-249X
[2] frb113@lenta.ru

Аннотация. В статье указывается необходимость и актуальность исследования уязвимостей в системах управления беспилотных летательных аппаратов. Приводится информация об используемых БПЛА радиочастотах. Рассматриваются возможные направления атаки на системы управления беспилотных летательных аппаратов цели и последствия этих атак. Указываются возможные причины возникновения уязвимостей систем управления.

Ключевые слова: информационная безопасность, беспилотный летательный аппарат, система управления, навигационная система.

Для цитирования: Седачев О. С., Шпичак С. А. Анализ уязвимостей в системах управления беспилотных летательных аппаратов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 241–243.

Беспилотные летательные аппараты (БПЛА) становятся всё более востребованы в различных областях — гражданской, коммерческой и особенно военной сфере. Одним из наиболее эффективных способов негативного воздействия на такие аппараты помимо физического является воздействие на системы управления и навигации, а также каналы связи между БПЛА и оператором. В связи с этим возникает необходимость обеспечения безопасности этих систем.

Система управления БПЛА играет ключевую роль в выполнении полетов, обеспечении их безопасности и наиболее эффективного использования ресурсов беспилотного летательного аппарата. Как правило, управление БПЛА осуществляется с помощью бортового комплекса навигации и управления, в состав которого входят:

– навигационная система, содержащая приемник спутниковой навигации, обеспечивающий прием навигационной информации (используются системы GPS, ГЛОНАСС, Beidou, Galileo);

– система датчиков, обеспечивающая определение ориентации и параметров движения БПЛА, измерение высоты и воздушной скорости;

– различные виды антенн и датчиков;

– модуль автопилота, позволяющий выполнять такие сценарии, как самостоятельный полет по заданному маршруту, поддержание заданной высоты и скорости полета, принудительная посадка;
– система накопления и передачи информации [1].

Надежность и защита этих систем от внешних угроз имеют критическое значение для успешного функционирования беспилотного летательного аппарата.

Одним из наиболее распространенных способов воздействия на каналы управления БПЛА, а именно их подавление более мощным, чем излучаемым пунктом (пультом) управления, сигналом на соответствующих частотах. К наиболее распространенным диапазонам частот коммерческих беспилотных летательных аппаратов относятся:
– RC433: 433 МГц;
– RC868: 868-916 МГц;
– GSM900: 890-915, 935-960 МГц;
– GSM1800: 1710-1880 МГц;
– сети 3G: 2110-2170 МГц;
– сети 4G: 725-770, 790-830, 850-894 МГц, 2,5-2,7 ГГц;
– сети CDMA: 850-894 МГц;
– сети Wi-Fi на базовой частоте 2,4 ГГц: 2,4-2,5 ГГц;
– сети Wi-Fi на базовой частоте 5,2 ГГц: 4,9-5,5 ГГц;
– сети Wi-Fi на базовой частоте 5,8 ГГц: 5,5-6,1 ГГц [2].

Также стоит отметить, что в случае с малыми коммерческими БПЛА по каналу на заданной частоте передается не только сигналы управления и телеметрия, но и видеосигнал. Большинство БПЛА используют метод псевдослучайной перестройки рабочей частоты (ППРЧ), заключающийся в смене рабочей частоты в соответствии с псевдослучайной последовательностью чисел, задаваемой специальным алгоритмом, результат работы которого известен приемнику и передатчику сигнала. Данный метод значительно повышает помехозащищенность канала связи и отлично зарекомендовал в сетях Wi-Fi. Однако, ППРЧ станет малоэффективной в случае формирования помех по всему используемому диапазону частот или, что наиболее вероятно, по всем возможным для использования диапазонам.

Также помехи возможно создать на частотах навигационных систем, что вызовет невозможность определения местоположения БПЛА в случае отсутствия известных видимых ориентиров.

В большинстве коммерческих малогабаритных носимых средств радиоэлектронного подавления, т. н. «противодроновых ружей» присутствует возможность раздельного или совместного подавления частот управления и навигации, что приводит к потере управления и полной дезориентации самого аппарата.

Также навигационную систему возможно подвергнуть атаке не путем полного «глушения» спутникового сигнала, а подмены его на ложный. Например, при подобном воздействии на коммерческий БПЛА с немодифицированной прошивкой возможно передать ему координаты аэропорта или другого

места, в котором запрещены полеты беспилотных летательных аппаратов, что вызовет экстренную посадку.

В случае неполучения БПЛА сигналов управления возможны различные варианты его действий: зависание на месте до возобновления сигнала (для мультикоптеров), выполнение последней полученной команды, продолжение полета по прямой, посадка, возвращение «домой» — к пульту управления. Однако, если в дополнение к подавлению сигналов управления происходит воздействие на навигационную систему, возможно не только принудительно посадить БПЛА в точке его текущего местонахождения, но и «угнать» путем задания ложных координат для возвращения к пульту управления.

Как правило, коммерческие БПЛА, использующие в качестве канала управления Wi-Fi, используют протоколы шифрования с низкой криптостойкостью — WEP и WPA, либо не используют шифрование вовсе. Это позволяет атакующему перехватить управление беспилотным летательным аппаратом.

Причины возникновения уязвимостей систем управления БПЛА связаны с конструктивными особенностями (например, размером), стандартизацией, удешевлением производства, ошибками проектирования или эксплуатации и другими факторами.

Активное применение беспилотных летательных аппаратов в ходе боевых действий в последние годы показало, что исследование данной темы крайне важно не только для боевого применения БПЛА и противодействия им на поле боя, но и для обеспечения безопасности граждан и государства. Кроме того, необходимо проведение двустороннего анализа уязвимостей систем управления БПЛА — со стороны производителя, эксплуатанта, оператора и со стороны атакующего.

Список источников

1. Иванова И.А., Никонов В.В., Царева А.А. Способы организации управления беспилотными летательными аппаратами // Актуальные проблемы гуманитарных и естественных наук. 2014. №11-1.

2. Макаренко С. И. Противодействие беспилотным летательным аппаратам. Монография. // Санкт-Петербург.: Наукоемкие технологии. 2020. 204 с.

Статья поступила в редакцию 232.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Седачев О. С. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Шпичак С. А. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.52

Повышение качества противодействия утечкам информации по каналу ПЭМИН в офисном помещении

Владимир Романович Семенов[1]✉, Павел Игоревич Андреев[2], Арина Викторовна Фурсова[3]
[1, 2] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[3] Тамбовский государственный технический университет, Тамбов, Россия
[1, 2] nauchnajarota@yandex.ru✉, https://orcid.org/0009-0007-5540-2719
[3] fursova_arina@inbox.ru, https://orcid.org/0009-0007-5540-2719

Аннотация. Данная статья исследует эффективные методы защиты информации от утечек через каналы побочных электромагнитных излучений и наводок (ПЭМИН) в информационно-вычислительных сетях (ИВС). Обсуждаются проблемы выбора средств защиты информации (СЗИ) и их качества, а также предлагается подход к решению данной проблемы через комбинацию различных СЗИ и разработку программного обеспечения для контроля за процессом генерации электромагнитного поля шума (ЭМПШ). Проведенный эксперимент демонстрирует положительные результаты совместного использования различных СЗИ в повышении качества шума и эффективности защиты информации.

Ключевые слова: Защита информации, утечка данных, электромагнитные излучения, каналы утечки, средства защиты информации, электромагнитное поле шума, программное обеспечение, информационно-вычислительные сети.

Для цитирования: Семенов В. Р., Андреев П. И., Фурсова А. В. Повышение качества противодействия утечкам информации по каналу ПЭМИН в офисном помещении // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 244–247.

Введение

Известно, что взаимодействие средств вычислительной техники сопровождается электромагнитными излучениями и наводками на проводные линии, цепи электропитания и заземления [1]. Захват сигналов излучений и наводок может открыть неавторизованным пользователям доступ к информации, передаваемой, хранимой и обрабатываемой в информационно-вычислительных сетях (ИВС). Эти виды утечек данных обычно называют каналом утечки через побочные электромагнитные излучения и наводки (ПЭМИН) [2].

Для обеспечения защиты информации от утечки через каналы ПЭМИН могут применяться такие методы как:

1. Ограничение доступа к территории, где находится объект ИВС, а также к его отдельным устройствам;

2. Шифрование данных, чтобы они оставались доступными только для тех, кто имеет ключ для расшифровки [3];

3. Использование экранирования и фильтрации для подавления электромагнитных помех;

4. Маскирование сигналов ПЭМИН от источников, создающих сопровождающий шум (зашумление) [1].

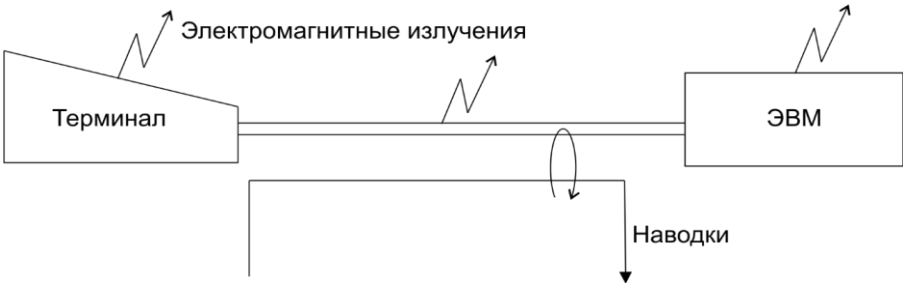


Рис. 1. Модель канала утечки на качественном уровне

Один из наиболее экономически выгодных и эффективных методов защиты информации от утечки через каналы ПЭМИН состоит в применении средств защиты информации (СЗИ).

Однако не всегда возможно полностью доверять одному производителю СЗИ в данном контексте, и процесс выбора системы должен включать в себя тщательный анализ охвата электромагнитного поля шума (ЭМПШ), его качества и стабильности генерируемого шума.

Хотя кажется, что устройства СЗИ, предназначенные для одной цели, должны быть одинаково эффективны в создании шума, на практике возможны различные технические недочеты или недобросовестное производство, что может привести к генерации ЭМПШ низкого качества, не отвечающего требованиям защиты конфиденциальной информации.

Для решения данной проблемы предлагается разработать программное обеспечение для контроля генератора или сети генераторов ЭМПШ, а также для контроля итоговой зоны защиты информации от утечек по каналу ПЭМИН. Начальным этапом в осуществлении такой идеи является комбинация различных СЗИ.

Экспериментальная часть

Для подтверждения гипотезы о том, что совместное использование различных средств защиты информации дает положительный результат в повышении качества шума, был проведен эксперимент.

Для этого были выбраны и собраны в стенд, изображенный на рисунке 2, следующие СЗИ: "Берилл СТБ 211" и "Соната 2Р". В качестве спектрального анализатора, представленного на рисунке 3, а), использовался Agilent E4402B с антенной и диапазоном частот от 100 МГц до 3,0 ГГц, что достаточно для измерения ЭМПШ, генерируемого СЗИ. Генераторы измерялись в их рабочем диа-

пазоне (100 МГц-2,0 ГГц), и полученные результаты спектрограммы, представленные на рисунке 3, б), были обработаны и проанализированы. Полученные подробные результаты представлены на рисунке 4.

Рис. 2. Стенд системы активной защиты информации от утечки за счёт ПЭМИН

а) б)

Рис. 3. а) Спектр анализатор Agilent, б) показания спектр анализатора

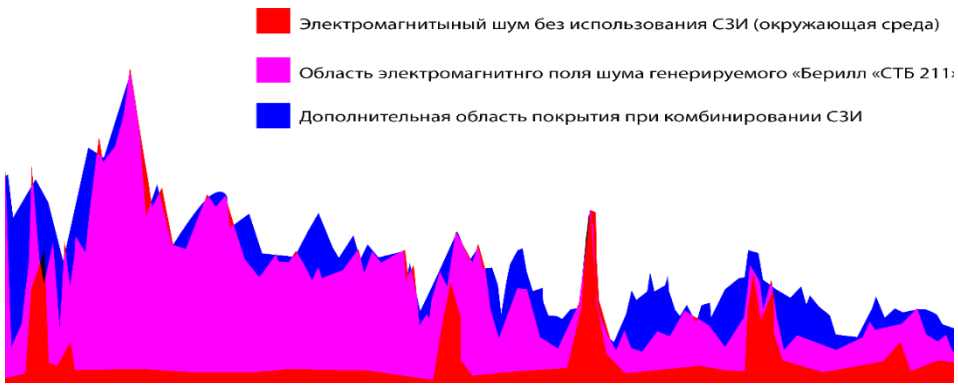


Рис. 4. Анализ полученных спектрограмм

Заключение

Таким образом, наблюдая площадь «синей зоны» следует сделать вывод том, что комбинация средств защиты информации, а также разработка программного обеспечения для контроля их работы имеет не малозначительную практическую выгоду в целях защиты информации в офисных помещениях от утечки за счёт побочных электромагнитных излучений и наводок.

Научный руководитель темы д.т.н. профессор Алексеев В.В., ФГБОУ ВО «ТГТУ».

Список источников

1. Маркин А.В. Безопасность излучений и наводок от средств электронно-вычислительной техники: Домыслы и реальность // Зарубежная радиоэлектроника 1089 №12 с 102-109

2. Герасименко В.А., Диев С.И., Размахин Н.К. Новые данные о защите информации в автоматизированных системах обработки данных\\ Зарубежная радиоэлектроника 1987, №3, с. 48-75

3. Спесивцев А.В., Вегнер А., Крутяков А.Ю. и др. Защита информации персональных ЭВМ – М.: Радио и связь МП «Весть» 1992. -192 с.

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Семенов В. Р. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Андреев П. И. – старший оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Фурсова А. В. – аспирант кафедры «Информационные системы и защита информации» ФГБОУ ВО «ТГТУ».

Вклад авторов

Семенов В. Р. – редактирование визуальной части (рисунков), проведение экспериментальной части, обработка результатов эксперимента, частичное написание статьи (60 %).

Андреев П. И. – подбор литературных источников, частичное написание статьи (20 %).

Фурсова А. В. – научное редактирование текста, составление плана эксперимента, частичное написание статьи (20 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 681.3

Создание тестовых шаблонов для верификации микросхем на функционально-логическом уровне

Татьяна Владимировна Скворцова[1], Юлия Алексеевна Литвинова[2], Екатерина Владимировна Грошева[3], Алексей Михайлович Плотников[4], Игорь Владимирович Скоркин[5]

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

[5] АО «Научно-исследовательский институт космического приборостроения», Россия

[1] soultan06@bk.ru

[2] litvinova_12@mail.ru

[3] grosh_91@mail.ru

[4] ploa_25@mail.ru

[5] ckork_ig@mail.ru

Аннотация. Данная статья посвящена функциональной верификации микросхем и подходам к синтезу тестов на функционально-логическом уровне. Обсуждаются два основных подхода: структурный, основанный на системах генерации тестовых последовательностей (ATPG), и функциональный, который опирается на анализ выполняемых схемой функций.

Ключевые слова: электронная компонентная база, верификация, радиация.

Для цитирования: Скворцова Т. В., Литвинова Ю. А., Грошева Е. В., Плотников А. М., Скоркин И. В. Создание тестовых шаблонов для верификации микросхем на функционально-логическом уровне // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 248–251.

Для функциональной проверки моделируемой микросхемы используются тестовые шаблоны (векторы). Они должны обеспечивать большой процент выявления неисправностей.

Существует два подхода к синтезу тестов на функционально-логическом уровне: функциональный и структурный. Структурные тесты могут быть сгенерированы системами генерации тестовых последовательностей (ATPG).

Второй подход — функциональный, основан на анализе выполняемых схемой функций. Задача функциональной верификации доказать, что схема ра-

ботает правильно, т. е. подтвердить функциональные возможности схемы. Ориентация на поведенческие свойства изделия, непосредственно не связанные с особенностью структурной реализации, затрудняет автоматизацию синтеза функциональных тестов [1, 2, 3].

На рис. 1 приведена общая схема СБИС СнК К1867ВЦ3АФ, разработанной в АО «НИИЭТ».

Каждый из элементов СнК имеет собственный предпочтительный способ тестирования, тестирование всей системы в целом затруднительно. Практически каждая СнК имеет одно или несколько программируемых процессорных ядер. Именно через этот компонент обычно становится возможным управлять (а, соответственно, протестировать) все остальные компоненты системы.

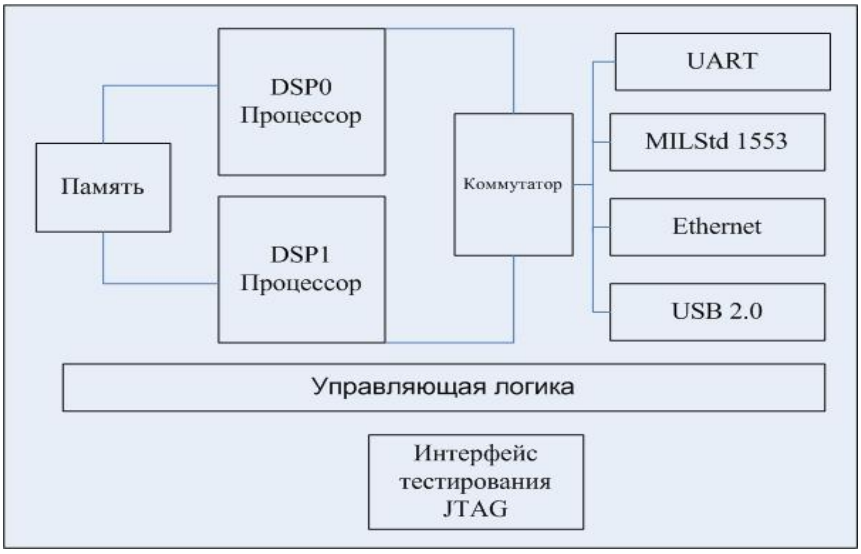


Рис. 1. Общая схема системы на кристалле К1867ВЦ3АФ

Главной целью любой функциональной верификации является проверка того, что разработанная RTL-модель действительно реализует описанную в спецификации функциональность (рис. 2).

Рис. 2. Схема функциональной верификации

Функциональная верификация устройства, содержащего микропроцессор, чрезвычайно трудоемкая задача. При этом для такого устройства достаточно популярным является метод верификации на основе инструкций. В этом случай тестовые сценарии пишутся на языке ассемблер или С, соответствующий образ памяти загружается в спроектированную модель, а результат моделирования сравнивается затем с ожидаемым поведением.

Данный метод поддаётся некоторой автоматизации при использовании базы знаний инструкции верифицируемой системы, а также тестовых случаев. Но совсем обойтись без ручного составления тестовых сценариев практически невозможно. Так, для проверки нормализатора вещественного числа формата double extended, используемого в микропроцессорах Pentium, вероятность того, что при случайных операндах сумма мантисс будет иметь 10 нулей в старших разряда $\sim 10^{-8}$, то есть близко к нулю, а значит, проверить такой случай с помощью случайных генераторов вряд ли удастся.

В начале необходимо получить функциональную спецификацию верифицируемого СФ-блока в варианте наиболее близком к окончательному.

Далее на основе функциональной спецификации необходимо идентифицировать список тестовых объектов. Верификационному инженеру нужно выделить те свойства проверяемого блока, которые определяют поведение объекта, интерфейсную информацию, реализуемые протоколы, структурные элементы (память, арбитр, FIFO и др.), производительность, индустриальные стандарты и т. д. Такой список может быть достаточно объёмным.

На следующем шаге определяется список тестовых программ для каждого из тестового случая. В случае систем на кристалле он может достигать очень больших размеров. Для грамотного составления такого списка необходимо определить, каков набор свойств данного тестового объекта, диапазон его значений, реализует ли этот объект какой-либо протокол или стандарт, какие взаимодействия существуют внутри объекта и с другими объектами.

Следующая задача — определить стратегию тестирования. Это может быть иерархическая стратегия, стратегия, направленная на повторное использование, стратегия на основе тестовых случаев.

В процессе тестирования важную роль играют метрики. Для верификации СБИС подходит метрика на основе тестовых объектов. Также достаточно популярны метрика на основе количества найденных ошибок, метрики для верификации программного кода, адаптированные к высокоуровневому поведенческому описанию аппаратного обеспечения.

Данная методика позволяет осуществить верификацию СФ-блока современных систем на кристалле.

Список источников

1. Повышение формализации задач верификации топологии и электрической схемы для систем автоматизированного проектирования. / А.В. Полуэктов, К.В. Зольников, А.В. Ачкасов, Ю.А. Чевычелов // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 102-111.

2. Интеграция программного продукта Calibre в среду Cadence Virtuoso и повышение интеллектуальных свойств САПР проектировании микросхем / А.В. Полуэктов, Д.В. Шеховцов, И.В. Скоркин, П.А. Чубунов // Моделирование систем и процессов. – 2023. – Т. 16, № 4. – С. 71-80.

3. Технология разработки RTL модели описания изделия при разработке программно-аналитического комплекса САПР / Д.В. Шеховцов, А.М. Плотников, К.В. Зольников, А.И. Заревич // Моделирование систем и процессов. – 2023. – Т. 16, № 3. – С. 7.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Скворцова Т. В. – к. т. н., декан факультета компьютерных наук и технологий ФГБОУ ВО «ВГЛТУ».

Литвинова Ю. А. – к. филол. н., доцент кафедры иностранных языков ФГБОУ ВО «ВГЛТУ».

Грошева Е. В. – аспирант ФГБОУ ВО «ВГЛТУ».

Плотников А. М. – аспирант ФГБОУ ВО «ВГЛТУ».

Скоркин И. В. – начальник отдела АО «НИИКП».

Вклад авторов

Скворцова Т. В. – идея, сбор материала, обработка материала, частичное написание статьи (40 %).

Литвинова Ю. А. – сбор материала, обработка материала, частичное написание статьи (15 %).

Грошева Е. В. – сбор материала, обработка материала, частичное написание статьи (15 %).

Плотников А. М. – сбор материала, обработка материала, частичное написание статьи (15 %).

Скоркин И. В. – сбор материала, обработка материала, частичное написание статьи (15 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 331.101.1

Патентная аналитика в области управления безопасностью контентов сайтов

Валерий Валентинович Спасенников[1]✉,
Александр Константинович Шкиров[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] spas1956@mail.ru✉, http://orcid.org/0000-0002-4378-3426
[2] alshkirov@gmail.com, https://orcid.org/0000-0002-1820-8710

Аннотация. Информационная безопасность современного информационного общества во многом определяется наличием новых идей и решений, которые запатентованы. В статье осуществлён обзор патентов, связанных с управлением доступом к внешним сайтам через Интернет, обеспечением информационной безопасности при доступе пользователя к внешнем информационным ресурсам через Интернет, с управлением доступом к информационным ресурсам компьютерных сетей различных уровней конфиденциальности.

Ключевые слова: контент сайта, информационная безопасность, Интернет, доступ пользователей.

Для цитирования: Спасенников В. В., Шкиров А. К. Патентная аналитика в области управления безопасностью контентов сайтов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 252–255.

В наши дни с постоянным развитием технологий также неумолимо растёт и количество сайтов. Сегодня невозможно представить магазин, сервис или событие, у которого не было бы своей страницы в сети Интернет. С ростом количества всяческих сайтов растёт и качество их наполнения: становится всё больше высокотехнологичного и разнообразного контента.

Как известно, чем система сложнее, тем больше в ней уязвимостей, поэтому данная статья призвана проанализировать существующие патенты в области информационной безопасности по управлению контентом сайта, выявить их особенности и сформировать перечень правил, которых следует придерживаться разработчикам сайтов. Патентная аналитика, как показано в работах [1] и [2] является действенным средством в прогнозировании развития различных направлений техники и областей научных исследований в соответствии с международной патентной классификацией.

Патент РФ №2002125855 от 23 марта 2001 г.

Первый рассмотренный патент РФ «Способ управления доступом к внешним сайтам через Интернет» №2002125855, класс G06F 17/30, G06F 13/00, от 2001.03.23 предполагает наличие специального устройства хранения информации с содержащимися в ней четырьмя базами данных, содержащих:

1) перечень доступных интернет-сайтов;
2) перечень запрещённых интернет-сайтов;
3) перечень запрещённых ключевых слов;
4) перечень полезных ключевых слов.

Пользователю разрешают доступ к интернет-сайтам, находящимся в первой базе данных. Когда пользователь пытается подключиться к сайту, включённому во вторую базу данных, доступ запрещается. Для интернет-ресурсов, не включённых ни в первую, ни во вторую базу данных, предполагается проверка наполнения на выявление ключевых слов. При наличии слов, относящихся к третьей базе данных (с запрещёнными словами), доступ на сайт может быть разрешён только в том случае, если есть слова из четвёртой базы данных (с полезными словами).

Имеются основания считать метод, описанный в патенте №2002125855, устаревшим в связи со стремительным развитием технологий, однако сама запатентованная идея может быть полезной для администраторов интернет-ресурсов. Существует множество сайтов, за материалы на которых отвечает не только администратор, но и сами пользователи-авторы. В таком случае, конечно, выкладываемый авторами контент должен модерироваться. Идея патента может быть использована или уже была использована для создания специального программного обеспечения, которое поможет автоматизировать модерацию тех материалов, которые присылают пользователи.

Патент РФ №2445692 от 21 января 2011 г.

«Способ обеспечения информационной безопасности при доступе пользователя к внешнем информационным ресурсам через интернет» по патенту РФ №2445692, класс G06F 17/30, от 21.01.2011 описывает принцип доступа пользователей к информационным ресурсам сети Интернет. Автор патента выступает с критикой изобретения, описанного в п. 1 текущей статьи, отмечая его недостатки, такие как:

- узкая область применения;
- недостаточное внимание вопросам безопасности сети.

Задачей описываемо патента ставится повышение защищённости клиентов от воздействия нарушителя при доступе пользователя к информационным ресурсам сети Интернет, скрытие точки выхода из корпоративной сети в сеть общего пользования, а также раннее определение нарушителя за счет применения в точках выхода в сеть общего пользования средств обеспечения информационной безопасности.

Изобретение находит выход в использовании SOCKS-серверов, интернет протоколов, использующихся для передачи пакетов с данными от сервера клиенту с помощью промежуточного прокси-сервера.

Принимается запрос клиента к информационной службе, проверяется тип запроса, проверяется запрос по определенным правилам на совпадение параметров запроса с имеющимися базами данных параметров. Запрос выполняется только в том случае, если он удовлетворяет указанным требованиям. В противном случае запрос отклоняется и строится SOCKS-сеть доступа, контролирующая входящие и исходящие пакеты антивирусными средствами, системами обнаружения атак, межсетевыми экранами. В случае тревоги сервер блокируют входящие и исходящие пакеты.

Описанный способ может применяться разработчиками при создании серверной части сайта. Установка доступа через SOCKS-сервера может помочь защитить соединение и целостность интернет-ресурса от так называемых «хакерских атак».

Патент РФ №2436154 от 1 декабря 2009 г.

«Способ управления доступом к информационным ресурсам компьютерных сетей различных уровней конфиденциальности и устройство, его реализующие» по патенту РФ №2436154, класс G06F 17/30, от 01.12.2009 относится к повышению безопасности в компьютерных сетях.

Задачей запатентованной группы изобретений является создание способа управления доступом к информационным ресурсам компьютерных сетей различных уровней конфиденциальности и устройства, его реализующего, позволяющих предотвратить утечку конфиденциальной информации из корпоративной компьютерной сети: с компьютера-клиента, защищенных компьютеров-серверов и со сменных носителей информации, подключаемых к компьютерам-клиентам.

Эта задача решается тем, что в заявленном способе предусматривается управление безопасным доступом к информационным ресурсам различных уровней конфиденциальности на основе классификации информационных ресурсов на два основных класса:

1) по степени (типу) конфиденциальности информации;
2) по уровню риска или опасности их воздействия на конфиденциальную (защищаемую) информацию.

Пользователь имеет возможность получения доступа к любому информационному ресурсу, но ему запрещается одновременный доступ к ресурсам разных уровней конфиденциальности.

Использование вышеуказанного метода в корпоративной сети разработчиков интернет-ресурса, в которой могут находится базы данных с личными данными пользователей, позволяет предотвратить утечку данных на сторонние ресурсы именно из-за запрета на одновременное подключение к ресурсам разных уровней конфиденциальности.

Заключение

В текущей статье были рассмотрены три патента Российской Федерации, выделены отличительные особенности каждого из них, а также были выведены

полезные практики, которые компании-разработчики сайтов могли бы использовать для осуществления безопасности доступа к ресурсам, а также безопасности администрирования и модерации контента:

1. Наличие четырёх баз данных, описанных в п. 1, которое поможет автоматизировать модерацию контента, оставленного пользователями на сайте.
2. Использование SOCKS-серверов для доступа к интернет-ресурсу, чтобы не только защитить его от вмешательства злоумышленников, но и для определения этих самых злоумышленников.
3. Запрет на одновременный доступ к ресурсам разной степени конфиденциальности в корпоративной сети компании-разработчика сайта для предотвращения утечки корпоративной конфиденциальной информации.

Список источников

1. Spasennikov, V. Ergonomic factors in patenting computer systems for personnel's selection and training / V. Spasennikov, K. Androsov, G. Golubeva // CEUR Workshop Proceedings : 30, Saint Petersburg, 22–25 сентября 2020 года. – Saint Petersburg, 2020. – P. 1. – EDN MRWCZX.

2. Кондратенко, С. В. Анализ динамики патентования изобретений в сфере удовлетворения жизненных потребностей человека / С. В. Кондратенко, А. А. Кузьменко, В. В. Спасенников // Вестник Брянского государственного технического университета. – 2017. – № 4(57). – С. 183-191. – DOI 10.12737/article_5a02fa1358eb23.38551383. – EDN ZRQHIV.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Спасенников В. В. – д. пс. н., профессор кафедры «Гуманитарные и социальные дисциплины» ФГБОУ ВО «БГТУ».

Шкиров А. К. – студент кафедры «Информатика и программное обеспечение», направление подготовки 09.04.04 – Программная инженерия, ФГБОУ ВО «БГТУ».

Вклад авторов

Спасенников В. В. – обработка материала, написание статьи (50 %).
Шкиров А. К. – сбор материала, частичное написание статьи (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056

Разработка методов противодействия атак с использованием социальной инженерии

Анатолий Денисович Степанов[1]✉, Дмитрий Андреевич Лысов[2]✉
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] anatolijs729@gmail.com✉, https://orcid.org/0009-0007-0052-5009
[2] lysovdmitriia@gmail.com✉, https://orcid.org/0009-0003-9666-7191

Аннотация. В статье проведено исследование главных методов кибер-атак методами социальной инженерии, а также противодействия им.

Ключевые слова: информационная безопасность, социальная инженерия.

Для цитирования: Степанов А. Д., Лысов Д. А. Разработка методов противодействия атак с использованием социальной инженерии // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 256–260.

В современном мире существует очень много различных угроз, но зачастую самые эффективные кибер-преступления происходят посредством манипуляции информацией, с подачи сотрудников или проникновения в компанию. Не сложно представить какая часть системы наиболее уязвима для злоумышленника, наши компьютеры достаточно безопасны до того момента, когда им начинает пользоваться человек (сотрудник), наибольшее количество кибер-преступлений совершается с использованием социальной инженерия по статистике лаборатории Касперского только за последний месяц методами социальной инженерии было обмануто ~ 16 000 000 (4 %) пользователей, к сравнению программы вымогатели затронули ~ 8 000 000 (2 %) [1]. В наше время главной уязвимостью в любой информационной системе остаётся человек, как самый наглядный пример это атака на иранскую ядерную программу со стороны FBI, каждый сотрудник — это потенциально главная уязвимость в информационной сети отдельного предприятия.

Социальная инженерия — в контексте информационной безопасности — психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. Совокупность уловок с целью сбора информации, подделки или несанкционированного доступа от традиционного мошенничества отличается тем, что часто является одним из многих шагов в более сложной схеме мошенничества.

Социальная инженерия отличается от других видов мошенничества тем, что она не основана на технических или кибернетических способах взлома сис-

тем, а на манипуляции людьми. Злоумышленники, используя социальную инженерию, стремятся обмануть и дезориентировать своих жертв, чтобы получить доступ к конфиденциальным данным или финансовым ресурсам.

В отличие от фишинга или вредоносных программ, использование социальной инженерии не требует сложных технологических навыков. Злоумышленники могут использовать как поддельные звонки*, электронные письма или сообщения в социальных сетях, чтобы убедить своих жертв раскрыть чувствительную информацию.

Таким образом, социальная инженерия представляет особую угрозу, поскольку она направлена не на слабые места в программах и уязвимости в системах, а на самого человека и его доверие, ведь из года в год более половины угроз реализуются именно через человека, имеющего легальный доступ, В 2023 доля инцидентов умышленного характера как в мире, так и в России превысила 98 %. Умышленные утечки данных только в России с 78,8 % выросли до 98,4 % [1] («Infowatch» ФИНАНСОВЫЙ СЕКТОР 2023). Различия в подходе и методах делают социальную инженерию более трудной для выявления и борьбы с ней, поэтому важно быть бдительным и следовать мерам предосторожности в онлайн и офлайн средах.

Опасности социальной инженерии

Социальные инженеры могут использовать различные способы, такие как маскировка под доверенное лицо или фальшивое представление, чтобы получить конфиденциальную информацию, такую как пароли, номера кредитных карт или личные данные.

Перечислим основные последствия от атак методами социальной инженерии:

1. Риск финансовых потерь. С помощью социальной инженерии мошенники могут обмануть людей и получить доступ к их банковским счетам или кредитным картам, что может привести к финансовым потерям.
2. Угроза безопасности сети. Социальные инженеры могут обмануть сотрудников организации, чтобы получить доступ к сети и скомпрометировать ее безопасность, украв конфиденциальные данные или распространяя вредоносное ПО.
3. Потенциальный ущерб репутации: Если организация становится жертвой социальной инженерии, и конфиденциальная информация о ее клиентах или сотрудниках утекает, это может нанести серьезный ущерб ее репутации и доверию общественности.
4. Возможность для других видов атак. Социальная инженерия может служить входной точкой для других видов кибератак, таких как фишинг или злоумышленное программное обеспечение, что увеличивает риск для организации.
5. Возможные финансовые потери. злоумышленники могут использовать социальную инженерию для обмана пользователей и получения доступа к их финансовым данным. Например, они могут представиться сотрудниками банка или другой финансовой организации и попросить пользователей предос-

тавить им свои личные данные, такие как номера кредитных карт, пин-коды и т. д.

Потеря конфиденциальной информации: социальная инженерия может привести к утечке конфиденциальных данных организации или ее сотрудников. Например, злоумышленники могут обмануть сотрудника, чтобы он предоставил им доступ к корпоративной сети или конфиденциальной информации.

Вред для репутации: успешные атаки с использованием социальной инженерии могут нанести серьезный ущерб репутации организации. Пользователи и клиенты могут потерять доверие к компании, если узнают, что их данные были скомпрометированы из-за неосторожности ее сотрудников).

Потенциальные последствия для личной безопасности при атаках с использованием социальной инженерии, за счёт заполучения информации злоумышленником, могут включать в себя:

1. Кражу личной информации.
2. Финансовые потери.
3. Репутационный ущерб.
4. Угрозы физической безопасности.

Последствия успешной атаки методом социальной инженерии могут быть различными и зависят от целей злоумышленников. Некоторые возможные последствия включают в себя:

1. Получение доступа к конфиденциальной информации: злоумышленники могут получить доступ к паролям, данным банковских счетов, персональная информация и др.
2. Финансовые потери: перевод средств с банковского счета жертвы на сторонние счета.
3. Нарушение безопасности систем: использование полученных данных для нанесения ущерба системе или сети, например, проведение DDoS-атаки.
4. Распространение вредоносного ПО: заражение системы с целью получения контроля над устройством, информацией или сетью.
5. Негативное воздействие на психологическое состояние: жертвы атак социальной инженерии могут испытывать стресс, страх или даже панику, что может привести к различным заболеваниям в результате нарушения их личной жизни и конфиденциальности.

В целом, успешная атака методом социальной инженерии может привести к серьезным последствиям для жертвы, и поэтому важно быть бдительным и предпринимать меры по защите от таких атак.

Для защиты от атак, посредством социальной инженерии важно:

– проводить обучение сотрудников на предмет определения подозрительных ситуаций;
– внедрять многофакторной аутентификации;
– актуализировать организационный и программно-аппаратный аспект защиты информации.

Обучение сотрудников для определения подозрительных ситуаций – важная часть защиты от атак с использованием социальной инженерии. Сотрудники должны уметь узнавать типичные признаки мошенничества, такие как попытки получить личную информацию, угрозы или принуждение к выполнению действий.

Систематические тренинги и обучающие программы повысят осведомленность сотрудников и укрепят защиту компании от атак со стороны социальных инженеров. Кроме того, важно создать внутренние политики и процедуры по обработке обращений и ситуаций, связанных с возможным мошенничеством.

Использование многофакторной аутентификации — важный способ защиты. При многофакторной аутентификации пользователь должен подтвердить свою личность не только с помощью пароля, но и с помощью другого фактора, такого как SMS-код, биометрические данные или специальные устройства. Это делает процесс взлома учетной записи гораздо сложнее для злоумышленников.

Кроме того, важно быть осторожным при общении с незнакомыми людьми, не раскрывать личную или рабочую информацию и не переходить по подозрительным ссылкам. Социальная инженерия представляет серьезную опасность для компаний и частных лиц. Мошенники, используя различные методы манипуляции и обмана, могут получить доступ к личной и конфиденциальной информации, взломать системы безопасности и причинить серьезный ущерб как финансовый, так и репутационный. Чтобы защитить себя от опасностей социальной инженерии, необходимо быть предельно бдительным и осведомленным, обучать сотрудников и соблюдать меры безопасности при обработке конфиденциальной информации. Кроме того, регулярное обновление программного обеспечения и использование надежных паролей также помогут укрепить защиту от атак мошенников.

Список источников

1. «Infowatch» Финансовый сектор: утечки конфиденциальной информации. Мир – Россия, 2021–2023. URL: https://www.infowatch.ru/sites/default/files/analytics/files/finansoviy-sektor-utechki-konfidentsialnoy-informatsii-za-tri-goda-mir-rossiya.pdf.

2. «Kaspersky lab» Статистика информационных-угроз. URL: https://statistics.securelist.com/mail-anti-virus/month.

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Степанов А. Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

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

Вклад авторов

Степанов А. Д. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Лысов Д. А. – написание статьи, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.53

Оценка уровня соответствия информационной безопасности стандартам и нормативам

Дмитрий Витальевич Терехов[1]✉, Павел Андреевич Менщиков[2], Владимир Романович Семенов[3]
[1, 2, 3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1, 2, 3] nauchnajrota@yandex.ru✉, https://orcid.org/0009-0007-5540-2719

Аннотация. В современном цифровом мире информационная безопасность играет ключевую роль в обеспечении стабильной работы организаций и защите их ресурсов от различных угроз. Однако, для достижения высокого уровня защиты необходимо не только иметь соответствующие технические средства, но и следовать стандартам и нормативам информационной безопасности. Оценка уровня соответствия этих стандартов и нормативов является важным этапом в процессе обеспечения безопасности информации в организации. В данной статье мы рассмотрим опыт внедрения такой оценки и предложим практические рекомендации для успешной реализации данного процесса.

Ключевые слова: информационная безопасность, оценка уровня соответствия, угрозы.

Для цитирования: Терехов Д. В., Менщиков П. А., Семенов В. Р. Оценка уровня соответствия информационной безопасности стандартам и нормативам // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 261–264.

Значение стандартов и нормативов в информационной безопасности

Первоначально разработанные для установления единых требований и подходов к обеспечению безопасности информации, стандарты и нормативы служат основой для создания систем управления информационной безопасностью (ИБ). Они определяют ключевые аспекты защиты информации, включая политики безопасности, процедуры управления рисками, технические меры защиты, а также требования к обучению и осведомленности сотрудников.

Одним из наиболее широко используемых наборов стандартов в области информационной безопасности является серия *ISO/IEC* 27000. Эти стандарты, начиная с *ISO/IEC* 27001:2013, определяют требования к системам управления информационной безопасностью и предоставляют общую методологию для их внедрения, аудита и постоянного совершенствования [1].

Однако следует отметить, что реализация стандартов и нормативов по информационной безопасности не является панацеей. Каждая организация должна адаптировать их под свои уникальные потребности и особенности своей деятельности. Это требует глубокого понимания бизнес-процессов, информационных потоков и угроз, с которыми организация может столкнуться [2].

Процесс оценки уровня соответствия

Процесс оценки уровня соответствия информационной безопасности стандартам и нормативам является многоступенчатым и включает в себя ряд ключевых этапов. Давайте рассмотрим каждый из них более подробно:

– подготовка. На этом этапе определяются цели и область применения оценки, выбираются соответствующие стандарты и нормативы, которым должна соответствовать организация. Также определяются ресурсы и ответственные лица, которые будут вовлечены в процесс оценки;

– сбор информации. Этот этап включает в себя сбор необходимой информации о текущих практиках и процедурах безопасности, политиках и стандартах, используемых технологиях, защищаемых ресурсах и других аспектах информационной безопасности;

– анализ. После сбора информации проводится ее анализ с целью выявления пробелов, недостатков и несоответствий с выбранными стандартами и нормативами. Этот этап может включать в себя аудит системы безопасности, технический анализ уязвимостей, оценку политик и процедур;

– оценка уровня соответствия. На основе результатов анализа проводится оценка уровня соответствия текущих практик и процедур выбранным стандартам и нормативам. Это может включать в себя оценку соответствия каждому требованию стандарта, выделение приоритетных областей для улучшения и определение общего уровня соответствия;

– разработка плана мероприятий. На основе выявленных несоответствий разрабатывается план мероприятий по устранению проблем и повышению уровня соответствия. В этот план включаются конкретные шаги, ресурсы, сроки и ответственные лица;

Процесс оценки уровня соответствия информационной безопасности стандартам и нормативам является ключевым элементом в обеспечении эффективной защиты информации в организации. Правильное выполнение каждого из этапов позволяет выявить и устранить проблемы в области безопасности и повысить уровень защиты организации от различных угроз [3].

Опыт внедрения стандартов и нормативов

В процессе внедрения стандартов и нормативов в области информационной безопасности ключевым аспектом является умение адаптировать их к конкретным потребностям и характеристикам организации.

Это требует тщательного анализа бизнес-процессов, выявления уязвимостей и оценки рисков. Важно также обеспечить поддержку и вовлечение руководства и персонала на всех уровнях, чтобы обеспечить успешную реализацию

изменений. Кроме того, регулярное обновление и адаптация стандартов и нормативов в соответствии с изменяющими угрозами и развитием технологий играют ключевую роль в обеспечении эффективной защиты информации.

Практические рекомендации

Внедрение стандартов и нормативов в области информационной безопасности может быть успешным при соблюдении определенных практических рекомендаций:

– адаптация к конкретной ситуации. Учитывайте особенности вашей организации при выборе и внедрении стандартов и нормативов. Не копируйте чужие подходы, а адаптируйте их к вашим потребностям;

– вовлечение всех заинтересованных сторон. Обеспечьте участие руководства, *IT*-отдела, юридического отдела и других заинтересованных сторон. Это поможет сформировать единую команду и обеспечить поддержку на всех уровнях организации;

– обучение персонала. Проведите обучение персонала по вопросам информационной безопасности и стандартам, чтобы они понимали свою роль и ответственность в обеспечении безопасности информации;

– постепенное внедрение. Разбейте процесс внедрения на этапы и постепенно внедряйте изменения. Это поможет избежать существенных перегрузок и улучшит адаптацию персонала к новым требованиям;

– мониторинг и обновление. Установите систему мониторинга и регулярно обновляйте стандарты и нормативы в соответствии с меняющими угрозами и технологическим развитием;

– постоянное совершенствование. Внедрение стандартов и нормативов является непрерывным процессом. Постоянно анализируйте свои практики и процедуры, ищите пути их улучшения и совершенствуйте систему защиты информации;

– внимание к человеческому фактору. Обратите внимание не только на технические аспекты безопасности, но и на человеческий фактор. Обучайте сотрудников основам информационной безопасности и поддерживайте культуру безопасности в организации.

Соблюдение этих рекомендаций поможет обеспечить успешное внедрение стандартов и нормативов информационной безопасности в вашей организации и повысить уровень защиты информации.

Заключение

Внедрение стандартов и нормативов информационной безопасности играет важную роль в обеспечении защиты цифровых ресурсов и конфиденциальности информации в современных организациях. Правильно спланированный и реализованный процесс внедрения позволяет организациям не только соблюдать требования регуляторов и стандартов, но и эффективно реагировать на существующие и новые угрозы информационной безопасности.

Важно подчеркнуть, что успешное внедрение стандартов и нормативов требует не только технических знаний, но и внимания к организационным и человеческим аспектам. Вовлечение руководства, обучение персонала и создание культуры безопасности являются ключевыми элементами этого процесса.

В конечном итоге, внедрение стандартов и нормативов информационной безопасности должно рассматриваться как стратегическая инвестиция, способствующая повышению конкурентоспособности организации и защите её репутации и доверия клиентов. Внимательное внедрение, систематический анализ и постоянное совершенствование помогут организациям оставаться надежными и устойчивыми в цифровой среде сегодня и в будущем.

Список источников

1. Волков М.И., Соколов В.В., Меньшенин Ю.С. Информационная безопасность: аудит и защита информационных систем // Информационная безопасность. 2013. №3. С. 134-144.

2. Иванов В.В. Информационная безопасность. Стандарты и сертификация // Стандартизация. 2011. №2. С. 11-21.

3. Андреев А.А., Бабушкин А.И., Михайленко И.В. Информационная безопасность предприятия. Стандарты, технологии, практики // Информационная безопасность. 2015. №5. С. 101-108.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Терехов Д. В. – старший оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Менщиков П. А. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Семенов В. Р. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Терехов Д. В. – идея, сбор материала, обработка материала, частичное написание статьи (60 %).

Менщиков П. А. – написание статьи, частичное написание статьи (20 %).

Семенов В. Р. – подбор литературных источников, научное редактирование текста (20 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 343

Проблема распространения деструктивной информации в социальных сетях

Анастасия Константиновна Тимашкова[1]✉,
Оксана Михайловна Голембиовская[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] timaschkova.nastya@yandex.ru, https://orcid.org/0009-0001-3142-4928
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133

Аннотация. В статье изучается проблема распространения деструктивной информации в социальных сетях. Дается определение деструктивной информации и анализируются факторы, способствующие ее распространению. Также обсуждаются воздействия вредоносного контента на пользователей и предлагаются меры по борьбе с ее распространением.

Ключевые слова: деструктивная информация, вредоносный контент, социальные сети, Интернет, негативное влияние.

Для цитирования: Тимашкова А. К., Голембиовская О. М. Проблема распространения деструктивной информации в социальных сетях // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 265–268.

В современном мире социальные сети стали неотъемлемой частью повседневной жизни многих людей. Согласно ежегодному отчету Digital 2023 Global Overview Report, где собраны все последние данные аудитории сети Интернет в России, на январь 2023 года насчитывалось 106 миллионов пользователей соцсетей, что составляет 73,3 % от общей численности населения страны [11]. Наиболее часто используемыми социальными платформами в России оказались: ВКонтакте 75,3 %, Telegram 64,4 % и Одноклассники 43,5 %.

Приведенные Интернет-ресурсы предоставляют возможность устанавливать коммуникацию, узнавать новости и проводить досуг. Однако вместе с этим социальные сети также могут быть источником деструктивной информации, которая может нанести вред пользователям.

Целью данного исследования является проведение анализа проблемы распространения деструктивной информации в социальных сетях и приведение рекомендаций по ее решению.

В законодательстве Российской Федерации нет определения «деструктивной информации», однако в Федеральном законе от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» есть понятие «информация, причиняющая вред здоровью и (или) развитию де-

тей» — «…побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью…; способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; обосновывающая или оправдывающая допустимость насилия и (или) жестокости…; отрицающая семейные ценности…; оправдывающая противоправное поведение…» и т. д. [2].

Кроме того, к деструктивной информации можно отнести информацию, распространение которой запрещено в Российской Федерации. Согласно Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» — это информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды [1]. В этот же перечень входит информация, за распространение которой предусмотрена уголовная или административная ответственность, в том числе за демонстрацию запрещенной нацисткой символики и атрибутики (ч. 1 ст. 20.3 КоАП РФ), возбуждение ненависти и вражды (ст. 20.3.1 КоАП РФ, ч. 1 ст. 282 УК РФ), распространение экстремистских материалов (ст. 20.29 КоАП РФ), призывы к осуществлению экстремистской деятельности (ч. 2 ст. 280 УК РФ), распространение порнографических материалов (ч. 3 ст. 242 УК РФ), публичные оскорбления (ч. 2 ст. 5.61 КоАП РФ), доведение и покушения до самоубийства (ч. 2 ст. 110 УК РФ), пропаганда нетрадиционных сексуальных отношений (ч. 3-4 ст. 6.21 КоАП РФ), распространение материалов, оказывающих вредное влияние на здоровье (ч. 1 ст. 13.15 КоАП РФ), сбыт наркотических средств (ч. 2 ст. 228.1 УК РФ) и т.д. [3, 4].

Таким образом под деструктивной информацией можно понимать любую информацию, которая имеет разрушительное, пагубное влияние и может нанести вред человеку или сподвигнуть его к причинению вреда другому. Вредоносный контент может быть представлен в различных формах, таких как текст, изображения, видео и аудио.

Проблема выявления деструктивных материалов в социальных сетях становится все более острой в связи с ростом числа пользователей и увеличением объема информации. Вредоносный контент может оказывать пагубное влияние на психическое и эмоциональное состояние владельцев аккаунтов, привести к развитию девиантного поведения, а также способствовать распространению негативных явлений в обществе.

Многие российские ученые исследуют проблемы, касающиеся деструктивной информации в Интернет-пространстве — изучают влияние на пользователей, разрабатывают методы ее обнаружения и противодействия. Такая тематика рассматривалась в работах авторов А. И. Дауров, Р. Р. Гедугошев [5], В. В. Тельбух, А. В. Десятых, С. С. Андрушкевич, Л. В. Пилипенко [6], М. Ж. Хачеритлова, Р. А. Хачидогов [7, 8], В. Н. Цимбал [9] и др.

Социальные сети особенно привлекательны для злоумышленников благодаря своей популярности, трансляции личной жизни пользователей и возмож-

ности налаживания коммуникации. По итогам 2023 года в России зафиксирован рост деструктивного контента почти в два раза, на основании решений Росмолодежи было заблокировано более 31,5 тысяч материалов, согласно новостной газете «Известия» [10].

Распространение вредоносного контента в Интернет-пространстве представляет большую угрозу, особенно для подростковой и молодежной аудитории. Поскольку несовершеннолетним часто присущи эмоциональность, отсутствие жизненного опыта и устойчивой сформированной психики, они часто не способны мыслить критически и не могут оценить достоверность поступающей информации. Такие факторы делают их подверженными негативному влиянию и информационным воздействиям.

Исходя из вышенаписанного проблема распространения деструктивной информации в социальных сетях является актуальной и требует должного внимания и принятия мер на уровне социальных сетей, государства и общества.

В соцсетях требуется внедрять механизмы контроля за содержанием публикуемой информации, такие как модерация, фильтрация и блокирование. В рамках законодательства необходимо и дальше разрабатывать и внедрять документацию, регулирующею распространение деструктивной информации на Интернет-платформах. На уровне общества нужно повышать осведомленность граждан о проблеме распространения вредоносного контента и обучать их распознавать его.

Также для обеспечения безопасности пользователей сети, предотвращения распространения информации, которая может нанести вред их психическому и эмоциональному состоянию, а также для защиты общества от возможных негативный последствий, необходимо разработать методику выявления деструктивной информации в социальных сетях.

Разработка такой методики позволит не только своевременно обнаруживать и блокировать вредоносный контент, но и принимать меры для предотвращения его появления в будущем.

В заключении стоит отметить, что рассмотренная проблема распространения деструктивной информации в социальных сетях является особенно серьезной в настоящее время. Используя комплексный подход совместными усилиями, можно добиться снижения ее распространения и защиты пользователей от негативного воздействия.

Список источников

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ. Доступ из СПС «Консультант Плюс».

2. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 г. № 436-ФЗ. Доступ из СПС «Консультант Плюс». – Ст. 5.

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Доступ из СПС «Консультант Плюс».

4. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ. Доступ из СПС «Консультант Плюс».

5. Дауров А.И., Гедугошев Р.Р. Деструктивная информация в социальных сетях и мессенджерах: проблемы обнаружения и противодействия // Журнал прикладных исследований. 2022. С. 92-95.

6. Тельбух В.В., Десятых А.В., Андрушкевич С.С., Пилипенко Л.В. Метод выявления деструктивного контента в информационных интернет-ресурсах // Известия Тульского государственного университета. Технические науки. 2023. С. 423-428.

7. Хачеритлов М.Ж., Хачидогов Р.А. Ультраправые экстремистские сообщества в социальных сетях: проблемы обнаружения и противодействия // Журнал прикладных исследований. 2022. С. 85-88.

8. Хачидогов Р.А. Проблемы обнаружения и блокировки в социальных сетях деструктивного медиаконтента // Журнал прикладных исследований. 2022. С. 161-164.

9. Цимбал В. Н. Анализ деструктивной информации в социальных сетях и мессенджерах // Вестник Московского университета МВД России. 2022. № 4. С. 269–274.

10. Объем деструктивного контента в РФ вырос вдвое в 2023 году // Известия URL: https://iz.ru/1633164/2024-01-12/obem-destruktivnogo-kontenta-v-rf-vyros-vdvoe-v-2023-godu (дата обращения: 19.04.2024).

11. DataReportal. Digital 2023: Russian Federation [Электронный ресурс]. URL: https://datareportal.com/reports/digital-2023-russian-federation (дата обращения: 19.04.2024).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Тимашкова А. К. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Тимашкова А. К. – идея, сбор материала, обработка материала, написание статьи, научное редактирование текста (90 %).

Голембиовская О. М. – научное руководство (10 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.52

Защита речевой информации от утечки по виброакустическим каналам

Никита Сергеевич Толстошеин[1]✉, Михаил Алексеевич Свиридов[2], Павел Андреевич Менщиков[3], Виктор Васильевич Шатских[4]

[1, 2, 3, 4] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1, 2, 3, 4] nauchnajarota@yandex.ru✉, https://orcid.org/0009-0007-5540-2719

Аннотация. В статье **рассмотрены** основные аспекты защиты речевой информации от утечки по виброакустическим каналам. Обсуждаются перспективы использования шумовой речеподобной помехи. Представлено комбинированное средство виброакустической защиты. Обсуждаются проблемы использования данного средства, а также подход к решению данной проблемы через модернизацию программного обеспечения дополнительными маскирующими речеподобными помехами.

Ключевые слова: виброакустический канал утечки информации, защита информации, речеподобная помеха.

Для цитирования: Толстошеин Н. С., Свиридов М. А., Менщиков П. А., Шатских В. В. Защита речевой информации от утечки по виброакустическим каналам // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 269–273.

Введение

В современном мире информация является одним из важнейших объектов для защиты. Главным источником передачи информации во все времена являлась речь. Современные средства нелегального съема информации способны получить конфиденциальную информацию по виброакустическим каналам без проникновения в защищаемое помещение. Таким образом, защита речевой информации от утечки по виброакустическим каналам — важная задача в комплексе мероприятий по обеспечению информационной безопасности.

Виброакустический канал состоит из следующих элементов: объект сигнала, среда распространения, агент, принимающий данные [1].

Принцип работы канала основан на способности звуковой волны вызывать механические колебания в препятствиях, через которые она проходит при распространении. Эти колебания при помощи оборудования и соответствующего программного обеспечения преобразуются в связный текст [2, 5].

Основные конструкции, используемые для перехвата виброакустических сигналов [3, 5]:

- несущие стены и перегородки;
- перекрытия;
- оконные рамы;
- коробы дверных проемов;
- стекла;
- трубы тепло- и водоснабжения;
- каналы вентиляции.

Съемное устройство может быть не только установлено на сами конструкции, но и направлены на них, находясь в отдалении от охраняемого помещения, что существенно затрудняет поиск этих технических средств.

Использование генераторов акустического и виброакустического шумов позволяют предотвратить утечку информации по виброакутическому каналу. Существует несколько типов шумов:

- «Белый» шум;
- «Розовый» шум;
- «Коричневый» шум;
- шумовая речеподобная помеха.

Наиболее перспективным является использование шумовой речеподобной помехи, так как она имитирует характеристики речи человека, тем самым затрудняя распознавание и выделение речевого сигнала говорящих. Принцип действия речеподобных помех заключается в создании помех, схожих с речевыми сигналами по спектральным и временным характеристикам. Это делает их незаметными для человеческого уха и затрудняет выделение полезного речевого сигнала [2]. Речеподобные помехи разделяются на два типа: речеподобная реверберационная и речеподобная инверсионная.

Принцип работы речеподобной реверберационной помехи основан на формировании помехи из речевых фрагментов говорящих, с многократным наложением их друг на друга на различных уровнях.

Комбинированное средство виброакустической защиты (рис. 1) может применяться для защиты от утечек по акустическому и виброакустическому каналу помещений и командных пунктов, в которых ведутся разговоры стратегической важности. Система создает виброакустические шумовые помехи в воздушной среде, элементах ограждающих конструкций и в инженерно-технических коммуникациях защищаемых помещений [4].

Генерация шума имеет следующие особенности [5]:

• вместе с белым шумом создается речеподобный, что улучшает маскирующие характеристики, отделение потоков друг от друга становится маловероятным;

• мощность шума автоматически повышается при усилении речи, что улучшает степень защиты;

• маскирующие шумы не мешают рабочему процессу.

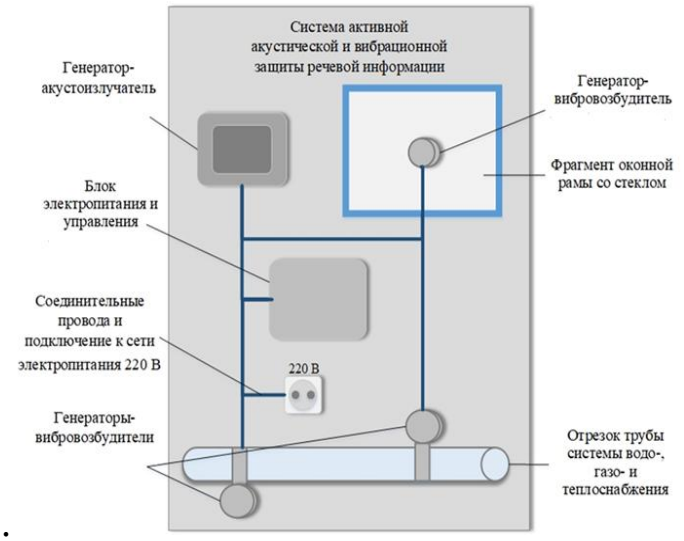
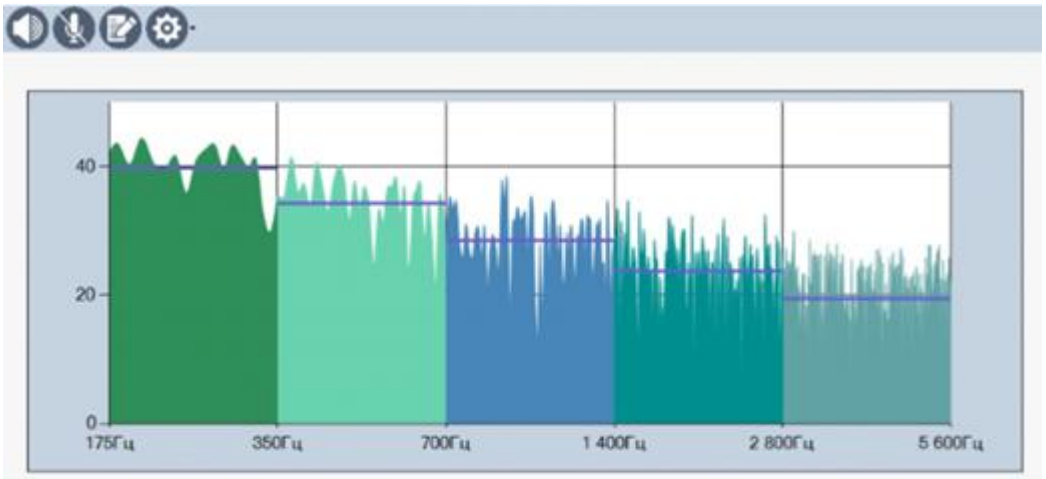


Рис. 1. Схема комплекса «Система активной акустической и вибрационной защиты речевой информации»

Программное обеспечение (рис. 2) используется для записи и построения спектра сигнала, настройки уровня акустической помехи для достижения необходимой защищенности помещения и вычисления коэффициента словесной разборчивости.



№ октавы	Диапазон частот	Средняя частота	Уровень сигнала, дБ	Уровень шума, дБ	W
1	175-350	250	72,0203210441...	42,998011294931	0,99622359111...
2	350-700	500	83,2573470191...	41,1686627267...	0,99622359111...
3	700-1400	1000	92,7085700058...	28,4820979658...	0,99622359111...
4	1400-2800	2000	84,2516611439...	26,9002811186...	0,99622359111...
5	2800-5600	4000	83,8139085167...	22,762621022739	0,99622359111...

Рис. 2. Программное обеспечение

Современные методы съема конфиденциальной информации позволяют злоумышленникам отделять помехи от интересующей их информации и если не в полной мере, то хотя бы отрывками понять суть разговора, что может привести к неприятным последствиям.

Заключение

Эффективная защита информации — ключ к успеху не только в конкурентной борьбе, но и в проведении СВО. Модернизированный программно-аппаратный комплекс позволит более эффективно противодействовать техническим средствам разведки противника и сохранить конфиденциальность разговора.

Список источников

1. Каторин, Ю.Ф. Защита информации техническими средствами: Учебное пособие [Текст] / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. – СПб.: НИУ ИТМО, 2012. – 416 с.

2. Алексеев, В.В. Сравнительная характеристика методов разборчивости речи / В.В. Алексеев, А.В. Яковлев, М.В. Моисеева // XXVIII Международная научно-техническая конференция «Современные технологии в задачах управления, автоматики и обработки информации». – М: Изд. «НИЯУ «МИФИ», 2019. – С. 85 – 86.

3. Хорев, А.А. Техническая защита информации [Текст]/ А.А. Хорев. – М.: НПЦ «Аналитика», 2008. – 436 с.

4. Бузов, Г.А. Защита от утечки информации по техническим каналам [Текст] / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия-Телеком, 2005. – 415 с.

5. Алексеев В.В., Клинков Д.А., Яковлев А.В. Способ защиты речевой информации в офисном помещении // Правовая информатика. – 2023. - № 2. – С. 44 – 53.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Толстошеин Н. С. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Свиридов М. А. – старший оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Менщиков П. А. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Шатских В. В. – старший научный сотрудник роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Толстошеин Н. С. – написание статьи, редактирование текста (40 %).

Свиридов М. А. – подбор литературных источников, частичное написание статьи (20 %).

Менщиков П. А. – научное редактирование текста, частичное написание статьи (20 %).

Шатских В. В. – научное редактирование текста, подбор литературных источников (20 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 378:004

Особенности проблематики системы менеджмента информационной безопасности

Данила Владимирович Хамцов
Брянский государственный технический университет, Брянск, Россия
danilaxv@yandex.ru, https://orcid.org/0009-0001-7839-4180

Аннотация. В данной статье будет рассмотрена проблематика популярного подхода управления информационной безопасностью в компаниях, проанализирован подход к автоматизации бизнес-процессов смежных отделов и сформулирован ответ на вопрос, что же можно и нужно делать, чтобы службы информационной безопасности тревожно не утопали в перегрузках от рутины, а становились крепким иммунитетом организаций, позволяя завоевывать новые вершины.

Ключевые слова: информационная безопасность, автоматизации бизнес-процессов, цикл Деминга.

Для цитирования: Хамцов Д. В. Особенности проблематики системы менеджмента информационной безопасности // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 274–277.

Краеугольными камнями любой системы защиты являются риск-ориентированный подход, в процессе которого выявляются цели и задачи на основании рисков реализации угроз ИБ, создание СЗИ и СОУЗИ, а также обеспечение операционной надежности бизнеса. На рисунке 1 изображен треугольник, как визуализация границ безопасности любой компании, углы фигуры это и три сущности, без которых невозможно построение функционирующей системы защиты, в случае отсутствия одной из них, система, как и пирамида без опоры, начнет постепенно разрушаться.

Любая СЗИ имеет жизненный цикл, без корректного его поддержания, даже в случае правильного выстраивания с нуля, она все равно не сможешь существовать, поэтому каждый этап от написания политики информационной безопасности до внедрения средств антивирусной защиты необходимо рассматривать через призму методологии PDCA (цикла Деминга).

Рассмотрев, из чего состоит ИБ в компаниях, необходимо определить, как этим ИБ управлять. В большинстве случаев для каждого из процессов, описанных ранее, установлены свои порядки хранения и обработки информации, кто-то использует Excel-таблиц с чек-листами и дорожными картами, кто-то отчеты

на бумаге с описанием нынешнего статуса СЗИ, план-графиками задач на ближайший квартал, месяц, неделю. Взаимодействие между подразделениями ИБ, ИТ, рисков как правило ведется в корпоративных почтах или мессенджерах, что дополнительно влияет на время отклика по задачам. В такой парадигме большинство организаций и живет, но живет не эффективно.

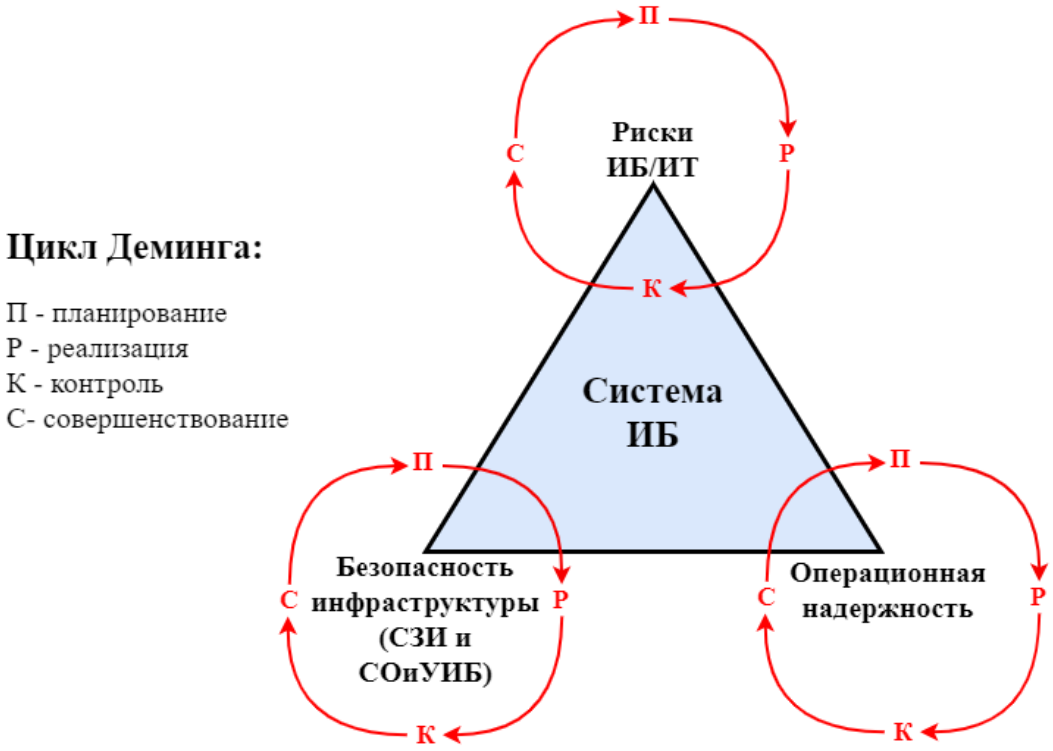


Рис. 1. Части построение системы информационной безопасности

Автоматизировав каждый процесс и исключив рутину формирования подобных отчетов, отслеживания состояние ИБ через мониторинг десятка автоматизированных систем, можно увеличить эффективность отделов информационной, экономической и физической безопасности на десятки процентов. Всеми процессами планирования-реализации-контроля-совершенствования можно управлять с использованием одной централизованной системы, которая интегрируется во все необходимые для этого ресурсы от Active Directory до базы рисков, позволяя взаимодействовать командам в режиме реального времени и сфокусироваться на коллективной работе для достижения максимального результата.

Для детального понимания похожим систем, необходимо проанализировать автоматизацию бизнес-процессов других подразделений организаций. Отделы продаж и отделы маркетинга для автоматизации процессов продаж, ускорения обработки информации о клиентах и аналитики используют CRM-системы. Подобные системы аккумулируют в себе все необходимые инструменты для быстрой, корректной, а самое главное эффективной работы, поэтому автоматизация бизнеса, очень важный инструмент для роста и стабильности компании.

В процессе построения системы защиты очень много взаимосвязанных элементов, начиная с людей и их взаимодействием, заканчивая непрерывным мониторингом функционирующих систем на наличие сбоев. Чем больше развивается компания, тем сложнее контролировать менеджмент ИБ, что приводит к деградации процессов.

Из-за большого количества задач, возложенных на службы ИБ, отследить и учесть все изменения в инфраструктуре практически невозможно, даже если это получается, то за счет обильного количества взаимосвязанных элементов, часть будет утеряна или забыта. Чтобы этого избежать, целесообразно использовать sGRC-системы, позволяющие объединять все процессы в единую сущность на базе общекорпоративной платформы и сокращать неэффективное время работы служб информационной безопасности, перенаправив ресурсы на более важные задачи.

Подводя итог, руководящий состав получает полную выжимку актуального статуса защищенности и соответствия инфраструктуры в виде понятных метрик. Ответственные за ИБ получают централизованный механизм управления процессами и мониторинга состояния СЗИ. Системные администраторы, и представители различных подразделений имеют возможность коммуницировать при выполнении задач по принципу «единого окна». А главное — на уровне всей организации есть общая модель компании, с единым перечнем активов и интеграцией с действующими средствами защиты. Это позволяет структурировать взаимодействие между подразделениями организации, гибко настраивать отчетность, управлять сложными задачами с уменьшением трудозатрат и транзакционных издержек.

Список источников

1. "Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27001-2021 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" " от 30.11.2021 № 27001-2021.

2. "Национальный стандарт РФ ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер"" от 08.07.2017 № 822-СТ // Центральный Банк России.

3. "Национальный стандарт РФ ГОСТ Р 57580.3-2022 "Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения"" от 22.11.2022 № 1548-ст.

4. "Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27005-2010 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности"" от 30.11.2010 №27005-2010.

5. "Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27000-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Систе-

мы менеджмента информационной безопасности. Общий обзор и терминология"" от 19.05.2021 № 27000-2021.

6. "Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27004-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание"" от 19.05.2021 № 27004-2021.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторе

Хамцов Д. В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, ФГБОУ ВО «БГТУ».

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 623.746.519

Использование современных методов шифрования для защиты канала управления беспилотным летательным аппаратом

Андрей Михайлович Хромов[1]✉, Владимир Владимирович Попов[2], Вячеслав Вячеславович Каштанов[3]
[1, 2, 3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1] nauchnajarota@yandex.ru✉, https://orcid.org/0009-0007-5540-2719
[2] lantrin3@gmail.com, https://orcid.org/0009-0007-5540-2719
[3] slavakashtanov302@gmail.com, https://orcid.org/0009-0007-5540-2719

Аннотация. Данная статья содержит краткий обзор роли беспилотных летательных аппаратов (БПЛА) в современном мире, актуальность темы необходимости защиты, каналов управления ими, а также методы шифрования, при помощи которых достигается определённый уровень защищённости канала управления БПЛА.

Ключевые слова: беспилотный летательный аппарат, канал управления БПЛА, методы шифрования, защита.

Для цитирования: Хромов А. М., Попов В. В., Каштанов В. В. Использование современных методов шифрования для защиты канала управления беспилотным летательным аппаратом // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 278–282.

Вступление

В настоящее время БПЛА достигли своего пика популярности благодаря технологическим достижениям в области микропроцессорных вычислений, навигации, информационных технологий (IT) и искусственного интеллекта (AI). Эти инновации привели к разработке различных типов беспилотных летательных аппаратов, каждый из которых имеет свое назначение, аэродинамические и тактико-технические характеристики.

Несмотря на растущую популярность беспилотных летательных аппаратов, их несанкционированное использование остается проблемой, особенно в таких строго контролируемых зонах, как аэропорты и военные базы. Это привело к необходимости принятия мер по противодействию этим летательным аппаратам.

Актуальность

Защита каналов связи между наземными станциями управления (НСУ) и беспилотными летательными аппаратами (БПЛА) от внешних программных и

аппаратных помех в настоящее время является серьезной проблемой [1]. Атаки на беспилотные летательные аппараты могут включать перехват управляющих сигналов, искажение телеметрических данных, вывод из строя транспортного средства, получение или изменение информации, передаваемой полезной нагрузкой, или инициирование дальнейших атак на сетевые системы.

Из-за особенностей радиосвязи между беспилотными летательными аппаратами и наземными станциями основным методом защиты является криптография с использованием секретных ключей на борту беспилотного летательного аппарата и на наземной станции. Однако, если один или несколько беспилотных летательных аппаратов будут скомпрометированы, ключи могут быть переданы злоумышленнику, что поставит под угрозу безопасность связи для остальных аппаратов.

Типы взломов БПЛА

Прежде чем рассмотреть особенности обеспечения информационной безопасности беспилотного летательного аппарата, необходимо для начала охарактеризовать типы взлома беспилотных летательных аппаратов.

Управление беспилотными летательными аппаратами осуществляется дистанционно посредством спутниковой или иной беспроводной линии передачи данных, вследствие чего возникают такие виды взлома беспилотных летательных аппаратов, как [2, 7]:

- Перехват трафика — более трудоемкий метод взлома беспилотного летательного аппарата, требующий применения специальных программ, либо антенны спутниковой связи. С помощью данного вида взламывания можно завладеть как управлением беспилотного летательного аппарат, так и конфиденциальными данными, которые передаются между пунктом управления и беспилотным летательным аппаратом и наоборот.
- Имитация и изменение геоданных: GPS передатчики, используемые беспилотным летательным аппаратом, передают мнимые сигналы, данные, чем нарушают навигационную систему беспилотного летательного аппарата. Данный способ обусловлен нарушением направления траектории беспилотного летательного аппарата для его захвата или посадки.

В качестве перспективных видов взломов беспилотных летательных аппаратов особое место занимают атаки с помощью технологий программно-определяемого радио, которые включают в себя [2, 7]:

- считывание и передачу сигнала на любой частоте: предполагается уязвимость всех частотных диапазонов, используемых для передачи конфиденциальной информации;
- применение универсального передатчика для перехвата и расшифровки радиосигналов: включает в себя не только перехват передаваемых данных от беспилотного летательного аппарата к оператору, и наоборот, но и полное завладение управлением беспилотного летательного аппарата;
- извлечение или расшифровка секретных ключей шифрования для передачи конфиденциальных данных.

На этом список угроз информационному обеспечению беспилотному летательному аппарату не ограничивается, так как виды взлома различают по их характеру, природе возникновения, и использованию различных вспомогательных средств и т. д.

Защита канала связи

Чтобы обеспечить конфиденциальность данных, передаваемых беспилотными летательными аппаратами, важно защитить их каналы связи. В настоящее время для этого используются различные методы, такие как периодическая регулировка рабочей частоты псевдослучайным образом, регулировка частот в случае прерываний связи и автоматическая посадка при длительной потере связи [3].

В симметричных методах шифрования используется один и тот же ключ как для кодирования, так и для декодирования данных, в то время как в асимметричных методах шифрования используются два разных ключа — один для шифрования, другой для дешифрования.

Схема симметричного шифрования представлена на рисунке 1 [4].

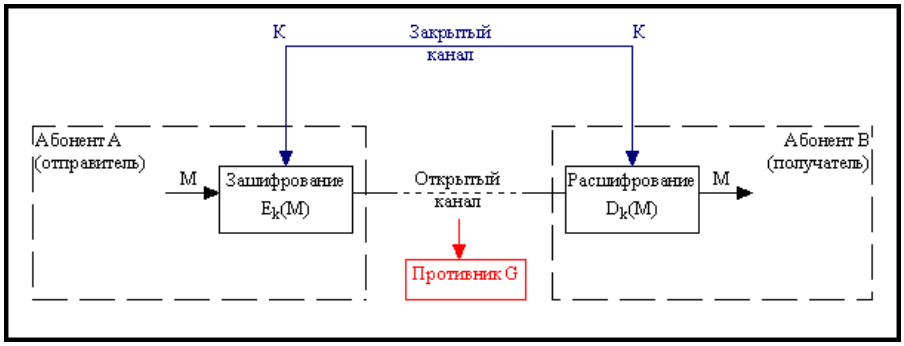


Рис. 1. Общая схема шифрования с закрытым ключом

Основным недостатком симметричного шифрования является сложность передачи ключа и обеспечения подлинности и надежности передаваемых данных. В отличие от этого, асимметричное шифрование использует пару открытых и закрытых ключей, которые математически связаны. Открытый ключ используется совместно с другими пользователями для шифрования данных, в то время как закрытый ключ хранится в секрете и используется для расшифровки зашифрованных данных. Это обеспечивает безопасную связь между сторонами, поскольку отправитель может зашифровать сообщение своим открытым ключом, а получатель может расшифровать его своим закрытым ключом.

Заключение

Несмотря на их широкое использование в различных областях, беспилотные летательные аппараты (БПЛА) подвержены взлому. Это не всегда делается с благими намерениями и может привести к неправильному использованию конфиденциальных данных. Чтобы свести к минимуму риск возникновения подобных ситуаций, важно принять меры для обеспечения безопасности беспи-

лотных летательных аппаратов. Это включает в себя использование методов шифрования для защиты передаваемых данных и обеспечение достаточной помехоустойчивости канала, используемого беспилотным летательным аппаратом.

Список источников

1. Способ криптографической защиты каналов связи между наземной станцией управления и одновременно несколькими управляемыми с нее беспилотными летательными аппаратами [Электронный ресурс] / И. Н. Оков, А. А. Устинов // РОССТИП : [патент] — URL: https://rosstip.ru/patents/... (дата обращения: 20.04.2024).

2. Фетисов В.С., Неугодникова Л.М., Адамовский В.В., Красноперов Р.А. Беспилотная авиация: терминология, классификация, современное состояние. Уфа., 2014

3. Панасенко С. Алгоритмы шифрования. - СПб., 2009.

4. Долгий, Е. Ю. Разработка схемы защищенного канала дальнего радиуса действия для наземной станции управления беспилотного летательного аппарата / Е. Ю. Долгий, К. В. Шошина, Р. А. Алешко. — Текст : непосредственный // Молодой ученый. — 2015. — № 13.1 (93.1). — С. 10-12. — URL: https://moluch.ru/archive/93/20826/ (дата обращения: 20.04.2024).

5. Боев Н.М. Анализ радиолиний связи с беспилотными летательными аппаратами. // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2012. С. 86-91.

6. Полынкин А.В. Исследование характеристик радиоканала связи с беспилотными летательными аппаратами // Известия ТулГУ. Технические науки. 2013. № 7., Ч.2.

7. Антощенко А.В. Особенности обеспечения информационной безопасности беспилотного летательного аппарата // Современные научные исследования и инновации. – 2021. - № 12 (128).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Хромов А. М. – оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Попов В. В. – старший инженер отдела опытной эксплуатации средств специальных воздействий, Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Каштанов В. В. – аспирант кафедры «Компьютерно-интегрированные системы в машиностроении», направление подготовки 2.3.8 Информатика и информационные процессы, ФГБОУ ВО «ТГТУ».

Вклад авторов

Хромов А. М. – сбор материала, обработка материала, написание статьи (50 %).

Попов В. В. – сбор материала, обработка материала (25 %).

Каштанов В. В. – идея, обработка материала (25 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004, 037

Инъекция команды операционной системы для воздействия на веб-ресурсы

Алина Михайловна Шапенская[1], Оксана Михайловна Голембиовская[2]
[1, 2]Брянский государственный технический университет, Брянск, Россия
[1] alinashapenskaya2002@gmail.com, https://orcid.org/0009-0007-8434-5848
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133

Аннотация. В данной статье рассмотрены особенности взаимодействия с инъекцией команды операционной системы и методы защиты системы от подобных атак.

Ключевые слова: внедрение команды, операционная система, инъекции веб-ресурс, веб-приложение, информационная безопасность.

Для цитирования: Шапенская А. М., Голембиовская О. М. Инъекция команды операционной системы для воздействия на веб-ресурсы // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 283–285.

Злоумышленники с каждым днем разрабатывают более сложные способы заполучить ценную информацию и оставаться безнаказанными. На сегодняшний день, одной из частых уязвимостей является внедрение команды операционной системы. «Шелл инъекция» или же внедрение команды ОС — это уязвимость веб-ресурсов, которая позволяет злоумышленнику выполнять произвольные команды операционной системы на сервере, на котором приложение выполняет свою работу, и, как правило, полностью скомпрометировать приложение и все его данные. [1] Как правило, термин «внедрение кода» относится к SQL-инъекциям, межсайтовому скриптингу (XSS), PHP-инъекциям и большому количеству других разновидностей инъекций. Главная особенность таких атак заключается в возможности выполнения несанкционированных команд ОС на удалённом сервере через любое уязвимое веб-приложение.

Используя такую уязвимость, злоумышленник может заполучить множество данных, в особенности следующую информацию:

- файлы паролей ОС;
- конфигурационные файлы ОС;
- исходный код самого веб-приложения.

Более того, хаккер имеет возможность получить командную оболочку для отправки системных команд на обратном шелле [2].

Инъекция уязвимости операционной системы происходит, когда пользовательский ввод используется непосредственно как часть команды ОС. Пользовательский ввод, должен прямо или косвенно влиять на веб-запрос, который выполняет системные команды. Языки веб-программирования имеют разные функции, которые позволяют разработчику выполнять команды операционной системы на внутреннем сервере. Это можно использоваться для различных целей, таких как установка плагинов или выполнение определенных действий. Выяснив на каком ЯП написано приложение и изучив его принцип действия, можно приступать к реализации атаки через уязвимость. Для примера возьмем веб-приложение, написанное на PHP. В таком случае можно использовать функции exec, system, shell_exec, passthru, popen для выполнения команд непосредственно на сервере, каждая из которых имеет несколько разные варианты использования. Если веб-приложение разработано в NodeJS, то для достижения такой же цели можно применить команду child_process.exec или child_process.spawn.

Одной из основных причин удачной реализации атак такого плана является отсутствие корректной валидации входных данных. Защита он инъекций команды ОС заключается в проверке входных данных на наличие разделителей команд и аргументов., а также необходимо убедиться в том, что внешние данные не приведут к подмене исходной команды.

Для обеспечения безопасности можно использовать функцию escapeshellcmd(). Она сможет экранировать символы, которые пользователь может использоваться для эксплуатации Command injection [3].

Еще один способ защиты заключается в использовании белых списков. Они являются более безопасными так как с их помощью разрешается к использованию только определенный набор символов. Все остальные символы должны быть запрещены. Использование черных списков крайне не рекомендуется т.к. злоумышленники смогут найти способ его обойти. Если все же есть необходимость в использовании черного списка, то в этом случае необходимо тщательно фильтровать применение следующих символов:

*{} () <> & * '| = ; [] $ - # ~! . ”% / \: +,`*

Не стоит забывать о программных средствах защиты. Существует много программного обеспечения для защиты веб-приложений от воздействия внешних факторов. Одним из такого ПО является межсетевой экран. Для подавляющего числа веб-приложений используется прикладной сетевой экран Web Application Firewall (WAF). Если это бизнес-приложение, которое содержит в себе базы данных с коммерческой информацией и сведениями о персональных данных клиентов, — то здесь необходимо использовать иной тип защиты — межсетевой экран баз данных Database Firewall (DBF). Это позволит защитить информацию на разных уровнях. [4] Кроме защиты от уязвимости внедрение команды ОС межсетевые экраны защищают от SQL-инъекций, от межсетевого скриптинга (XSS), помогают контролировать доступ к данным, тем самым предотвращая НСД. Брандмауэры своей работой могут предупредить множество негативных последствий, в особенности утечек данных, именно поэтому стоит

уделять особое внимание выбору файрвола и обязательно использовать его для защиты веб-приложений.

Подводя итоги, инъекция команды операционной системы является частой уязвимостью в ныне существующих веб-приложениях. Процесс реализации атаки через данную уязвимость довольно прост, а подтверждает этот факт огромное количество статей и видеороликов в сети Интернет. Из-за простоты реализации, некоторые пользователи сети Интернет решаются реализовать такую атаку ради забавы и даже не подозревают, что эти действия караются законодательством РФ. Однако предотвратить лишние воздействия на веб-ресурсы сможет лишь более сложная структура приложения и использование средств защиты информации.

Список источников

1. Внедрение команды ОС для атаки на веб приложения: [Электронный ресурс] – Режим доступа: https://itsecforu.ru/2019/09/27/%F0%9F%94%90-%D0%B2%D0%BD%D0%B5%D0%B4%D1%80%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D1%8B-%D0%BE%D1%81-%D0%B4%D0%BB%D1%8F-%D0%B0%D1%82%D0%B0%D0%BA%D0%B8-%D0%BD%D0%B0-%D0%B2%D0%B5/ (Дата обращения 19.03.2024).

2. Внедрение команд ОС: понятие, эксплуатация, автоматизированный поиск уязвимости: [Электронный ресурс] – Режим доступа: https://hackware.ru/?p=1133 (Дата обращения 19.03.2024).

3. Статья про инъекции команд | Command Injection: [Электронный ресурс] – Режим доступа: https://codeby.net/threads/statja-pro-inekcii-komand-command-injection.82042/ (Дата обращения 20.03.2024).

4. Зачем нужна защита web-приложений?: [Электронный ресурс] – Режим доступа: https://gardatech.ru/articles/smi/informatsionnaya-bezopasnost-web-prilozheniy-sovremennye-resheniya/ (Дата обращения 20.03.2024).

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Шапенская А. М. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – «Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Вклад авторов

Шапенская А. М. – обработка материала, написание статьи, научное редактирование текста (50 %).

Голембиовская О. М. – научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004

Рекомендации к разработке средств защиты информации с применением технологий искусственного интеллекта

Алина Михайловна Шапенская[1], Оксана Михайловна Голембиовская[2], Виталий Владимирович Вороненко[3], Дмитрий Владимирович Логвинов[4]
[1, 2, 4] Брянский государственный технический университет, Брянск, Россия
[3] Брянский филиал Российского экономического университета им. Г. В. Плеханова, Брянск, Россия
[1] alinashapenskaya2002@gmail.com, https://orcid.org/0009-0007-8434-5848
[2] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133
[3] voronenkovitalik666@gmail.com, https://orcid.org/0009-0001-1115-5935
[4] logvinovdmitriv@gmail.com, https://orcid.org/0009-0004-6399-4396

Аннотация. В данной статье освещается актуальность разработки средств защиты информации с применением технологий искусственного интеллекта. Обсуждаются методы обеспечения безопасности данных в контексте кибератак и угроз кибербезопасности с использованием ИИ. Подчеркнута важность инновационных решений для эффективной защиты информации, с уточнением роли искусственного интеллекта в повышении кибербезопасности.

Ключевые слова: защита информации, технологии искусственного интеллекта, кибербезопасность, информационная безопасность, кибератаки, угрозы кибербезопасности.

Для цитирования: Шапенская А. М., Голембиовская О. М., Вороненко В. В., Логвинов Д. В. Рекомендации к разработке средств защиты информации с применением технологий искусственного интеллекта // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 286–290.

С развитием цифровых технологий и расширением информационного пространства вопрос об обеспечении защищенности данных является наиболее актуальным. В контексте современных вызовов на первый план выходит необходимость разработки эффективных средств защиты информации. В этом контексте технологии искусственного интеллекта (ИИ) становятся неотъемлемой частью стратегии обеспечения цифровой безопасности. Рассмотрим ключевые аспекты этого направления.

В ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» можно найти перечень терминов, которые раскроют представление об сфере защиты информации. В них даётся чёткое определение: Безопасность

информации (или информационная безопасность, сокращенно ИБ) — это состояние защищенности информации, при котором обеспечиваются её целостность, конфиденциальность, доступность [1].

Искусственный интеллект — это комплекс технологий, разработанный для моделирования когнитивных процессов человека с целью достижения результатов, аналогичных тем, которые могут быть достигнуты при решении интеллектуальных задач человеком. Внедрение подобных технологий происходило постепенно в различных отраслях, оказывая значительное воздействие на развитие технологий. Искусственный интеллект становится ключевым элементом средств защиты информации, обеспечивая более интеллектуальные и адаптивные решения в сфере кибербезопасности.

Основная причина внедрения искусственного интеллекта в кибербезопасность — это его способность быстро проработать и проверить большие объемы информации. Технология способна обработать массивы данных, которые человек не в состоянии проработать за короткий период времени, что обеспечивает возможность оперативного выявления угроз и принятия мер по их предотвращению.

Автоматизация процессов обнаружения и реагирования на кибератаки является еще одним преимуществом использования искусственного интеллекта. Искусственный интеллект способен проводить постоянный мониторинг сети и выявлять нетипичное поведение, что может свидетельствовать о возможной кибератаке. Кроме того, ИИ самостоятельно реагирует на угрозы, препятствуя несанкционированному доступу хакеров и предотвращая утечку данных. Одним из ключевых аспектов применения искусственного интеллекта в области кибербезопасности является его способность обучаться на предыдущих атаках для улучшения своих алгоритмов и более точного выявления угроз в будущем.

Разработка средств защиты информации с применением искусственного интеллекта представляет собой эффективный способ улучшить обнаружение и реагирование на угрозы информационной безопасности. Вот несколько рекомендаций по разработке средств защиты:

1. Используйте технологии машинного обучения для анализа больших объемов данных и обнаружения аномалий в поведении системы или пользователя, что поможет выявить потенциальные угрозы.

2. Создайте систему мониторинга, которая автоматически анализирует события на сети и в системах на предмет потенциальных атак или нарушений безопасности.

3. Используйте системы обнаружения вторжений (IDS), которые используют алгоритмы машинного обучения для выявления необычного поведения в сети или системе.

4. Разработайте средства автоматического реагирования на инциденты безопасности, чтобы быстро реагировать на угрозы и минимизировать ущерб.

5. Нейронные сети могут помочь в обнаружении угроз и паттернов в поведении хакеров, что позволит улучшить процессы безопасности, поэтому их необходимо применять на практике

6. Важно регулярно обновлять модели ИИ для адаптации к новым угрозам и изменениям в окружающей среде.

7. Обеспечьте обучение сотрудников по использованию и пониманию систем защиты информации на основе искусственного интеллекта.

При разработке средств защиты информации с применением искусственного интеллекта следует руководствоваться определенными принципами. Основные принципы разработки СЗИ с применением ИИ:

- принцип обеспечения безопасности по умолчанию;
- принцип многоуровневой защити;
- принцип непрерывного мониторинга и обновления;
- принцип контроля доступа и привилегий;
- принцип принятия решений на основе данных;
- принцип автоматизации процессов;
- принцип аудита и мониторинга;
- принцип постоянного обучения и обновления моделей.

Соблюдение этих принципов поможет разработать эффективные средства защиты информации на основе искусственного интеллекта, способные обнаруживать, предотвращать и реагировать на угрозы информационной безопасности с большей эффективностью и точностью.

Стоит отменить существенный недостаток, который заключается в том, что злоумышленники также имеют доступ к машинному обучению и искусственному интеллекту. Здесь можно в пример привести целый раздел ML Adversarial machine learning (AML). Переводя буквально - Вредоносное машинное обучение — это целенаправленное воздействие на искусственный интеллект, призванное вызвать ошибки в её поведении, и имеет 3 основные стратегии. Вкратце рассмотрим каждую:

1. Отравление данных (Data Poisoning) — создание предпосылок для ошибки на этапе обучения.

2. Атака уклонения (Evasion Attack) — создание предпосылок для ошибки на этапе применения нейросети.

3. Кража модели (Model Extraction) — определение на каких данных обучалась модель или извлечение обучающих данных из обученной модели.

Здесь мы рассмотрели, когда сами злоумышленники используют в своих целях искусственный интеллект, но и сами технологии ИИ могут создать сложности в применении. Системы на базе ИИ могут генерировать ложные срабатывания. Это происходит, когда системы ошибочно определяют законную деятельность как угрозу, что может вызвать сбои в функционировании ИТ-сети организации. Также стоит отметить высокую сложность алгоритмов искусственного интеллекта из-за чего затрудняется их понимание специалистами по безопасности и это приводит к отсутствию прозрачности и вызывает опасения по поводу доверия и подотчетности. Одним из главных минусов можно отнести обновление этих самых алгоритмов. Регулярные обновления необходимы для адаптации к появляющимся киберугрозам, однако они также могут привести к новым уязвимостям. Постоянная гонка между защитой и атакой требует высо-

кой степени внимания к безопасности обновлений, чтобы предотвратить возможные слабые места в системе [3].

В заключение можно сказать, что даже с потенциальными недостатками ИИ будет способствовать развитию кибербезопасности и поможет организациям создать более надежную систему безопасности, также стоит учесть, что ИИ в кибербезопасности — это сложный процесс, требующий непрерывного обучения, адаптации и вложений. С учетом современных вызовов и инновационных технологий, применение ИИ становится неотъемлемым элементом современной стратегии кибербезопасности. Использование ИИ в средствах защиты информации может значительно повысить эффективность обнаружения и предотвращения угроз информационной безопасности. Однако важно создавать комплексные системы, учитывающие различные аспекты безопасности и регулярно обновлять их для борьбы с постоянно изменяющимися угрозами.

Список источников

1. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» [Электронный ресурс] – URL: https://files.stroyinf.ru/Data1/52/52303/ (Дата обращения: 17.02.2024).
2. Искусственный интеллект: технологии и применение [Электронный ресурс] – URL: https://rdc.grfc.ru/2020/12/aitech/ (Дата обращения: 17.02.2024).
3. RuSIEM: Как искусственный интеллект в SIEM-системах может остановить киберпреступников [Электронный ресурс] – URL: https://safe.cnews.ru/articles/2019-09-04_kak_iskusstvennyj_intellekt_v_siemsistemah (Дата обращения: 17.02.2024).
4. Термины и определения в области информационной безопасности [Электронный ресурс] – URL: https://www.securityvision.ru/blog/terminy%20-i-opredeleniya-v-oblasti-informatsionnoy-bezopasnosti/ (Дата обращения: 17.02.2024).
5. Применение технологий искусственного интеллекта в информационной безопасности [Электронный ресурс] – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security (Дата обращения: 17.02.2024).
6. Роль искусственного интеллекта в кибербезопасности [Электронный ресурс] – URL: https://vc.ru/dev/621020-rol-iskusstvennogo-intellekta-v-kiberbezopasnosti (Дата обращения: 17.02.2024).
7. Перспективы развития искусственного интеллекта и машинного обучения в корпорации Майкрософт [Электронный ресурс] – URL: https://learn.microsoft.com/ru-ru/security/engineering/securing-artificial-intelligence-machine-learning (Дата обращения: 17.02.2024).

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Шапенская А. М. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вороненко В. В. – студент СПО, направление подготовки 09.02.01 – Компьютерные системы и комплексы, Брянский филиал ФГБОУ ВО «РЭУ им. Г. В. Плеханова».

Логвинов Д. В. – студент кафедры «Информатика и программное обеспечение», направление подготовки 09.04.04 – «Программная инженерия, ФГБОУ ВО «БГТУ».

Вклад авторов

Шапенская А. М. – обработка материала, написание статьи, научное редактирование текста (25 %).

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

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

Логвинов Д. В. – обработка материала, написание статьи, научное редактирование текста (25 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.8

Менеджмент событий информационной безопасности в условиях современного общества

Алина Михайловна Шапенская[1]✉, Кирилл Андреевич Седаков[2]
[1, 2] Брянский государственный технический университет, Брянск, Россия
[1] alinashapenskaya2002@gmail.com✉, https://orcid.org/0009-0007-8434-5848
[2] sekira98@mail.ru, https://orcid.org/0009-0002-9284-4624

Аннотация. В данной статье рассматриваются информационные риски, а также проблемы современного менеджмента безопасности информации.

Ключевые слова: риски, менеджмент, информационная безопасность, системное управление, защита информации.

Для цитирования: Шапенская А. М., Седаков К. А. Менеджмент событий информационной безопасности в условиях современного общества // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 291–293.

Управление рисками информационной безопасности — это процесс определения, оценки и управления потенциальными угрозами для информационных систем организации. Существует два вида рисков:

- внутренние информационные риски, которые связаны с недостатком контроля и ограничений внутри организации;
- внешние информационные риски, которые происходят извне и могут включать в себя кибератаки и другие угрозы [1].

Процесс управления информационными рисками включает в себя следующие этапы:

Этап 1. Идентификация рисков: на этом этапе вы определяются и классифицируются потенциальные риски информационной безопасности, которые могут повлиять на ваше предприятие.

Этап 2. Оценка рисков: здесь проводится анализ вероятности возникновения рисков и их потенциального воздействия на организацию. Это поможет определить, какие риски требуют преоритизации для последующего управления.

Этап 3. Управление рисками: после определения и оценки рисков необходимо разработать стратегии по их управлению, что может включать в себя принятие мер по снижению рисков, передаче рисков сторонним организациям (например, страховые компании), избеганию рисков или их принятию.

Этап 4. Мониторинг и анализ: после внедрения стратегий управления рисками необходимо постоянно мониторить ситуацию и проводить анализ эффективности принятых мер. В случае необходимости корректировать стратегии управления рисками.

Этап 5. Обучение и обучение персонала: изучение новых угроз и методов защиты является важным компонентом управления рисками информационной безопасности. Сотрудники должны быть информированы о принятых политиках и процедурах по безопасности информации.

Хорошо спланированное управление рисками информационной безопасности помогает организации избежать угроз, связанных с нарушениями безопасности данных, и обеспечить целостность, конфиденциальность и доступность информации.

Основными преимуществами грамотной реализации управления информационными рисками можно отнести:

– улучшение безопасности информации так как системное управление помогает в обеспечении надежной защиты информационных ресурсов организации;

– снижения количества потерь от информационных рисков позволяет минимизировать возможные убытки и последствия, связанные с возможными угрозами.

– создается уверенность у клиентов, партнеров и других заинтересованных сторон в надежности и безопасности информационных процессов [2].

К сожалению, менеджмент событий информационной безопасности наполнен проблемами, которые в свою очередь требуют огромное количество внимания. Проблемы, с которыми сталкиваются организации в области менеджмента информационной безопасности, могут быть разнообразными. Некоторые из основных проблем в этой области включают в себя:

– недостаточное финансирование;

– недостаток осведомленности и обучения персонала;

– несоответствие нормативным требованиям и стандартам;

– внутренний нарушитель;

– увеличение количества используемых устройств и информационных технологий.

Решение этих проблем требует комплексного подхода, включающего в себя обучение персонала, выделение достаточных ресурсов, соблюдение стандартов безопасности, регулярное обновление систем безопасности и постоянное мониторинг угроз и рисков [3].

Таким образом, менеджмент событий информационной безопасности является основой обеспечения безопасности информационных систем внутри любого предприятия или организации. Внедрение новых технологий и методов управления рисками, а также улучшение понимания человеческого фактора в информационной безопасности является важнейшей перспективой развития системного управления рисками информационной безопасности.

Список источников

1. Управление рисками информационной безопасности: [Электронный ресурс] – Режим доступа: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-konspekt-lektsii/ (Дата обращения: 17.03.2024).

2. Система управления рисками в компании: [Электронный ресурс] – Режим доступа: https://projecto.pro/blog/theory/sistema-upravleniya-riskami-v-kompanii/ (Дата обращения: 16.03.2024).

3. Основы построения системы управления рисками ИБ: [Электронный ресурс] – Режим доступа: https://lib.itsec.ru/articles2/control/osnovy-postroeniya-sistemy-upravleniya-riskami-ib (Дата обращения: 18.03.2024).

Статья поступила в редакцию 24.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Шапенская А. М. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «БГТУ».

Седаков К. А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Шапенская А. М. – идея, сбор материала, обработка материала, частичное написание статьи (50 %).

Седаков К. А. – написание статьи, научное редактирование текста (50 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.53

Анализ систем обнаружения и предотвращения вредоносной активности в среде выполнения контейнеров приложений

Илья Сергеевич Шишкин[1]✉, Денис Александрович Вислобоков[2]
[1, 2] Тамбовский государственный технический университет, Тамбов, Россия
[1] ilya.shishkin.14@bk.ru✉, https://orcid.org/0009-0004-6413-8364
[2] denis.vislobokov@mail.ru, https://orcid.org/0009-0006-6986-4132

Аннотация. В данной статье проведен сравнительный анализ программного обеспечения (ПО) в категории систем обнаружения и предотвращения вредоносной активности в среде выполнения контейнеров приложений. Результаты анализа позволяют оценить функционал и разнообразие доступных решений и выбрать наиболее подходящее для конкретных потребностей организации.

Ключевые слова: слова: информационная безопасность, кибербезопасность, системы обнаружения и предотвращения вредоносной активности, SIEM, контейнеры приложений, открытое программное обеспечение.

Для цитирования: Шишкин И. С., Вислобоков Д. А. Анализ систем обнаружения и предотвращения вредоносной активности в среде выполнения контейнеров приложений // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 294–300.

Введение

В современном мире контейнеризация приложений набирает все большую популярность. Этот метод позволяет изолировать приложения друг от друга и от операционной системы, что повышает безопасность и масштабируемость. Однако контейнеры также не лишены своих уязвимостей, которые могут быть использованы злоумышленниками для нанесения вреда. В этих условиях обеспечение безопасности информационных ресурсов становится критической задачей для организаций любого масштаба. Одним из действенных методов защиты является использование систем управления информацией и событиями безопасности (SIEM). SIEM-решения позволяют организациям централизованно собирать и анализировать данные безопасности из различных источников, таких как журналы приложений, сетевые устройства, системы безопасности хостов и контейнеры приложений. Эти данные используются для выявления потенциальных угроз, таких как Privilege Escalation и Escape to Host.

Цель исследования заключается в проведении обзора существующих решений с открытым исходным кодом в области SIEM с целью выявления их особенностей, преимуществ и ограничений. Актуальность данного исследова-

ния обусловлена необходимостью повышения уровня безопасности контейнеров приложений в связи с их популярностью использования.

Системы управления информацией и событиями безопасности

Система управления информацией и событиями безопасности (SIEM) — это программное решение, предназначенное для централизованного сбора, агрегирования, анализа и корреляции данных безопасности из различных источников, таких как журналы приложений, сетевые устройства, системы безопасности хостов, облачные сервисы и другие (табл. 1).

Таблица 1

Основные функции SIEM и их описание

Функция	Описание
Сбор данных	Собирает данные безопасности из различных источников, таких как журналы приложений, сетевые устройства, системы безопасности хостов, облачные сервисы и другие.
Анализ данных	Анализирует данные безопасности с помощью различных методов, таких как статистический анализ, машинное обучение и искусственный интеллект, для выявления потенциальных угроз, аномалий и подозрительной активности.
Корреляция событий	Коррелирует события из разных источников, чтобы получить более полное представление о происходящем в ИТ-инфраструктуре.
Генерация оповещений	Генерирует оповещения о потенциальных угрозах, аномалиях и подозрительной активности, позволяя сотрудникам службы безопасности быстро реагировать на инциденты.
Активное реагирование	Автоматически или вручную реагирует на обнаруженные угрозы, например, блокирует IP-адреса, изолирует системы или запускает антивирусное сканирование.
Расследование инцидентов	Помогает расследовать инциденты, предоставляя информацию о том, когда, где и как произошла атака.
Соответствие требованиям	Помогает организациям соответствовать нормативным требованиям в области кибербезопасности.

SIEM представляет собой мощный инструмент для управления кибербезопасностью, обладающий рядом ключевых преимуществ. Во-первых, он значительно сокращает время реагирования на кибератаки, обеспечивая более быстрое обнаружение инцидентов и минимизируя возможный ущерб. Во-вторых, SIEM повышает эффективность расследования инцидентов, предоставляя всю необходимую информацию для точного анализа и последующих действий.

SIEM способствует соответствию требованиям нормативов в области кибербезопасности, таких как PCI DSS и SOX, обеспечивая необходимую отчетность и контроль. Наконец, применение SIEM может снизить расходы на кибербезопасность за счет повышения ее эффективности и оптимизации процессов. Необходимо также отметить, что связь безопасности контейнеров с SIEM становится все более важной в контексте современной разработки приложений, поскольку контейнеры представляют собой новый вектор угроз и должны быть включены в систему мониторинга и аналитики безопасности.

Исследование, проведенное TAdviser и Positive Technologies, свидетельствует о постоянном росте рынка SIEM и увеличении количества продуктов. Существует множество решений на рынке, как коммерческих, так и открытых. Коммерческие продукты, такие как QRadar, ArcSight и Splunk, нередко являются популярными выборами благодаря своей мощности и функциональности. Среди отечественных продуктов можно выделить MaxPatrol SIEM, KUMA и RuSIEM. Они предлагают свои уникальные подходы к обеспечению безопасности информации и инфраструктуры, учитывая особенности и требования российских компаний и организаций. Есть место и для open source решений, которые могут стать значимым вкладом в область кибербезопасности, предоставляя доступ к современным инструментам и технологиям без огромных затрат [1].

Интеграция безопасности контейнеров с SIEM становится все более важной в контексте современной разработки приложений. Контейнеры представляют собой новый вектор угроз, и их безопасность должна быть включена в систему мониторинга и аналитики безопасности. Это позволяет обнаруживать и реагировать на угрозы, связанные с контейнерами, и минимизировать риски для инфраструктуры. В этом контексте открытые решения, такие как Wazuh и Suricata, представляют собой доступные альтернативы, обеспечивая пользователям возможность использовать современные технологии безопасности без значительных финансовых затрат.

Сравнительный анализ систем управления информацией и событиями безопасности

При принятии решения о выборе подходящей системы управления информационной безопасностью (SIEM), необходимо учитывать разнообразие доступных решений на рынке. Многие из них представлены как коммерческие продукты, интегрированные в системы безопасности от одного производителя. Эти решения обычно обладают обширным функционалом, ориентированным на различные сетевые сценарии, а также гарантируют постоянную поддержку и обновления.

Однако открытые решения, разработанные на базе открытого исходного кода, представляют собой привлекательную альтернативу. Они обеспечивают большую гибкость и прозрачность, позволяя организациям настраивать систему в соответствии с их конкретными потребностями безопасности.

Анализ различных открытых SIEM, таких как Wazuh и Suricata, направлен на выявление их особенностей, архитектуры, поддерживаемых протоколов и сервисов, а также возможностей интеграции. Это позволяет осознанно выбирать между различными решениями, учитывая их преимущества и ограничения, и обеспечивает обоснованное принятие решения при выборе SIEM-системы, основанной на открытом исходном коде.

В качестве анализируемых представлены следующие системы: Wazuh, Suricata, QRadar и ArcSight.

Wazuh — это бесплатная платформа безопасности с открытым исходным кодом, объединяющая возможности XDR и SIEM. Она защищает рабочие на-

грузки в локальных, виртуализированных, контейнерных и облачных средах. Wazuh помогает организациям и частным лицам защищать свои информационные активы от угроз безопасности. Его широко используют тысячи организаций по всему миру, от малых предприятий до крупных корпораций [2].

Suricata — это высокопроизводительный сетевой IDS, IPS и механизм мониторинга сетевой безопасности. Он имеет открытый исходный код и принадлежит некоммерческому фонду Open Information Security Foundation (OISF), управляемому сообществом [3].

QRadar — это модернизированное решение для обнаружения угроз и реагирования на них, призванное унифицировать работу аналитиков по безопасности и ускорить их работу на протяжении всего жизненного цикла инцидента. В портфель встроены искусственный интеллект и автоматизация корпоративного уровня, которые значительно повышают производительность аналитиков, помогая ограниченным в ресурсах командам безопасности более эффективно работать с основными технологиями. Он предлагает интегрированные продукты для защиты конечных точек (EDR, XDR, MDR), управления логами, SIEM и SOAR - все с общим пользовательским интерфейсом, общими знаниями и взаимосвязанными рабочими процессами. [4].

ArcSight — это мощный, адаптируемый SIEM, предлагающий комплексный сбор данных и анализ угроз в режиме реального времени, а также встроенный канал анализа угроз и встроенный SOAR. Опираясь на лучший в отрасли механизм корреляции, ArcSight ESM предупреждает аналитиков о связанных с угрозами событиях по мере их возникновения, значительно сокращая время на обнаружение, реагирование и устранение угроз кибербезопасности [5].

Далее требуется определить критерии сравнения рассматриваемых систем. Основными параметрами, определяющими функциональность подобных решений, являются:

- поддерживаемые операционные системы (ОС);
- поддерживаемые системы виртуализации;
- поддерживаемые облачные сервисы;
- мониторинг контейнеров;
- безагентность;
- интеграция с DevOps инструментами;
- анализ Big Data;
- интеграция с системами сбора логов;
- коммерческий продукт или Open Source;
- обнаружение угроз;
- анализ сетевого трафика;
- система обнаружения вторжений;
- управление и реагирование на инциденты;
- мониторинг уязвимостей;
- анализ пользовательской активности;
- корреляция событий.

Результаты сравнения представлены в табл. 2.

Таблица 2

Сравнение систем управления информацией и событиями безопасности

Критерий	Wazuh	Suricata	QRadar	ArcSight
Поддерживаемые ОС	Linux, Windows, macOS	Linux, Windows, FreeBSD	Linux, Windows, AIX	Linux, Windows, HP-UX
Поддерживаемые системы виртуализации	VMware, Hyper-V, Docker	VMware, KVM	VMware vSphere, Microsoft Hyper-V	VMware, Docker, Kubernetes
Поддерживаемые облачные сервисы	AWS, Azure, Google Cloud Platform	AWS, Azure, Google Cloud Platform	AWS, Azure, IBM Cloud	AWS, Azure, Google Cloud Platform
Мониторинг контейнеров	Да	Да	Да	Да
Безагентность	Нет (требуется агент на целевых хостах)	Нет (требуется сенсор или агент)	Есть (возможен безагентный сбор)	Есть (возможен безагентный сбор)
Интеграция с DevOps инструментами	Ansible, Puppet, Chef	–	Ansible, Terraform	Ansible, Puppet, Chef
Анализ Big Data	Да (поддержка анализа больших объемов данных)	Да (поддержка анализа сетевого трафика)	Да (анализ больших объемов событий)	Да (анализ больших объемов данных)
Интеграция с системами сбора логов	Elasticsearch, Logstash, Filebeat, Fluentd, Beats, Syslog	Fluentd, Logstash, Filebeat, Syslog	Splunk, Logstash, QRadar Log Event Extended (LEEF)	Splunk, Logstash, Elasticsearch, QRadar Log Event Extended (LEEF), syslog-ng
Коммерческий продукт или Open Source	Open Source	Open Source	Коммерческий продукт	Коммерческий продукт
Обнаружение угроз	Да	Да	Да	Да
Анализ сетевого трафика	Да	Да	Да	Да
Система обнаружения вторжений	Да	Да	Да	Да
Управление и реагирование на инциденты	Да	Нет	Да	Да
Мониторинг уязвимостей	Да	Да	Да	Да

Окончание табл. 2

Критерий	Wazuh	Suricata	QRadar	ArcSight
Анализ пользовательской активности	Да	Нет	Да	Да
Корреляция событий	Да	Да	Да	Да

Результаты сравнения показывают, что среди открытых решений в области SIEM существуют достаточно развитые платформы, которые обладают гибкостью для настройки под конкретные потребности пользователей. В частности, выделяется система Wazuh благодаря ее совместимости с различными операционными системами и облачными сервисами, а также разнообразием интеграционных возможностей.

Кроме того, система Suricata также заслуживает внимания за свои возможности анализа сетевого трафика и открытый исходный код, что обеспечивает прозрачность и гибкость в настройке.

Таким образом, как наиболее устоявшееся решение можно выделить Wazuh, благодаря его широкому функционалу, поддержке сообщества и возможности доработки под конкретные условия использования.

Заключение

Обзор существующих открытых решений в области SIEM свидетельствует о широком распространении данного направления в кибербезопасности и его активном развитии. Внедрение SIEM-технологий представляет собой важный шаг в обеспечении безопасности информационных систем, создавая дополнительные уровни защиты и повышая вероятность обнаружения потенциальных угроз.

Анализ рассмотренных решений выявил их разнообразие и функциональные возможности, предоставляя пользователям широкий спектр выбора в зависимости от потребностей и особенностей их инфраструктуры. Например, система Wazuh проявляет себя как одно из наиболее привлекательных решений благодаря своей совместимости с различными операционными системами и облачными сервисами.

Следует также отметить, что ряд рассмотренных систем продолжает активное развитие, сопровождаемое расширением функционала и улучшением совместимости с другими системами безопасности. Для достижения дальнейшего совершенствования SIEM-систем необходимо проведение дальнейших исследований в этой области, учитывая постоянное изменение угроз и требований кибербезопасности. Это позволит разработчикам и пользователям успешно

бороться с современными киберугрозами и эффективно защищать информационные ресурсы.

Список источников

1. Исследование TAdviser и Positive Technologies: Рынок SIEM в России. URL: https://www.ptsecurity.com/ru-ru/research/analytics/siem-market-in-of-russia/#id3.
2. Wazuh - Getting started with Wazuh. URL: https://documentation.wazuh.com/current/getting-started/index.html.
3. Suricata - What is Suricata. URL: https://docs.suricata.io/en/latest/what-is-suricata.html.
4. IBM Security QRadar SIEM. URL: https://www.ibm.com/qradar.
5. OpenText ArcSight Enterprise Security Manager. URL: https://www.opentext.com/products/arcsight-enterprise-security-manager.

Статья поступила в редакцию 23.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Шишкин И. С. – студент кафедры «Информационные системы и защита информации», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «ТГТУ».

Вислобоков Д. А. – студент кафедры «Информационные системы и защита информации», специальность 10.05.03 – Информационная безопасность автоматизированных систем, ФГБОУ ВО «ТГТУ».

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004.056.52

Методы защиты акустической речевой информации от утечек за счет акустоэлектрических преобразований

Николай Юрьевич Шпаковский[1]✉, Александр Александрович Гусев[2], Роман Михайлович Башкиров[3]
[1, 2, 3] Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный), Тамбов, Россия
[1, 2, 3] nauchnajarota@yandex.ru✉, https://orcid.org/0009-0007-5540-2719

Аннотация. При выполнении мер по технической защите конфиденциальной информации в организациях принимаются в том числе меры по защите акустической речевой информации в защищаемых помещениях. Однако в данных помещениях также могут присутствовать вспомогательные технические системы и средства, которые могут передавать информацию за счет акустоэлектрических преобразований.

В данной статье рассматривается принцип перехвата речевой информации за счет акустоэлектрических преобразований, а также некоторые методы по ее защите.

Ключевые слова: защита информации, речевая информация, акустоэлектрические преобразования.

Для цитирования: Шпаковский Н. Ю., Гусев А. А., Башкиров Р. М. Методы защиты акустической речевой информации от утечек за счет акустоэлектрических преобразований // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 301–304.

При ведении конфиденциальных переговоров в защищаемых помещениях большое внимание уделяется защите речевой информации. Именно защита речевой информации является одной из важных проблем технической защиты конфиденциальной информации.

На данный момент ФСТЭК России была разработана методика оценки эффективности защиты акустической речевой конфиденциальной информации, где предусматривается защита от намеренного или ненамеренного прослушивания и перехвата информации в воздушной среде или за счет виброакустического преобразования. Однако защита речевой конфиденциальной информации за счет акустоэлектрических преобразований не предусмотрена (имеется такая методика только для защиты информации, составляющих государственную тайну, но не для защиты конфиденциальной информации).

Акустоэлектрическим преобразованием называют преобразование акустического сигнала в электрический. Некоторые элементы вспомогательных технических систем и средств (ВТСС), в том числе трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов и т. п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), либо к модуляции токов, протекающих по этим элементам в соответствии с изменениями воздействующего акустического поля.

ВТСС, кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект акустоэлектрического преобразования в специальной литературе называют «микрофонным эффектом». Причем из ВТСС, обладающих «микрофонным эффектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации.

В связи с этим для получения или перехвата речевой информации за счет акустоэлектрических преобразований злоумышленник может использовать следующие способы:

- гальванический съем акустической информации, то есть путём контактного подключения подслушивающих устройств в любом месте проводной сети передачи речевой информации. Пример такого перехвата представлен на рис. 1.

Рис. 1. Схема утечки акустической информации за счет подслушивающих устройств

- путём высокочастотного навязывания сигнала, то есть по линии подается высокочастотный тональный сигнал, который воздействует на нелинейные элементы ВТСС (диоды, транзисторы, микросхемы) на которые также воздействует акустический сигнал. В результате в такой линии формируется высоко-

частотный модулированный сигнал. Схема формирования данного канала утечки приведена на рис. 2.

Рис. 2. Схема утечки акустической информации с помощью ВЧ-навязывания

- индуктивный способ негласного съёма информации, то есть за счёт электромагнитной индукции, возникающей в процессе переговоров вдоль провода линии подключения ВТСС. В качестве приемного устройства съёма информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии.

- емкостной способ негласного съема информации, то есть съем информации за счет формирования на обкладках конденсатора электростатического поля, изменяющегося в соответствии с изменением уровня переговоров. В качестве приёмника съёма телефонных переговоров используется ёмкостной датчик, выполненный в виде двух пластин, плотно прилегающих к проводам линии подключения ВТСС.

Исходя из данных методов добывания и перехвата информации можно реализовать различные организационно-технические мероприятия, направленные на исключение или существенное затруднение ее добывания. К ним можно отнести:

- проведение специальных исследований ВТСС, находящихся в защищаемом помещении;

- генераторы шума, зашумляющие линии, выходящие за пределы контролируемой зоны во время проведения переговоров;

- установка ограничителей сигналов малой амплитуды и размыкателей цепи;

- установка трансформаторной развязки внутри контролируемой зоны и подключение к ней ВТСС.

Таким образом можно заключить, что защита речевой конфиденциальной информации за счет акустоэлектрических преобразований возможна путем реализации вышеперечисленных мер.

Список источников

1. Остапенко Н. А., Яресько А. П. Защита информации от утечек по каналу акустоэлектрических преобразований, 2017 г.
2. Хорев А. А. Защита информации от утечек по техническим каналам
3. ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, влияющие на информацию. Общие положения.
4. Сапожков М. А. Электроакустика.

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Шпаковский Н. Ю. – старший оператор роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Гусев А. А. – младший научный сотрудник роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Башкиров Р. М. – младший научный сотрудник роты (научной), Межвидовой центр подготовки и боевого применения войск РЭБ (учебный и испытательный).

Вклад авторов

Шпаковский Н. Ю. – идея, сбор материала, обработка материала, написание статьи (60 %).

Гусев А. А. – научное редактирование текста, подбор литературных источников (20 %).

Башкиров Р. М. – научное редактирование текста, подбор литературных источников (20 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Порядок оценки заинтересованности нарушителя в нарушении свойств информационной безопасности конфиденциальной информации

Марат Рафаилович Юмакаев[1]✉, Екатерина Владимировна Кондрашова[2], Максим Михайлович Голембиовский[3], Кирилл Евгеньевич Шинаков[4]
[1, 2, 3, 4] Брянский государственный технический университет, Брянск, Россия
[1] bryansk-tu@yandex.ru✉
[2] kondrashova_katerina@bk.ru
[3] maksim32region@yandex.ru
[4] shinakov@it-craft.net, https://orcid.org/0000-0003-2000-7528

Аннотация. Оценка заинтересованности нарушителя является важным инструментом для обеспечения безопасности конфиденциальной информации и предотвращения возможных инцидентов безопасности. При этом необходимо постоянно совершенствовать методы обнаружения и предотвращения угроз, чтобы минимизировать риски для информационных систем и сохранности данных.

Ключевые слова: информационная безопасность, оценка заинтересованности нарушителя, конфиденциальная информация.

Для цитирования: Юмакаев М. Р., Кондрашова Е. В., Голембиовский М. М., Шинаков К. Е. Порядок оценки заинтересованности нарушителя в нарушении свойств информационной безопасности конфиденциальной информации // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 305–307.

Количество киберугроз, как и ущерб от хакерских атак, растет с каждым годом. По экспертным оценкам, потери от киберпреступлений достигнут $10,5 трлн в 2025 году [1].

Значительное влияние на вероятность наступления ущерба для объекта оказывает заинтересованность нарушителя в реализации противоправных действий относительно защищаемого объекта. Высокая заинтересованность нарушителя

Для определения заинтересованности нарушителя предлагается анкета с набором факторов для каждого вида конфиденциальной информации (таблица 1). Для объекта, обрабатывающего каждый из видов конфиденциальной информации предложен перечень факторов, оказывающих влияние на заинтересованность нарушителя. Если на объекте присутствует менее 50 % факторов — заинтересованность нарушителя низкая, если на объекте присутствует 50 %

факторов — заинтересованность нарушителя средняя, если на объекте присутствует более 50 % факторов — заинтересованность нарушителя высокая. Список факторов может корректироваться в зависимости от специфики объекта.

Таблица 1

Оценка заинтересованности нарушителя в нарушении свойств информационной безопасности конфиденциальной информации

Фактор	Наличие фактора (Да / Нет)
Персональные данные	
Число субъектов, чьи ПДн обрабатываются на объекте превышает 100	
В число субъектов, чьи ПДн обрабатываются на объекте входят известные личности (политики, бизнесмены, актеры и тд.)	
На объекте часто происходят конфликтные ситуации между руководством и работниками	
На рынке большое количество (более трех на населенный пункт) крупных предприятий-конкурентов со схожим видом деятельности	
Профессиональная тайна	
На объекте выполняются крупные заказы по профилю деятельности (например, громкие адвокатские дела, массовые медосмотры)	
Объект относится к КИИ	
На объекте часто происходят конфликтные ситуации между руководством и работниками	
На рынке большое количество (более трех на населенный пункт) крупных предприятий-конкурентов со схожим видом деятельности	
Коммерческая тайна	
Наличие режима коммерческой тайны значительно влияет на доход организации (после внедрения существенно выросли экономические показатели)	
На объекте выполняются крупные заказы по профилю деятельности	
На объекте часто происходят конфликтные ситуации между руководством и работниками	
На рынке большое количество (более трех на населенный пункт) крупных предприятий-конкурентов со схожим видом деятельности	
Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них	
Регистрация разработанного изобретения, полезной модели или промышленного образца потенциально принесет большой доход (более 30% от чистого годового дохода)	
Разработанное изобретение, полезная модель или промышленный образец может быть востребован и полезен большому количеству предприятий-производителей	
На объекте часто происходят конфликтные ситуации между руководством и работниками	
На рынке большое количество (более трех на населенный пункт) крупных предприятий-конкурентов со схожим видом деятельности	

Таким образом, представленная анкета оценки факторов позволяет оценить, насколько гипотетический нарушитель заинтересован в причинении ущерба объекту. Показатель важен для определения, поскольку даже при высоком уровне защищенности объекта, высокозаинтересованный нарушитель может найти способ воздействия на свойства информационной безопасности конфиденциальной информации и причинить ущерб.

Нивелировать представленные в таблице факторы не проставляется возможным, однако косвенно можно повлиять на фактор конфликтных ситуаций, если данный фактор отмечен как присутствующий, рекомендуется внедрить в организации корпоративную и мотивационную политику, в которых точно будут прописаны обязанности сотрудников и меры их поощрения. С течением времени фактор снизит свое влияние, что напрямую скажется на вероятности нарушения свойств информационной безопасности конфиденциальной информации.

Список источников

1. Интернет несет потери [Электронный ресурс] – Режим доступа: https://www.vedomosti.ru/importsubstitution/new_technologies/articles/2023/03/14/966290-internet-neset-poteri (Дата обращения: 02.03.2024).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Юмакаев М. Р. – выпускник кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Кондрашова Е. В. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

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

Шинаков К. Е. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Юмакаев М. Р. – обработка материала, написание статьи (50 %).

Кондрашова Е. В. – сбор материала, частичное написание статьи (17 %).

Голембиовский М. М. – сбор материала, частичное написание статьи (17 %).

Шинаков К. Е. – идея, научное редактирование (16 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 004: 056

Оценка профессиональной подготовки работников, обеспечивающих информационную безопасность на объекте

Марат Рафаилович Юмакаев[1]✉, Станислав Владимирович Сафоненко[2], Оксана Михайловна Голембиовская[3]
[1, 2, 3] Брянский государственный технический университет, Брянск, Россия
[1, 2] bryansk-tu@yandex.ru✉
[3] Bryansk-tu@yandex.ru, https://orcid.org/0000-0002-6433-3133

Аннотация. Оценка профессиональной подготовки работников, обеспечивающих информационную безопасность на объекте, является ключевым элементом обеспечения безопасности информации в современном мире. Работники, занимающиеся информационной безопасностью, должны обладать не только необходимыми знаниями и навыками, но и быть готовыми реагировать на возникающие угрозы и атаки.

Ключевые слова: информационная безопасность, профессиональная подготовка сотрудников, анкета общей подготовки сотрудников.

Для цитирования: Юмакаев М. Р., Сафоненко С. В., Голембиовская О. М. Оценка профессиональной подготовки работников, обеспечивающих информационную безопасность на объекте // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 308–315.

Оценка профессиональной подготовки работников, занимающихся обеспечением информационной безопасности на объекте, играет ключевую роль в обеспечении эффективной защиты информационных ресурсов организации. Компетентные специалисты в этой области способны своевременно выявлять угрозы безопасности, принимать меры по их предотвращению и минимизации возможных рисков. Важно также учитывать актуальность и достоверность знаний сотрудников в сфере информационной безопасности, уровень осведомленности о последних трендах и угрозах в области кибербезопасности.

Уровень знаний специалистов по информационной безопасности следует контролировать как при приеме на работу, так и в ходе осуществления деятельности, добавляя оценочные средства в соответствии с новыми технологиями и требованиями.

Оценивать знания работников предлагается при помощи анкетирования (таблица 1). В анкету следует внести вопросы об углубленных знаниях в сфере ИБ, а также учесть требования Приказа Минтруда РФ № 525Н от 14 сентября

2022 года «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах», в рамках которого к специалисту по защите информации предъявляются требования, относительно знаний по информационной безопасности [0].

Таблица 1

Анкета по общей подготовке сотрудников, ответственных за информационную безопасность в компании, в сфере ИБ

Усл. Обознач.	**Вопрос / варианты ответов**	**Количество начисляемых баллов за ответ** *(раздел для проверяющего)*
V_1	Принцип Кирхгофа это:	
	секретность ключа определена секретностью открытого сообщения	0
	секретность информации определена скоростью передачи данных	0
	секретность закрытого сообщения определяется секретностью ключа	0.03125
V_2	Угроза информационной системе (компьютерной сети) – это:	
	вероятное событие	0.03125
	детерминированное событие	0
	событие, происходящее периодически	0
V_3	Наиболее важным при реализации защитных мер политики безопасности является:	
	аудит, анализ затрат на проведение защитных мер	0
	аудит, анализ безопасности	0
	аудит, анализ уязвимостей, риск-ситуаций	0.03125
V_4	К конфиденциальной информации не относится	
	коммерческая тайна	0
	персональные данные граждан	0
	"ноу-хау"	0.03125
V_5	Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает	
	Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"	0.03125
	ГК РФ	0
	Закон "Об информации, информатизации и защите информации"	0
	Конституция	0
V_6	В течении какого времени следует сообщить в Роскомнадзор о произошедшем инциденте в случае его выявления?	
	в течении 24 часов	0.03125
	в течении 48 часов	0
	в течении 72 часов	0
V_7	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять ру-	

Усл. Обознач.	**Вопрос / варианты ответов**	**Количество начисляемых баллов за ответ** *(раздел для проверяющего)*
	ководству?	
	снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования	0
	требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации	0
	улучшить контроль за безопасностью этой информации	0.03125
	снизить уровень классификации этой информации	0
V_8	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?	
	никогда, для обеспечения хорошей безопасности нужно учитывать и снижать все риски	0
	когда необходимые защитные меры слишком сложны	0
	когда стоимость контрмер превышает ценность актива и потенциальные потери	0.03125
V_9	Активный перехват информации это перехват, который:	
	заключается в установке подслушивающего устройства в аппаратуру средств обработки информации	0
	основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций	0
	осуществляется путем использования оптической техники	0
	осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера	0.03125
V_{10}	Какой из указанных приказов ФСТЭК России регламентирует требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации?	
	Приказ №21	0
	Приказ №31	0
	Приказ №239	0.03125
V_{11}	Сколько различных вариантов идентификации пользователей включает в себя ПО Secret Net Studio?	
	2	0
	3	0.03125
	4	0
V_{12}	Какое максимально возможное количество категорий конфиденциальности информации можно создать в ПО Secret Net Studio?	
	5	0
	11	0
	16	0.03125
V_{13}	Для чего предназначен контроллер домена только для чтения ?	
	для развертывания контроллера домена в местах, где невозможно гарантировать физическую безопасность	0.03125

Усл. Обознач.	**Вопрос / варианты ответов**	**Количество начисляемых баллов за ответ** *(раздел для проверяющего)*
	для развертывания контроллера домена в случае жесткого механизма разграничения доступа	0
	в случае если при помощи контроллеров необходимо восстановить полноценную работу службы каталогов.	0
V_{14}	Что такое лес в active directory?	
	глобальный каталог	0
	нейминг спецпроекта по поиску доменов	0
	коллекция одного или нескольких доменов	0.03125
V_{15}	Для чего предназначен протокол TCP?	
	для быстрой передачи порции данных без гарантии доставки и без предварительной установки соединения	0
	для доставки данных через соединение, предварительно установленное между двумя компьютерами	0.03125
V_{16}	Если при работе с песочницей файл прошел проверку средствами защиты первого рубежа (потоковые антивирусы на межсетевых экранах, антивирусные программы на рабочих станциях и т. д.), он может быть допущен к запуску непосредственно в системе?	
	Да	0
	Да, но не во всех случаях	0
	Нет	0.03125
V_{17}	Для чего нужен протокол S/MIME?	
	он обеспечивает конфиденциальность и целостность содержимого электронной почты путем шифрования сообщения и проверки личности отправителя	0.03125
	он защищает от подслушивания и несанкционированного доступа во время пересылки	0
	он добавляет цифровую подпись к исходящим сообщениям	0
V_{18}	В чем заключается атака типа отказ в обслуживании?	
	злоумышленники генерируют большое количество пакетов или запросов, которые в конечном счете перегружают работу целевой системы	0.03125
	злоумышленники исследуют внешний периметр и инициируют отключение питания критически важных для функционирования организации систем	0
V_{19}	Что такое инъекция?	
	Вид атаки, когда вредоносный код через внешний носитель передается конкретному устройству	0
	Вид атаки, когда ненадежные данные передаются интерпретатору кода через ввод формы или с помощью другого способа отправки информации в веб-приложение	0.03125
V_{20}	На чем основано действие антивирусной программы?	
	на ожидании начала вирусной атаки	0
	на сравнении программных кодов с известными вирусами	0.03125

Усл. Обознач.	**Вопрос / варианты ответов**	**Количество начисляемых баллов за ответ** *(раздел для проверяющего)*
	на удалении зараженных файлов	0
V_{21}	Что такое SOC?	
	центр по обеспечению информационной безопасности и мониторинга систем	0.03125
	приложение для мониторинга аномальной активности	0
	разновидность операционной системы	0
V_{22}	Что такое соленый хеш?	
	техника шифрования паролей	0.03125
	способ передачи данных	0
	алгоритм обеспечения защиты периметра	0
V_{23}	В чем разница серых и белых IP-адресов?	
	белые – внешние, серые –внутренние	0.03125
	белые – защищенные. серые – скомпрометированные	0
	белые – локальные, серые – глобальные	0
V_{24}	Чем отличается DHCP от DNS?	
	DNS-сервер сопоставляет доменные имена с IP-адресами, DHCP-сервер автоматически назначает IP-адреса хостам в сети при каждом подключении к сети	0.03125
	DNS-сервер автоматически назначает IP-адреса хостам в сети при каждом подключении к сети, DHCP-сервер сопоставляет доменные имена с IP-адресами	0
V_{25}	Что такое Kerberos?	
	ПО для проведения сканирования сетевых портов	0
	протокол передачи данных	0
	сетевой протокол аутентификации	0.03125
V_{26}	Что такое бестелесный вирус?	
	вирус, который вовремя обезврежен системой защиты и не оказал влияния на систему	0
	вирус, который не создаёт файлы и использует уже существующие системные ресурсы и вредоносные скрипты	0.03125
	вирус, который предназначен для массового распространения	0
V_{27}	Чем CSRF отличается от XSS?	
	в XSS веб-сайт принимает вирусный код, а в CSRF вирусный код хранится на сторонних веб-сайтах	0.03125
	в XSS вирусный код хранится на сторонних веб-сайтах, а в CSRF веб-сайт принимает вирусный код	0
V_{28}	Что такое watering hole?	
	утилита для тестирования систем	0.03125
	стратегия компьютерной атаки	0
	ПО для защиты информации	0
V_{29}	ля чего нужен NAT?	
	обеспечивает доступ локальных хостов к общедоступному Интернету и защищает их от прямого доступа извне	0.03125
	позволяет объединить несколько хостов в одну сеть с целью обеспечения обмена данными между ними	0

Усл. Обознач.	**Вопрос / варианты ответов**	**Количество начисляемых баллов за ответ** *(раздел для проверяющего)*
	обеспечивает стандартизированный механизм передачи сетевыми устройствами важной информации о подключении и состоянии сети	0
V_{30}	Для чего используется команда cd в linux?	
	для навигации между каталогами	0.03125
	для вывода содержимого файла	0
	для отображения полного пути до текущей рабочей директории	0
V_{31}	Что такое «Cyber Kill Chain» ?	
	Модель атаки на информационную инфраструктуру	0.03125
	Вредоносный троян, эксплуатация которого нанесла огромный ущерб предприятиям критической информационной инфраструктуры в 2018 году	0
V_{32}	Что такое APT-атака?	
	это атака, осуществляемая с применением ранее неизвестных технологий или уязвимостей	0
	это целевая продолжительная атака повышенной сложности	0.03125

Анкета может быть модернизирована в зависимости от специфики организации и обновляться для каждого последующего тестирования.

Показатели подготовки работников в области ИБ рассчитываются по следующей формуле (формула 1):

, (1)

где P — показатель общий подготовки работника в области ИБ, — оценка по каждому отдельному вопросу анкеты.

Результат интерпретируется с использованием шкалы Харрингтона. Численные значения шкала Харрингтона переводит качественные оценки в количественные в диапазоне от 0 до 1 на основе статистической обработки психологических особенностей человека, универсальна и может использоваться для оценки различных качественных показателей [0]. Для исключения двусмысленности при граничных значениях числовые значения шкалы смещены на 0,1 в рамках данного подхода:

0,81–1,0 — уровень подготовки работника очень высокий;
0,64–0,8 — уровень подготовки работника высокий;
0,38–0,63 — уровень подготовки работника средний;
0,21–0,37 — уровень подготовки работника низкий;
0–0,2 — уровень подготовки работника очень низкий.

Немаловажно также оценить не только подготовку каждого из работников, но и общий уровень подготовки сотрудников организации. Для его оценки используется следующая формула (формула 2):

, (2)

где — общий уровень подготовки сотрудников организации, P — показатель общий подготовки работника в области ИБ, n — количество заполненных работниками анкет.

Результат интерпретируется аналогично частному анкетированию по шкале Харрингтона:

0,81–1,0 — общий уровень подготовки сотрудников организации очень высокий;

0,64–0,8 — общий уровень подготовки сотрудников организации высокий;

0,38–0,63 — общий уровень подготовки сотрудников организации средний;

0,21–0,37 — общий уровень подготовки сотрудников организации низкий;

0–0,2 — общий уровень подготовки сотрудников организации очень низкий.

В случае выявления у работника, который непосредственно занимается обеспечением ИБ в организации очень низкого или низкого уровня подготовки, целесообразно произвести ротацию кадрового состава. При обнаружении среднего уровня подготовки следует направить сотрудника на курсы повышения квалификации.

Помимо оценки профессиональной подготовки сотрудников, важно также провести оценку самой системы обеспечения информационной безопасности в организации. Необходимо убедиться в адекватности и эффективности принятых политик безопасности, процедур мониторинга и реагирования на инциденты, использования средств защиты информационных ресурсов.

Проведение аудита информационной безопасности поможет выявить слабые места в системе защиты и рекомендовать улучшения в работе персонала, политике безопасности, технических мероприятиях и процедурах управления данными.

Здесь важно учитывать не только факторы внутренней угрозы, связанные с действиями или небрежностью сотрудников, но и внешние угрозы, такие как хакерские атаки, вредоносные программы и другие виды киберугроз.

Таким образом, предложенный подход позволяет оценить подготовку сотрудников объекта в области ИБ как в общем, так и каждого в отдельности и предпринять меры, минимизирующие влияние человеческого фактора на состояние защищенности объекта. А также анализ и улучшение системы информационной безопасности в целом, позволят организации эффективно реагиро-

вать на угрозы и обеспечить надежную защиту конфиденциальной информации и цифровых ресурсов.

Список источников

1. Приказа Минтруда РФ № 525Н от 14 сентября 2022 года «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» [Электронный ресурс] – Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=436271 (Дата обращения: 02.03.2024).

2. Шкалы показателей без планового значения [Электронный ресурс] – Режим доступа: https://upr.ru/article/upravlencheskie-shkaly-chast-1-shkaly-pokazateley-bez-planovogo-znacheniya/ (Дата обращения: 18.11.2023).

Статья поступила в редакцию 22.04.2024; принята к публикации 15.05.2024.

Информация об авторах

Юмакаев М. Р. – выпускник кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Сафоненко С. В. – студент кафедры «Системы информационной безопасности», специальность 10.05.04 – Информационно-аналитические системы безопасности, ФГБОУ ВО «БГТУ».

Голембиовская О. М. – к. т. н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Юмакаев М. Р. – обработка материала, написание статьи (50 %).
Сафоненко С. В. – сбор материала, частичное написание статьи (25 %).
Голембиовская О. М. – идея, научное редактирование (25 %).

Конфликт интересов отсутствует.

ISBN 978-5-907570-87-0 *Информационная безопасность и защита персональных данных. Проблемы и пути их решения: XVI межрегиональная научно-практическая конференция. Брянск, 2024, сборник материалов и докладов*

Научная статья
УДК 381.3

Состав и последовательность диагностики радиационной стойкости

Андрей Ильич Яньков[1], Олеся Владимировна Оксюта[2], Юрий Васильевич Гриднев[3], Артём Петрович Лапшин[4], Николай Николаевич Литвинов[5]
[1, 2, 3, 4, 5] Воронежский государственный лесотехнический университет имени Г. Ф. Морозова, Воронеж, Россия
[1] yaidom@bk.ru
[2] kor_o@mail.ru
[3] grid_u_v@mail.ru
[4] lap109@mail.ru
[5] nilit1990@mail.ru

Аннотация. Статья рассматривает важность диагностики радиационной стойкости электронных компонентов (ЭКБ) на различных этапах их жизненного цикла: при проектировании, производстве и эксплуатации. Авторы предлагают рациональный состав испытаний, основанный на требованиях государственных стандартов «Климат-7», включающий воздействие нейтронного потока и экспозиционной дозы гамма-излучения. Кроме того, в статье указывается на важность проведения испытаний на стойкость к воздействию тяжелых заряженных частиц и высокоэнергетических протонов космического пространства для радиационно-стойких микросхем.

Ключевые слова: электронная компонентная база, диагностика, радиация.
Для цитирования: Яньков А. И., Оксюта О. В., Гриднев Ю. В., Лапшин А. П., Литвинов Н. Н. Состав и последовательность диагностики радиационной стойкости // Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Брянск, 2024. С. 316–320.

Диагностика радиационной стойкости ЭКБ должна осуществляться на всех этапах жизненного цикла: на этапе проектирования, постановки на производство и в процессе эксплуатации (этап серийного производства).

Диагностика на этапе проектирования проводится на основе моделирования, диагностика в процессе производства заключается в проведении экспериментальных исследований и проведении аттестационных испытаний разработанной ЭКБ на стойкость к воздействию специальных воздействующих факторов.

Состав и последовательность диагностики радиационной стойкости (далее испытания), проводимой на последних этапах, основаны на требованиях комплекса государственных стандартов «Климат-7».

Исходя из требований действующей в настоящее время нормативной базы, для проведения испытаний и оптимизации получения достоверной информации авторским коллективом был выбран рациональный состав испытаний на необратимые изменения параметров по эффектам ионизации и структурных повреждений.

Он основан на принципах: аддитивности изменения параметров ИЭТ от ионизации и структурных повреждений; равноценности поглощенных ионизационных доз от различных видов ИИ; равноценности поглощенных структурных доз от различных видов ИИ.

В соответствии с указанными принципами все основные испытания на необратимые изменения параметров по эффектам ионизации и структурных повреждений заменяются двумя видами воздействия — воздействие нейтронного потока и экспозиционной дозы гамма-излучений, моделирующих или имитирующих установок, с учетом необходимых для этих целей норм испытаний.

В настоящее время для радиационно-стойких микросхем в состав обязательных видов испытаний введено испытание микросхем на стойкость к воздействию тяжелых заряженных частиц (ТЗЧ) и высокоэнергетических протонов космического пространства.

Полученный на основе общих методических положений рациональный состав испытаний выглядит следующим образом: испытания на стойкость к воздействию мощности экспозиционной дозы гамма- и плотности потока энергии рентгеновского излучений ядерного взрыва по уровню бессбойной работы; испытания на стойкость к воздействию максимальной мощности экспозиционной дозы гамма- и плотности потока энергии рентгеновского излучений ядерного взрыва; испытания на стойкость, обусловленную ионизационными эффектами гамма-рентгеновского и нейтронного излучений ядерного взрыва, гамма-нейтронного излучения ядерных установок, электронного и протонного излучений космического пространства; испытания на стойкость, обусловленную эффектами структурных повреждений нейтронного излучения ядерного взрыва и ядерных установок и протонного излучения космического пространства [1–5].

Для проведения любой группы испытаний авторским коллективом предложен следующий состав подготовительных операции, которые включают:

- испытания на стойкость к воздействию ТЗЧ космического пространства по одиночным эффектам, обусловленную локальными ионизационными эффектами в активной области кристалла;

- пересчет по методикам, приведенным в действующей нормативной документации заданных значений характеристик 7.И2, 7.И3, 7.И7, 7.И12, 7.И13, 7.С1, 7.К1, 7.К4 факторов 7.И, 7.С, 7.К, в эквивалентные значения характеристик 7.И1, 7.И6, 7.И7 (7.С4) и 7.И6;

- выбор методов испытаний — испытательное воздействие и реализующих их моделирующие и имитирующие установки (по результатам анализа за-

данных требований по стойкости к спецфакторам, конструктивного исполнения микросхемы, доминирующих эффектов и механизмов их отказов);

- определение норм испытаний в соответствии с НД;

- выбор параметров-критериев годности микросхем (согласно документам по стандартизации оборонной продукции и ТУ с учетом особенностей функционирования в аппаратуре), включая параметры, потенциально чувствительные к испытательному воздействию в заданном диапазоне изменений характеристик спецфакторов;

- выбор методов и технических средств задания режимов работы и контроля значений параметров и функционирования микросхем;

- подготовку испытательного комплекса (источника с конструктивными средствами, в том числе для испытаний в диапазоне температур, средств определения параметров воздействия, дозиметрического сопровождения испытаний, устройств управления, задания режимов работы, измерения электрических параметров и контроля функционирования микросхем);

- подготовку испытываемых образцов (например, удаление крышек корпусов, распайка на платы и др.) и испытательной оснастки, которая должна обеспечивать доступ испытательного воздействия к кристаллу микросхем (с учетом проникающих способностей воздействий) и возможность подключения по схеме испытаний;

- разработка и согласование в установленном порядке программы-методики испытаний.

В соответствии действующей НД оценка стойкости ЭКБ осуществляется при их проектировании, производстве и эксплуатации. Для этого было предложено на разных этапах использовать расчетные, расчетно-экспериментальные и экспериментальные методы оценки.

На ранних стадиях проектирования оценка стойкости проводится расчетным методом, например, на этапе технического проекта проводят расчетную оценку стойкости разрабатываемых микросхем с использованием программных средств в составе САПР или разработанного тестового обеспечения. Расчетно-экспериментальный метод применен на средних уровнях иерархии и конечном этапе проектирования, а также при изготовлении и испытании изделий. Такой подход является актуальным в условиях мелкосерийного и неритмичного производства.

При изготовлении изделий проводится экспериментальная оценка стойкости непосредственно на моделирующих или имитирующих установках, которая является критерием правильности всех ранее осуществляемых мероприятий по оценке стойкости, а также расчетно-экспериментальные методы оценки стойкости готового изделия в реальных условиях, т. е. на этапе получения опытных образцов проводятся однократные испытания на стойкость к воздействию специальных факторов, в составе квалификационных испытаний (подгруппы испытаний «К»), на основании которых предоставляется информация в ТУ на разработанные микросхемы;

При серийном производстве дополнительно проводится контроль пластин на соответствие требованиям стойкости, что гарантирует неизменность технологии и снабжение потребителя изделиями, которые с гарантией обеспечивают требуемый уровень стойкости. Таким образом, на этапе серийного изготовления микросхем, для изделий требования по стойкости к которым соответствует группам исполнения 3Ус – 6Ус по ГОСТ РВ 20.39.414.2-98, проводятся испытания каждой партии пластин (подгруппы испытаний «Е») на стойкость к воздействию минимального набора специальных факторов. Данный вид диагностики выделен в отдельный пункт, как наиболее важный для подтверждения стабильности техпроцесса и соответственно качества изготовления пластин.

Так как подтверждение адекватности разработанных авторским коллективом математических моделей расчета радиационной стойкости осуществляется только проведением испытаний, рассмотрим более подробно применённые методы экспериментальной оценки радиационной стойкости.

Список источников

1. Повышение формализации задач верификации топологии и электрической схемы для систем автоматизированного проектирования / А.В. Полуэктов, К.В. Зольников, А.В. Ачкасов, Ю.А. Чевычелов // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 102-111.

2. Полуэктов, А.В. Моделирование влияния электромагнитных полей на микросхемы / А.В. Полуэктов, Р.Ю. Медведев, К.В. Зольников // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 129-136.

3. Технология разработки RTL модели описания изделия при разработке программно-аналитического комплекса САПР / Д. В. Шеховцов, А. М. Плотников, К. В. Зольников, А. И. Заревич // Моделирование систем и процессов. – 2023. – Т. 16, № 3. – С. 7.

4. Применение изделий полупроводниковой электроники в экстремальных условиях / М. И. Колесников, М. Э. Харченко, В. А. Дорохов, К. В. Зольников // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 46-56.

5. Полуэктов, А. В. Моделирование работы диода и оценка параметров его работы / А. В. Полуэктов, Р. Ю. Медведев, В. К. Зольников // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 85-93.

Статья поступила в редакцию 05.05.2024; принята к публикации 15.05.2024.

Информация об авторах

Яньков А. И. – к. т. н., заведующий лабораторией ФГБОУ ВО «ВГЛТУ».

Оксюта О. В. – к. т. н., доцент кафедры вычислительной техники и информационных систем ФГБОУ ВО «ВГЛТУ».

Гриднев Ю. В. – к. филол. н., доцент кафедры иностранных языков ФГБОУ ВО «ВГЛТУ».

Лапшин А. П. – аспирант ФГБОУ ВО «ВГЛТУ».
Литвинов Н. Н. – к. т. н., доцент ФГБОУ ВО «ВГЛТУ».

Вклад авторов

Яньков А. И. – идея, сбор материала, обработка материала, частичное написание статьи (40 %).

Оксюта О. В. – сбор материала, обработка материала, частичное написание статьи (15 %).

Гриднев Ю. В. – сбор материала, обработка материала, частичное написание статьи (15 %).

Лапшин А. П. – сбор материала, обработка материала, частичное написание статьи (15 %).

Литвинов Н. Н. – сбор материала, обработка материала, частичное написание статьи (15 %).

Конфликт интересов отсутствует.