БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 1 (116). – 53–69

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-1-53-69

АНАЛИЗ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ НА ОСНОВЕ ЭЛЕКТРОМАГНИТНЫХ СИГНАЛОВ РАДИОДИАПАЗОНА В СОВРЕМЕННЫХ ТЕХНОЛОГИЯХ ПЕРЕДАЧИ ДАННЫХ*

И.В. ТРУБИН[1], А.Д. НАБОРЩИКОВА[2], П.Р. ЧЕРНЫШЕВ[3]

[1] *630087, г. Новосибирск, ул. Немировича-Данченко 138, офис 2/2, Общество с ограниченной ответственностью «КБ “Автоматика”», заместитель директора. E-mail: i.trubin@corp.nstu.ru*

[2] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: naborshhikova.2020@stud.nstu.ru*

[3] *630082, г. Новосибирск, ул. Дачная 60/1, Акционерное общество «Радио и микроэлектроника», инженер-программист студенческого КБ. E-mail: p.chernyshev.2021@stud.nstu.ru*

С развитием современных технологий угроза утечки информации становится всё более актуальной. Представлена классификация технических каналов утечки информации, рассмотрена более подробная классификация для каналов утечки информации на основе электромагнитных сигналов радиодиапазона. Описана область применения некоторых распространенных и доступных технологий, таких как Wi-Fi, Bluetooth, системы мобильной связи и Zigbee. Рассмотрена возможность организации канала утечки, связанного с побочными электромагнитными излучениями (ПЭМИ). Осуществлен анализ сценариев проведения атак с использованием некоторых распространенных технологий передачи данных, а именно: Wi-Fi, Bluetooth, системы мобильной связи и Zigbee с целью получения доступа к конфиденциальным данным или с целью перехвата управления устройствами с дальнейшей эксплуатацией данной уязвимости. Все рассмотренные каналы утечки подвержены общим видам атак злоумышленников: аппаратные атаки, атаки с использованием вредоносного ПО (программного обеспечения), атаки на цепочки поставок, перехват передаваемой информации. Анализ имеющихся уязвимостей и возможных мер защиты для некоторых распространенных технологий передачи данных, таких как Wi-Fi, Bluetooth, системы мобильной связи и Zigbee. Исходя из результатов проведенного анализа уязвимостей и возможных сценариев атак предложен комплекс программных, аппаратных и организационных мер для снижения вероятности возникновения утечки информации по техническим каналам на основе электромагнитных сигналов радиодиапазона. Рассмотрена возможность использования программного обеспе-

* Статья получена 30 января 2025 г.

чения в целях мониторинга утечек информации. Даны рекомендации по использованию рассмотренных технологий для снижения эффективности и предотвращения атак злоумышленников.

Ключевые слова: каналы утечки, Wi-Fi, Bluetooth, Zigbee, системы мобильной связи, перехват данных, mesh, ПЭМИ

ВВЕДЕНИЕ

В современном мире информация является одним из самых ценных ресурсов, поэтому проблема ее утечки становится всё более актуальной. Каналы утечки информации представляют собой различные пути, через которые конфиденциальные данные могут быть переданы без разрешения владельца или украдены. Эти каналы могут включать в себя как технические средства, такие как сети и устройства, так и человеческий фактор, в том числе инсайдерские угрозы.

Информация – это полезные данные, получаемые в процессе работы устройств, которые могут храниться, использоваться и передаваться по каналам передачи информации. Технология – это совокупность методов, инструментов и процессов для работы с информацией и ее передачей. С развитием технологий появляется угроза утечки информации – процесса несанкционированного получения данных через каналы утечки информации [1].

В настоящей обзорной статье рассматриваются четыре технологии передачи информации: Wi-Fi, Bluetooth, системы мобильной связи и Zigbee. Каждая из них имеет свои уникальные характеристики и уязвимости, которые могут быть использованы злоумышленниками для несанкционированного доступа к данным.

Wi-Fi-сети используются для передачи данных очень широко, однако они подвержены различным атакам, таким как перехват данных и несанкционированный доступ. Это высказывание справедливо и для технологии Bluetooth. Возможна реализация угрозы с перехватом управления устройствами при использовании Zigbee. Наконец, сотовые сети, используемые для мобильной связи, подвержены различным видам атак, включая перехват сообщений и подслушивание разговоров.

В статье подробно рассмотрены вышеперечисленные технологии передачи информации, описана их область применения. Уделено внимание некоторым возможным сценариям атак, проведен их анализ. Рассмотрены уязвимости этих технологий. На основании анализа предложен комплекс мер, направленных на снижение вероятности возникновения утечки информации.

1. КЛАССИФИКАЦИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Можно выделить несколько видов каналов утечки информации [2, 3], а именно:

- каналы утечки информации на основе акустических сигналов;
- каналы утечки информации на основе электрических сигналов;
- каналы утечки информации на основе электромагнитных сигналов радиодиапазона;
- каналы утечки информации на основе электромагнитных сигналов оптического диапазона.

В настоящей статье рассматриваются преимущественно каналы утечки на основе электромагнитных сигналов радиодиапазона. Данный вид объединяет следующие каналы:

- прямой радиоканал;
- радиоэлектрический канал;
- радиорадиоэлектронный канал.

Для рассмотренных в статье технологий, а именно: для Wi-Fi, Bluetooth, систем мобильной связи и Zigbee – наиболее вероятными являются утечки по прямому радиоканалу и по радиорадиоэлектронному каналу.

2. КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

В настоящее время в связи с широким распространением мобильных телефонов, планшетов, компьютеров и ноутбуков, на которых хранится ценная информация, достаточно часто используются следующие технологии передачи информации: Wi-Fi, Bluetooth, системы мобильной связи. Также широкое распространение получил Zigbee, используемый в системах «умный дом». Такие системы всё больше набирают популярность, так как позволяют повысить комфорт и контролировать безопасность квартиры. Ниже рассмотрены возможные способы атаки злоумышленников в отношении указанных технологий и некоторые способы защиты.

2.1. WI-FI

Широкое распространение интернета в повседневной жизни накладывает определенные требования к обеспечению безопасности мобильных устройств. Всё больше создается оборудования, работающего с так называемым «интернетом вещей». «Интернет вещей» (Internet of Things – IOT) – это концепция, в которой устройства соединены в единую сеть с помощью интернета [4], они

обмениваются требуемой информацией без прямого участия человека, а также могут передавать команды между узлами. Эта технология используется во многих отраслях жизни, например в системах «умного дома». Такое широкое распространение IOT-устройств заставляет оценивать информацию по степени ее важности, и для чувствительных сведений требуется принятие мер защиты.

Можно выделить несколько вероятных сценариев атаки на инфраструктуру, среди них наиболее актуальны следующие:

- Deauth (атака, при которой злоумышленник отправляет поддельные пакеты deauthentication, принуждая устройства отключаться от точки доступа);
- DDOS (атака, при которой множество скомпрометированных компьютеров одновременно отправляют запросы на сервер, перегружая его и делая его недоступным для пользователей);
- Brute force (атака, при которой злоумышленник перебирает все возможные комбинации паролей, пока не найдет правильный);
- Man-in-the-middle (атака, при которой злоумышленник перехватывает и потенциально изменяет коммуникацию между двумя узлами, не выдавая своего присутствия);
- Injection (атака, при которой злоумышленник вставляет вредоносный код в запросы через пользовательский ввод) [5].

Многие из возможных рисков угроз могут быть вызваны некорректной настройкой устройств или самой сети. Но эти проблемы зачастую могут быть устранены только при использовании доверенной Wi-Fi-сети, например домашней сети или сети компании. Однако при использовании публичных сетей Wi-Fi следует проявлять осторожность, так как у пользователя нет возможности влиять на настройки сети, такие как протокол шифрования, парольная защита и ряд других параметров. Из-за этого выполнение задачи обеспечения информационной безопасности ложится на конечное устройство [6]. Следует обращать внимание на протокол безопасности используемой сети Wi-Fi, например, OPEN, WEP, WPA (Wi-Fi Protected Access), WPA2, WPA3 (табл. 1).

Наиболее предпочтительным стандартным протоколом для Wi-Fi является WPA3. Устройства, поддерживающие этот тип безопасности, используют WPA2. Однако существенная часть устройств выпущена до создания данного протокола, и они поддерживают только Wi-Fi Protected Access 2. Также не стоит использовать сети с протоколом OPEN (без защиты) или WEP, в силу того что он является устаревшим и небезопасным.

Канал утечки данных технологии Wi-Fi является очень опасным в связи с тем, что атака происходит без физического контакта, дальность связи в условиях помещения может превышать 100 метров, в условиях же прямой

видимости – до 500 метров. Почти 30 миллиардов устройств могут подключаться к сети, это предоставляет злоумышленникам возможность выбирать в качестве цели любого пользователя.

Таблица 1

Характеристики протоколов Wi-Fi Protected Access

	WPA	WPA2	WPA3
Краткое описание	Основан на стандарте 802.11i и не требует нового оборудования	Все обязательные функции стандарта 802. 11i и новое оборудование	Анонсирован Wi-Fi Alliance
Шифрование	TKIP + RC4	CCMP/AES	GCMP-256
Аутентификация	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Целостность данных	Алгоритм MIC	Код аутентификации сообщения в цепочке блоков шифрования, основанный на AES	256-битный код аутентификации сообщений Галуа по протоколу обеспечения целостности широковещательной / многоадресной рассылки (BIP-GMAC-256)
Управление ключами	Четырехстороннее рукопожатие	Четырехстороннее рукопожатие	Обмен данными по эллиптической кривой Диффи – Хеллмана (ECDH) и алгоритм цифровой подписи по эллиптической кривой (ECDSA)

Стоит обратить внимание на то, что существует возможность установки скрытых точек доступа, которые будут инициировать подключение устройств в тайне от владельцев. Такое действие трудноосуществимо при грамотно настроенных параметрах безопасности на устройствах [7].

Некоторые устройства могут быть оснащены специальными программными средствами для противодействия атакам. Например, средства IDS (Intrusion Detection System – система обнаружения вторжений), DLP (Data Leak/Loss Prevention – система, защищающая от утечек конфиденциальной информации, анализирует данные и их передачу в информационных системах) и другие. Эти решения преимущественно направлены на выявле-

ние начала атаки, что позволяет заблокировать подозрительные устройства [8].

Однако существуют атаки, которые сложно обнаружить заранее (например, которые основаны на времени отклика). С помощью специальных устройств генерируются сигналы, которые немного изменяют время отклика. По полученной информации можно расшифровать данные, которые передаются по каналу путем сравнения полученного времени отклика с известными пакетами (например, ARP-запросы и ответы на них) [9].

2.2. BLUETOOTH

В наши дни многие гаджеты оборудованы специальными микросхемами, предназначенными для передачи данных между устройствами с помощью Bluetooth. Все новые смартфоны выпускаются с поддержкой такого канала передачи, это относится и ко многим носимым устройствам. При подключении нескольких ведомых устройств к одному ведущему формируется пикосеть (рис. 1). Пикосеть – небольшая беспроводная локальная сеть, число активных ведомых устройств – от 1 до 7.

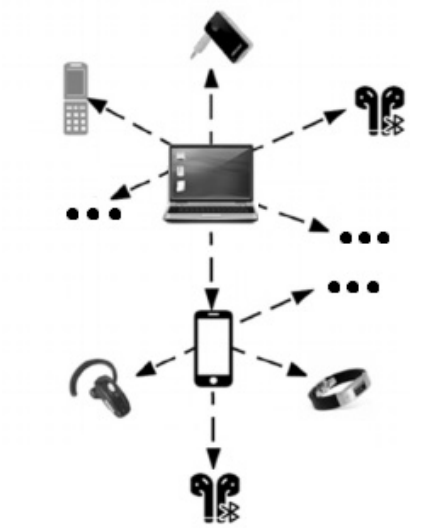

Рис. 1. Две пикосети Bluetooth

Благодаря появлению стандарта BLE (Bluetooth Low Energy) многие устройства не отключают Bluetooth полностью, просто переводят из «активного» режима в режим «приема» [10]. В режиме «приема» устройство не отправляет пакеты в сеть, но ведется сканирование частот, при нахождении авторизованного устройства выполняется сопряжение и перевод устройства в «активный» режим. В настоящее время существует только две спецификации Bluetooth – это Bluetooth BLE и Bluetooth Classic. Кроме того, есть устройства, которые поддерживают оба протокола (рис. 2).

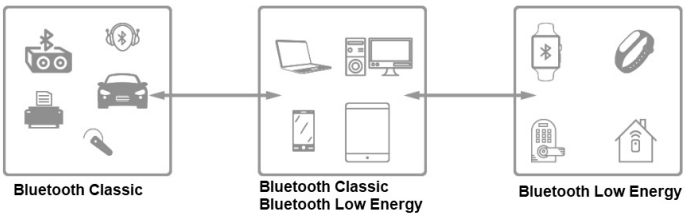

Рис. 2. Типы Bluetooth-устройств

Злоумышленник может легко получить информацию о том, какие устройства находятся поблизости. Наиболее часто используются Bluetooth-передатчики с мощностью, не превышающей 2,5 мВт (табл. 2). Если же злоумышленник создаст несколько точек Bluetooth, то он сможет достаточно достоверно определить местоположение устройств пользователя с помощью трассировки сигнала [11].

Таблица 2

Параметры Bluetooth

Класс	Максимальная мощность, мВт	Примерный радиус действия, м
1	100	100
2	2,5	10
3	1	1

Есть и другой способ отслеживать местоположение пользователя, для этого достаточно одной точки Bluetooth. В журналах мониторинга можно найти информацию, в какое время были доступны конкретные устройства, и на основе этих данных вычислить местоположение этих устройств [12].

Технология Bluetooth имеет ряд уязвимостей при сопряжении устройств. Вероятными сценариями могут быть такие атаки, как атака с подменой MAC (атака ведется еще до формирования пикосети при генерации ключей связи), brute-force (атака с перебором адресов устройств и паролей для подключения). При успешной атаке злоумышленник может получить доступ к аудио- и видеоканалу данных и системам управления. Как пример – «умный дом». Для уменьшения вероятности успешной атаки на устройство существует несколько методов, например: использование сложных и длинных паролей, при утере устройства необходимо удалять его из списка доверенных. Одним из методов является перевод устройств в режим, недоступный для обнаружения, при этом доверенные устройства смогут осуществить подключение [13].

Технология Bluetooth имеет и шанс утечки данных по каналу ПЭМИ. Цифровые микросхемы генерируют электромагнитные импульсы, которые могут оказать влияние на чувствительные элементы, при условии что они расположены достаточно близко друг к другу, таким образом информационный сигнал может дойти до антенны. При получении данного сигнала злоумышленник может восстановить данные, которые обрабатывались микросхемой. Этот эффект носит название Screaming channels («кричащие каналы») [14]. Одним из наиболее эффективных способов предотвращения утечки по данному каналу является выбор микросхем с разделенными задачами.

2.3. СИСТЕМЫ МОБИЛЬНОЙ СВЯЗИ

Существенная часть мобильных устройств, таких как смартфоны, планшеты и ноутбуки, имеет возможность подключения по каналам мобильной связи. Использование этих каналов позволяет осуществлять обмен информацией между устройствами практически по всему миру, а именно в зоне покрытия базовых станций, обеспечивающих работу данных каналов.

В настоящее время имеется целый ряд поколений мобильной сети, таких как 2G, 3G, 4G и не так давно появившийся стандарт сети 5G (табл. 3). Каждый из представленных стандартов работает в своем частотном диапазоне и обеспечивает пропускную способность, соответствующую заранее определенным критериям (чем выше стандарт, тем выше скорость сети).

Сети 2G, появившиеся в начале 1990-х годов, стали одним из первых стандартов мобильной связи. Основным протоколом этих сетей является GSM (Global System for Mobile Communications – глобальная система мобильной связи). Технология предоставила возможность передавать голос и обмениваться текстовыми сообщениями (SMS). Среди особенностей 2G можно выделить

наличие цифровой модуляции, которая обеспечила защиту сигналов от помех путем встраивания базовых методов шифрования передаваемых данных.

Таблица 3

Параметры сотовой связи

Поколение сотовой связи	Частотный диапазон для связи от телефона к базовой станции	Частотный диапазон для связи от базовой станции к телефону	Скорость траффика
2G (GSM)	890…915 МГц и 1710…1785 МГц	935…960 МГц и 1805…1880 МГц	14,4 кбит/с
3G	2010…2070 МГц	1920…1980 МГц	до 384 кбит/с в стандартном режиме и до 42 Мбит/с с использованием технологии HSPA+
4G	2500…2570 МГц	2620…2690 МГц	1 Гбит/с при скачивании и до 100 Мбит/с при отправке данных
5G	4400…5000 МГц	4400…5000 МГц	До 10 Гбит/с

Сети 3G, начавшие свое развитие с 2000-х годов, знаменовали переход к более высоким скоростям передачи информации относительно предыдущих стандартов, что позволило осуществлять выход в интернет. Основной стандарт – UMTS (Universal Mobile Telecommunications System) – обеспечил значительные улучшения скорости с использованием технологии HSPA+ (High Speed Packet Access). Более того, стала доступна поддержка мультимедиа и технологии CDMA (Code Division Multiple Access), что обеспечило более высокую плотность пользователей на одну базовую станцию.

Сети 4G стали прорывом в скорости, стандарт LTE (Long Term Evolution) предоставил пользователям скорость сети, сравнимую с проводным интернетом. В сетях 4G использована технология мультиплексирования OFDM (Orthogonal Frequency-Division Multiplexing), обеспечивающая высокую устойчивость к помехам. Вся передача данных происходит по протоколу IP, что упрощает внедрение голосовых услуг через VoIP (Voice over IP), имеется поддержка приоритизации трафика QoS (Quality of Service) для чувствительных к задержкам приложений.

Технология 5G, появившаяся в 2020 году, предлагает еще больше возможностей для мобильной сети, включая скорость до 10 Гбит/с с задержками

до 1 мс и поддержку до 1 миллиона устройств на квадратный километр для интернета вещей. Но использование миллиметровых волн для обеспечения более высокой пропускной способности требует также использования большего количества базовых станций из-за меньшего радиуса действия.

Такие типы подключения позволяют злоумышленникам достаточно легко передавать информацию с атакованного устройства. Атака может выполняться с помощью шпионских приложений, установленных на устройство. Очень большой список приложений в открытом доступе позволяет злоумышленнику создать поддельное приложение с названием, почти совпадающим с оригинальным. В качестве среды распространения идеально подходят магазины приложений (marketplace), такие как RuStore, AppStore и т. д. [15].

Однако мобильные сети используются не только в смартфонах. Широкое распространение эта технология получила в системах безопасности автомобилей, в системах «умного дома», в СКУД. В таком случае злоумышленнику сложно использовать шпионское программное обеспечение для кражи данных, такие устройства не устанавливают приложения, а происходит обновление программного обеспечения. Если же злоумышленник атакует цепочку поставок, у него будет возможность загрузки шпионского ПО на устройство. Атака заключается в поиске уязвимостей у разработчиков программного обеспечения и внедрения уязвимостей в код легитимных приложений. Для таких устройств больше подходит сценарий атаки с перехватом пакетов, например, с помощью подмены базовой станции, поскольку этот способ позволяет не использовать атаку на цепочку поставок. Однако метод тоже имеет ряд трудностей (например, шифрование пакетов). Злоумышленник, даже имея перехваченные пакеты, будет иметь трудности с их расшифровкой [16].

В качестве противодействия атакам необходимо использовать антивирусное программное обеспечение для обнаружения и защиты от вредоносного ПО. В качестве дополнения к антивирусному ПО, для выявления факта утечки данных можно использовать специальные программы, выполняющие полное логирование всех операций. Еще один, более сложный метод анализа утечек – это поднятие собственной базовой станции. С использованием собственной базовой станции возможно фиксировать все отправляемые пакеты и устанавливать несанкционированные каналы отправки данных.

2.4. ZIGBEE

Zigbee – это стандарт беспроводной связи, основанный на протоколе IEEE 802.15.4 и разработанный специально для приложений с низким уровнем потребления энергии и малой скоростью передачи данных, таких как системы

«умного дома», промышленная автоматизация и медицинские устройства. Низкое энергопотребление устройств Zigbee достигается за счет нахождения их в спящем режиме во время отсутствия передачи данных. Для защиты от перехвата и подмены данных используется 128-битное шифрование AES [17].

Скорость передачи данных Zigbee составляет 250 кбит/с, что достаточно для большинства приложений, работает на частотах 2,4 ГГц, 868 МГц (Европа) и 915 МГц (США). Основной частотный диапазон 2,4 ГГц обеспечивает глобальную совместимость всех устройств, доступных в сети.

Стандарт поддерживает такие топологии, как «звезда», «дерево» и «сетка» (Mesh). Mesh-топология особенно важна для надежной передачи данных, так как каждый узел может служить ретранслятором, однако это может стать уязвимостью, когда злоумышленник получает доступ через скомпрометированный узел сети. В качестве защиты рекомендуется использовать системы обнаружения аномалий и мониторинга узлов.

Существуют возможности подмены устройств, когда злоумышленник имитирует устройство в сети для получения данных и для атаки с целью создания помех и перегрузки сети. Из-за ограниченной пропускной способности канала шифрование может быть недостаточно сильным для предотвращения атак на основе анализа трафика.

Для защиты от подобных атак лучше всего использовать проверку идентификаторов устройств и повторную их аутентификацию, настройку лимитов на объем передаваемых данных и использование уникальных ключей шифрования для каждого устройства в сети.

ЗАКЛЮЧЕНИЕ

Утечка данных представляет собой серьезную угрозу, охватывающую различные каналы передачи информации, такие как Wi-Fi, Bluetooth, Zigbee и сотовые сети. Каждый из этих каналов имеет свои уникальные уязвимости, которые могут быть использованы злоумышленниками для несанкционированного доступа к конфиденциальным данным, что подчеркивает необходимость тщательного анализа и разработки стратегий защиты.

Wi-Fi-сети, несмотря на свою популярность и удобство, подвержены множеству атак, включая перехват данных, атаки типа «Человек посередине» и DDoS-атаки. Публичные сети особенно уязвимы, так как пользователи не могут контролировать их безопасность, что делает их привлекательной целью для злоумышленников. Чтобы минимизировать риски, крайне важно использовать надежные протоколы шифрования, такие как WPA3, и избегать подключения к открытым сетям. Нужно уделить внимание своевременному об-

новлению программного обеспечения на роутерах. Следует использовать сложные пароли для точки доступа и для интерфейса управления.

Bluetooth-технологии также имеют свои риски, включая возможность отслеживания местоположения и атаки на сопряжение устройств. Уязвимости, связанные с подменой MAC-адресов и перебором паролей, могут привести к утечке конфиденциальной информации. Для повышения безопасности рекомендуется использовать сложные пароли, полностью отключать Bluetooth, когда он не нужен, регулярно проверять список доверенных устройств и удалять ненужные.

Zigbee, например, в системах «умный дом» может быть атакован внедрением злоумышленников в систему при помощи имитации устройства, анализа трафика и перегрузки системы. Для защиты от подобного вида атак рекомендуется на этапе установки использовать проверку идентификаторов устройств, настройку лимита трафика и уникальные ключи шифрования для каждого из устройств в сети.

Каналы, используемые для мобильной связи, могут быть подвержены атакам через шпионские приложения и перехват пакетов. Злоумышленники, чтобы получить доступ к данным пользователей, могут создавать поддельные приложения, которые выглядят как легитимные. Для защиты от таких угроз необходимо использовать антивирусное программное обеспечение на устройствах и системы журналирования, такие как SysLog, которые могут выявлять подозрительную активность и утечки данных.

Для эффективной защиты от утечек данных необходимо использовать комплексные меры безопасности, включая надежные протоколы шифрования, регулярное обновление программного обеспечения, использование многофакторной аутентификации и систем обнаружения вторжений. Важно повышать осведомленность пользователей о потенциальных рисках и методах защиты. Регулярные проверки устройств на наличие уязвимостей помогут минимизировать вероятность утечек данных и обеспечить безопасность информации в цифровом пространстве.

Все каналы утечки информации подвержены общим видам атак, которые можно классифицировать как аппаратные, атаки с использованием вредоносного ПО и перехват передаваемых данных. В дальнейшем планируется использование SDR-приемника для более детального исследования возможных каналов утечки информации для данных технологий. Будут использоваться возможности SDR-платформы по работе с сигналами и в целях эмуляции описанных в статье атак.

Все описанные технологии в той или иной степени подвержены вышеописанным видам атак, и на это необходимо обращать внимание при выборе методов защиты. В каких-то случаях будет достаточно простых организацион-

ных мер, в других же следует вносить поправки в программную или аппаратную конфигурацию.

Таким образом, в условиях постоянно развивающихся технологий и угроз защита данных должна стать неотъемлемой частью любой стратегии управления информацией, что позволит сохранить конфиденциальность и целостность данных в современном мире.

СПИСОК ЛИТЕРАТУРЫ

1. Deep learning for cyber threat detection in IoT networks: a review / A. Aldhaheri, F. Alwahedi, M.A. Ferrag, A. Battah // Internet of Things and Cyber-Physical Systems. – 2024. – Vol. 4. – P. 110–128. – DOI: 10.1016/j.iotcps.2023.09.003.

2. *Süzen A.A.* Cyber attacks for data breach and possible defense strategies in internet of healthcare things ecosystem // International Journal of 3D Printing Technologies and Digital Industry. – 2023. – Vol. 7 (1). – P. 55–63. – DOI: 10.46519/ij3dptdi.1240743.

3. Analysing leakage during VPN establishment in public Wi-Fi networks / C. Burkert, J.A. McDougall, H. Federrath, M. Fischer // IEEE International Conference on Communications. – IEEE, 2021. – DOI: 10.1109/ICC42927.2021.9500375.

4. *Lukova-Chuiko N., Lapteva T.* Improvement of the method of detection and location of illegal access points to the wireless network of information activity objects // Information Systems and Technologies Security. – 2023. – Vol. 1 (6). – P. 21–27. – DOI: 10.17721/ists.2023.1.21-27.

5. *Das A., Pramod*. Design and development of an efficient network intrusion detection system using ensemble machine learning techniques for Wifi environments // International Journal of Advanced Computer Science and Applications. – 2022. – Vol. 13 (4). – P. 856–866. – DOI: 10.14569/IJACSA.2022.0130499.

6. Characterization and detection of cross-router covert channels / O. Shvartzman, A. Ovadya, K. Zvi, O. Shwartz, R. Ogen, Y. Mallah, N. Gilboa, Y. Oren // Computers and Security. – 2023. – Vol. 127. – DOI: 10.1016/j.cose.2023.103125.

7. *Celosia G., Cunche M.* DEMO: Himiko: a human interface for monitoring and inferring knowledge on bluetooth-low-energy objects // WiSec 2019: Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks. – ACM, 2019. – P. 292–293. – DOI: 10.1145/3317549.3326297.

8. *Zhang H., Maji A.K., Bagchi S.* Privacy in the mobile world: an analysis of bluetooth scan traces // CPSIOTSEC '20: Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy. – ACM, 2020. – P. 61–65. – DOI: 10.1145/3411498.3419962.

9. *Andani S.R.* Analysis of information security in data leaks in the PeduliLindungi application // The IJICS (International Journal of Informatics and Computer Science). – 2021. – Vol. 5 (3). – P. 246. – DOI: 10.30865/ijics.v5i3.3406.

10. Security vulnerabilities in bluetooth technology as used in IoT / A.M. Lonzetta, P. Cope, J. Campbell, B.J. Mohd, T. Hayajneh // Journal of Sensor and Actuator Networks. – 2018. – Vol. 7 (3). – DOI: 10.3390/jsan7030028.

11. Screaming channels: when electromagnetic side channels meet radio transceivers / G. Camurati, S. Poeplau, M. Muench, T. Hayes, A. Francillon // CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – ACM, 2018. – P. 163–177. – DOI: 10.1145/3243734.3243802.

12. *Kulkarni S.P., Bojewar S.* Vulnerabilities of smartphones // International Research Journal of Engineering and Technology. – 2015. – Vol. 2 (9). – P. 2422–2426.

13. *Sayyad J., Taha M., Sankpal A.* Advanced car security system // International Journal of Scientific Research in Network Security and Communication. – 2017. – Vol. 5 (3). – P. 165–169.

14. ZPA: a smart home privacy analysis system based on ZigBee encrypted traffic / R. Li, W. Zhang, L. Wu, Y. Tang, X. Xie // Wireless Communications and Mobile Computing. – 2023. – Vol. 2023. – P. 1–16. – DOI: 10.1155/2023/6731783.

Трубин Игорь Витальевич, заместитель директора ООО «КБ “Автоматика”». Основное направление научных исследований – защита технических каналов утечки информации. E-mail: i.trubin@corp.nstu.ru

Наборщикова Александра Денисовна, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – разработка систем предотвращения утечки информации по техническим каналам. E-mail: naborshhikova.2020@stud.nstu.ru

Чернышев Павел Романович, инженер-программист студенческого КБ АО «Радио и микроэлектроника». Область научных интересов – разработка систем обнаружения утечки информации по техническим каналам. E-mail: p.chernyshev.2021@stud.nstu.ru

DOI: 10.17212/2782-2230-2025-1-53-69

Analysis of information leakage channels based on electromagnetic radio band signals in modern data transmition technologies*

I.V. Trubin[1], A.D. Naborshchikova[2], P.R. Chernyshev[3]

[1] *"DB AUTOMATION" LTD, 138 Nemirovich-Danchenko str., Novosibirsk, 630087, Russian Federation, associate director. E-mail: i.trubin@corp.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of Information Security Department. E-mail: naborshhikova.2020@stud.nstu.ru*
[3] *"Radio and Microelectronics" JSC, Dachnaya St. 60/1, Novosibirsk, 630082, Russian Federation, software Engineer at the Student DB. E-mail: p.chernyshev.2021@stud.nstu.ru*

With the development of modern technologies, the threat of information leakage is becoming more urgent. The classification of technical information leakage channels is presented, and a more detailed classification for information leakage channels based on electromagnetic signals of the radio band is considered. It provides a brief description and describes the scope of some common and affordable technologies such as Wi-Fi, Bluetooth, cellular communication systems and Zigbee. The possibility of organizing a leakage channel associated with Side effects of electromagnetic radiation (TEMPEST) is considered. The scenarios of attacks using some common data transmission technologies, namely Wi-Fi, Bluetooth, mobile communication systems and Zigbee, were analyzed in order to gain access to confidential data or to intercept device control, with further exploitation of this vulnerability. All the considered leakage channels are subject to common types of attacks by intruders: app attacks, attacks using malware (software), attacks on supply chains, interception of transmitted information. Analysis of existing vulnerabilities and possible protection measures for some common data transmission technologies such as Wi-Fi, Bluetooth, mobile communication systems and Zigbee. Based on the results of the vulnerability analysis and possible attack scenarios, a set of software, hardware and organizational measures has been proposed to reduce the likelihood of information leakage through technical channels based on electromagnetic radio signals. The possibility of using the software for monitoring information leaks is considered. Recommendations are given on the use of the considered technologies to reduce the effectiveness and prevent malicious attacks.

Keywords: leakage channels, Wi-Fi, Bluetooth, Zigbee, cellular communication systems, data interception, mesh, TEMPEST

REFERENCES

1. GOST R 53114-2008. Protection of information. Provision of information 1. Aldhaheri A., Alwahedi F., Ferrag M.A., Battah A. Deep learning for cyber threat

* *Received 30 January 2025.*

detection in IoT networks: a review. *Internet of Things and Cyber-Physical Systems*, 2024, vol. 4, pp. 110–128. DOI: 10.1016/j.iotcps.2023.09.003.

2. Süzen A.A. Cyber attacks for data breach and possible defense strategies in internet of healthcare things ecosystem. *International Journal of 3D Printing Technologies and Digital Industry*, 2023, vol. 7 (1), pp. 55–63. DOI: 10.46519/ij3dptdi.1240743.

3. Burkert C., McDougall J.A., Federrath H., Fischer M. Analysing leakage during VPN establishment in public Wi-Fi networks. *IEEE International Conference on Communications*. IEEE, 2021. DOI: 10.1109/ICC42927.2021.9500375.

4. Lukova-Chuiko N., Lapteva T. Improvement of the method of detection and location of illegal access points to the wireless network of information activity objects. *Information Systems and Technologies Security*, 2023, vol. 1 (6), pp. 21–27. DOI: 10.17721/ists.2023.1.21-27.

5. Das A., Pramod. Design and development of an efficient network intrusion detection system using ensemble machine learning techniques for Wifi environments. *International Journal of Advanced Computer Science and Applications*, 2022, vol. 13 (4), pp. 856–866. DOI: 10.14569/IJACSA.2022.0130499.

6. Shvartzman O., Ovadya A., Zvi K., Shwartz O., Ogen R., Mallah Y., Gilboa N., Oren Y. Characterization and detection of cross-router covert channels. *Computers and Security*, 2023, vol. 127. DOI: 10.1016/j.cose.2023.103125.

7. Celosia G., Cunche M. DEMO: Himiko: a human interface for monitoring and inferring knowledge on bluetooth-low-energy objects. *WiSec 2019: Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2019, pp. 292–293. DOI: 10.1145/3317549.3326297.

8. Zhang H., Maji A.K., Bagchi S. Privacy in the mobile world: an analysis of bluetooth scan traces. *CPSIOTSEC '20: Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy*. ACM, 2020, pp. 61–65. DOI: 10.1145/3411498.3419962.

9. Andani S.R. Analysis of information security in data leaks in the PeduliLindungi application. *The IJICS (International Journal of Informatics and Computer Science)*, 2021, vol. 5 (3), p. 246. DOI: 10.30865/ijics.v5i3.3406.

10. Lonzetta A.M., Cope P., Campbell J., Mohd B.J., Hayajneh T. Security vulnerabilities in bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks*, 2018, vol. 7 (3). DOI: 10.3390/jsan7030028.

11. Camurati G., Poeplau S., Muench M., Hayes T., Francillon A. Screaming channels: when electromagnetic side channels meet radio transceivers. *CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 163–177. DOI: 10.1145/3243734.3243802

12. Kulkarni S.P., Bojewar S. Vulnerabilities of smartphones. *International Research Journal of Engineering and Technology*, 2015, vol. 2 (9), pp. 2422–2426.

13. Sayyad J., Taha M., Sankpal A. Advanced car security system. *International Journal of Scientific Research in Network Security and Communication*, 2017, vol. 5 (3), pp. 165–169.

14. Li R., Zhang W., Wu L., Tang Y., Xie X. ZPA: a smart home privacy analysis system based on ZigBee encrypted traffic. *Wireless Communications and Mobile Computing*, 2023, vol. 2023, pp. 1–16. DOI: 10.1155/2023/6731783.

Для цитирования:

Трубин И.В., Наборщикова А.Д., Чернышев П.Р. Анализ каналов утечки информации на основе электромагнитных сигналов радиодиапазона в современных технологиях передачи данных // Безопасность цифровых технологий. – 2025. – № 1 (116). – С. 53–69. – DOI: 10.17212/2782-2230-2025-1-53-69.

For citation:

Trubin I.V., Naborshchikova A.D., Chernyshev P.R. Analiz kanalov utechki informatsii na osnove elektromagnitnykh signalov radiodiapazona v sovremennykh tekhnologiyakh peredachi dannykh [Analysis of information leakage channels based on electromagnetic radio band signals in modern data transmition technologies]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 1 (116), pp. 53–69. DOI: 10.17212/2782-2230-2025-1-53-69.