УДК 621.3

Акишин Андрей Владимирович
Доцент, КВВУ, Краснодар

Малютин Александр Андреевич
Слушатель, КВВУ, Краснодар

ИССЛЕДОВАНИЕ ЭЛЕКТРИЧЕСКИХ УСТРОЙСТВ ПЕРЕХВАТА ИНФОРМАЦИИ

Аннотация: В статье рассматриваются электрические устройства перехвата информации, дается их определение как специализированных технических средств для несанкционированного получения электронных данных. Проводится классификация этих устройств по методу перехвата, типу информации, среде передачи и конструктивному исполнению. Анализируются основные принципы работы устройств, включая физические основы передачи и приема сигналов, а также механизмы аналого-цифрового преобразования. Особое внимание уделяется современным тенденциям развития технологий перехвата, таким как миниатюризация, применение искусственного интеллекта и машинного обучения, эксплуатация Интернета вещей, а также оцениваются потенциальные последствия внедрения новых технологий в контексте информационной безопасности и необходимость разработки мер противодействия.

Ключевые слова: электрические устройства перехвата информации, классификация устройств перехвата, принципы работы устройств перехвата, аналого-цифровое преобразование, современные технологии перехвата, информационная безопасность.

Электрические устройства перехвата информации представляют собой специализированные технические средства, разработанные и применяемые для несанкционированного получения, копирования или анализа данных, передаваемых или хранящихся в электронном виде, охватывая широкий спектр технологий и методов, направленных на скрытое извлечение конфиденциальной информации из различных каналов связи и информационных систем. Классификация данных устройств может быть осуществлена по нескольким ключевым критериям, включая метод перехвата, тип перехватываемой информации, среду передачи данных и конструктивное исполнение, что позволяет выделить такие категории, как пассивные устройства, осуществляющие негласное прослушивание или наблюдение за информационными потоками без активного вмешательства в них, и активные устройства, которые могут внедряться в коммуникационные каналы или информационные системы для целенаправленного извлечения или модификации данных [3, 4].

В зависимости от типа перехватываемой информации выделяются устройства, предназначенные для перехвата голосовых данных (например, телефонные «жучки»), цифровых данных (например, снифферы сетевого трафика, кейлоггеры), видеоинформации (например, скрытые камеры с возможностью передачи данных), а также комбинированные устройства, способные осуществлять перехват различных типов данных одновременно.

С учетом среды передачи данных можно классифицировать устройства на предназначенные для перехвата информации в проводных каналах связи (например, устройства, подключаемые к телефонным линиям или Ethernet-кабелям) и в беспроводных каналах связи (например, устройства, перехватывающие Wi-Fi, Bluetooth или сотовую связь) [1].

Актуальность исследования данной темы в условиях современных угроз информационной безопасности обусловлена непрерывным ростом числа и сложности киберпреступлений, направленных на хищение конфиденциальных данных, нарушение функционирования информационных систем и нанесение значительного ущерба как отдельным лицам, так и организациям и государствам, что делает критически важным

глубокое понимание принципов действия, возможностей и методов противодействия электрическим устройствам перехвата информации для обеспечения надежной защиты информационного пространства.

В основе функционирования электрических устройств перехвата информации лежат фундаментальные принципы передачи и приема сигналов, которые обеспечивают возможность скрытого получения данных, циркулирующих в различных коммуникационных средах. Передача информации в большинстве современных электронных систем осуществляется посредством кодирования данных в физические сигналы, такие как электромагнитные волны, электрические токи или оптические импульсы, распространяющиеся по определенным каналам связи, будь то проводные соединения, беспроводное пространство или оптоволоконные линии [5].

Анализ физических основ передачи сигналов включает изучение характеристик этих сигналов, включая их частоту, амплитуду, фазу и поляризацию, а также особенностей их распространения в зависимости от среды и наличия препятствий, что позволяет определить оптимальные методы и технические средства для их приема и последующей обработки. Процесс приема сигналов начинается с улавливания энергии передаваемого сигнала при помощи соответствующих приемных устройств, таких как антенны для радиоволн, фотоприемники для оптических сигналов или специализированные электронные схемы для электрических токов, после чего принятый сигнал подвергается усилению и фильтрации для выделения полезной информации из фонового шума и помех.

Важным этапом в работе многих устройств перехвата информации, особенно применительно к современным цифровым системам связи, является изучение механизмов преобразования аналоговых сигналов в цифровые данные, поскольку большинство передаваемой информации, изначально представленной в аналоговой форме (например, голос, видео), для дальнейшей обработки, хранения и анализа в электронном виде подвергается дискретизации и квантованию [2].

Процесс аналого-цифрового преобразования (АЦП) включает несколько ключевых этапов: дискретизацию, в ходе которой непрерывный аналоговый сигнал измеряется через определенные промежутки времени с заданной частотой (частотой дискретизации), квантование, на этапе которого измеренные значения амплитуды сигнала округляются до ближайшего уровня из заданного набора дискретных уровней, и кодирование, в процессе которого каждому квантованному уровню присваивается уникальный цифровой код, обычно представленный в двоичной форме.

Качество и точность преобразования аналогового сигнала в цифровой формат напрямую зависят от частоты дискретизации и разрядности квантования, определяющих соответственно временное разрешение и амплитудное разрешение цифрового представления исходного сигнала, что является критически важным для устройств перехвата информации, стремящихся к максимально достоверному и полному извлечению передаваемых данных. Понимание этих фундаментальных принципов позволяет разработчикам устройств перехвата информации создавать высокоэффективные технические средства, способные незаметно получать и декодировать широкий спектр информационных сигналов, циркулирующих в современном информационном пространстве.

Одной из ключевых тенденций является дальнейшая миниатюризация электронных компонентов и развитие нанотехнологий, позволяющих создавать чрезвычайно компактные и легко скрываемые устройства перехвата, которые могут быть интегрированы практически в любые бытовые предметы или незаметно размещены в элементах инфраструктуры, значительно усложняя их обнаружение традиционными методами [1]. Параллельно наблюдается активное внедрение технологий искусственного интеллекта и машинного обучения в системы перехвата и анализа информации, что позволяет автоматизировать процессы выявления значимых данных в больших объемах перехваченного трафика, распознавать образы и речь с высокой точностью, а также обходить традиционные механизмы защиты путем адаптации к изменениям в поведении пользователей и сетевой активности.

Значительное влияние на развитие технологий перехвата оказывает распространение Интернета вещей (IoT), поскольку многочисленные подключенные устройства, зачастую обладающие недостаточным уровнем безопасности, становятся потенциальными точками проникновения в информационные системы и могут быть использованы для скрытого сбора и передачи данных [4]. Технологии программно-определяемого радио (SDR) предоставляют злоумышленникам гибкие и перенастраиваемые инструменты для перехвата различных видов радиосигналов, включая сотовую связь, Wi-Fi и Bluetooth, что позволяет адаптироваться к различным стандартам связи и частотным диапазонам без необходимости использования специализированного аппаратного обеспечения.

Оценка возможных последствий внедрения новых технологий перехвата информации в контексте информационной безопасности свидетельствует о значительном возрастании угроз и рисков. Повышение эффективности и скрытности устройств перехвата затрудняет их обнаружение и нейтрализацию, что может привести к увеличению числа успешных кибератак и утечек конфиденциальной информации. Расширение спектра потенциальных объектов для перехвата, включая устройства IoT, создает новые векторы атак и увеличивает поверхность уязвимости информационных систем. Развитие интеллектуальных систем анализа перехваченных данных позволяет злоумышленникам быстрее и эффективнее извлекать ценную информацию, что может иметь серьезные финансовые, репутационные и даже политические последствия.

В заключение следует отметить, что исследование электрических устройств перехвата информации позволило всесторонне рассмотреть их определение, классификацию, принципы работы и современные тенденции. Эти устройства представляют собой специализированные средства для несанкционированного получения данных, которые классифицируются по типу информации, методам внедрения и маскировки. Анализ работы устройств выявил ключевые аспекты их функционирования, подчеркнув важность понимания физических и технических основ для противодействия угрозам. Современные тенденции показывают рост сложности и скрытности атак, что делает исследование данной проблематики крайне актуальным в условиях роста киберпреступности.

Список литературы:

1. Власов, Н. Е. Разработка имитационной модели функционирования устройства радиоэлектронного поражения средств перехвата акустической информации / Н. Е. Власов, В. А. Щербаков // Интернаука. – 2024. – № 21-3 (338). – С. 64-69.

2. Гаманова, М. А. Способы защиты информации и предотвращения несанкционированного съема информации с помощью использования специальной аппаратуры / М. А. Гаманова, Д. С. Клюев, А. О. Фролов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): XI Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 15–16 февраля 2022 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. – С. 329-333.

3. Горлов, А. П. Анализ средства обнаружения закладного устройства «Сигнал-РМ» / А. П. Горлов, М. А. Шаманский // Новые горизонты: VIII научно-практическая конференция с международным участием. Сборник материалов и докладов, Брянск, 20 марта 2021 года. – Брянск: Брянский государственный технический университет, 2021. – С. 352-356.

4. Кругов, А. Г. Модели оценки защищенности информации от утечки за счет побочных электромагнитных излучений на объектах информатизации органов внутренних дел: диссертация на соискание ученой степени кандидата технических наук / Кругов Артём Геннадьевич, 2023. – 158 с.

5. Сосорева, А.И. Анализ физических эффектов в прослушивающих устройствах / А.И. Сосорева, В.И. Смирнов // Безопасность человека и устойчивое развитие общества перед вызовами глобальных трансформаций: Материалы международной междисциплинарной научной конференции. В 2-х частях, Йошкар-Ола, 03 декабря 2020 года / Под общей редакцией В.П. Шалаева. Том Часть 2. – Йошкар-Ола: Поволжский государственный технологический университет, 2021. – С. 158-161.