Хечиев Наран Валерьевич, студент
Краснодарское Высшее военное училище
им. Генерала-армии С.М Штеменко, г. Краснодар

Ахунов Салават Марселевич, студент
Краснодарское Высшее военное училище
им. Генерала-армии С.М Штеменко, г. Краснодар

Охотин Данил Александрович, студент
Краснодарское Высшее военное училище
им. Генерала-армии С.М Штеменко, г. Краснодар

Топанов Антон Сергеевич, студент
Краснодарское Высшее военное училище
им. Генерала-армии С.М Штеменко, г. Краснодар

Акишин Андрей Владимирович, доцент
Краснодарское Высшее военное училище
им. Генерала-армии С.М Штеменко, г. Краснодар

АНАЛИЗ ВОЗМОЖНЫХ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ ПРИ ФУНКЦИОНИРОВАНИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Аннотация: Данная работа посвящена анализу возможных каналов утечки информации по техническим каналам при функционировании объекта информатизации. Мы рассмотрим основные виды таких каналов, как электромагнитное излучение, акустические колебания, визуальные наблюдения и другие, проанализируем механизмы их функционирования и оценим потенциальные риски для различных типов ОИ.

Цель исследования – представить систематизированный обзор существующих угроз и предложить практические рекомендации по обеспечению безопасности информации в условиях потенциального воздействия технических каналов утечки.

Ключевые слова: Технические каналы утечки информации, объект информатизации, меры по защите от утечки информации по техническим каналам.

Термины и определения:

Информация – любые сведения (сообщения, данные) не зависимо от формы их представления [1].

Технические каналы утечки информации (ТКУИ) – пути распространения информации, возникающие в результате физических явлений, таких как электромагнитное излучение, акустические колебания, визуальное наблюдение и другие. В отличие от программных или организационных уязвимостей, ТКУИ используют физические свойства устройств и окружающей среды, что делает их особенно сложными для противодействия [8].

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [8].

Введение. В современном мире, характеризующемся стремительным развитием информационных технологий и повсеместным использованием цифровых систем, защита информации приобретает первостепенное значение. Объекты информатизации (ОИ), независимо от их масштаба и сферы деятельности, хранят и обрабатывают огромные объёмы

данных, многие из которых являются конфиденциальными и требуют надёжной защиты. Однако, наряду с программными и организационными уязвимостями, существуют физические, или технические, каналы утечки информации, которые часто остаются незамеченными и представляют серьёзную угрозу безопасности. Эти каналы основаны на физических процессах, сопровождающих работу компьютерных систем и коммуникационных сетей, и позволяют получить несанкционированный доступ к информации без прямого вмешательства в программное обеспечение.

Основные виды технических каналов утечки информации:

1. Электромагнитное излучение (ЭМИ):

• Побочные электромагнитные излучения и наводки (ПЭМИН): возникают при работе любого электронного устройства и могут содержать информацию об обрабатываемых данных. Мониторы, процессоры, принтеры, клавиатуры и другие устройства излучают электромагнитные волны, которые могут быть перехвачены на расстоянии с помощью специального оборудования. Например, содержимое экрана может быть восстановлено по электромагнитным излучениям монитора, а текст, набираемый на клавиатуре, – по излучениям её контроллера.

• Электрические наводки: информация может распространяться по электрическим цепям, таким как сети питания и линии связи, в виде наведенных сигналов. Подключение к этим цепям позволяет перехватывать конфиденциальную информацию.

• Радиочастотные идентификаторы (RFID): RFID-метки, используемые для идентификации и отслеживания объектов, могут передавать информацию по радиоканалу, которая может быть перехвачена злоумышленниками.

2. Акустические каналы:

• Акустические колебания (речевая информация): разговоры, происходящие в помещении, могут быть записаны с помощью микрофонов, диктофонов и даже лазерных микрофонов, которые улавливают вибрацию оконных стёкол.

• Виброакустические каналы: вибрации, возникающие при работе устройств, таких как принтеры и клавиатуры, могут распространяться по твердым телам (стенам, столам, трубам) и передавать информацию о выполняемых действиях. Для извлечения этой информации можно использовать специальные датчики вибрации.

3. Визуальные каналы:

• Наблюдение: подглядывание через окна, двери, видеокамеры позволяет злоумышленникам следить за действиями пользователей и содержимым их экранов.

• Оставленные документы и носители информации: забытые распечатки, USB-накопители и жесткие диски могут стать источником утечки конфиденциальных данных.

4. Иные каналы:

• Термографические каналы: тепловое излучение от работающих устройств может быть использовано для получения информации об их состоянии и активности. Например, тепловизор может показать, какие устройства в помещении работают и насколько интенсивно.

• Утечка через сети питания и заземления: паразитные токи и напряжения, возникающие в процессе работы оборудования, могут содержать информацию о его работе. Анализируя эти параметры в электрической сети, злоумышленники могут получить конфиденциальные данные.

Факторы, влияющие на уязвимость объекта к ТКУИ:

• Тип обрабатываемой информации: чем более конфиденциальна и ценна информация, тем выше риск утечки.

• Тип оборудования: Уровень излучения, чувствительность к внешним воздействиям.

• Физическое расположение объекта: доступность помещений, наличие слабых мест в защите периметра.

- Уровень защиты: наличие и эффективность мер по противодействию ТКУИ.
- Квалификация персонала: осведомленность о рисках и мерах защиты.

Меры по защите от утечки информации по техническим каналам:

- Экранирование: использование специальных материалов и конструкций для ослабления электромагнитного излучения и наводок.
- Маскировка: добавление помех и шумов в излучение для затруднения его перехвата.
- Фильтрация: применение фильтров для подавления нежелательных частот в электрических цепях.
- Заземление: организация правильной системы заземления для минимизации наводок.
- Контроль доступа: ограничение доступа в помещения, где обрабатывается конфиденциальная информация.
- Криптография: Шифрование данных при передаче и хранении.
- Регулярные проверки: проведение проверок для выявления каналов утечки и оценки эффективности принятых мер.
- Обучение персонала: повышение осведомленности сотрудников о рисках и методах защиты от ТКУИ.
- Применение специальных средств защиты: генераторы шума, подавители электромагнитного излучения, средства виброакустической защиты.

Заключение:

Анализ ТКУИ является неотъемлемой частью комплексной защиты информации на объекте информатизации. Игнорирование этих каналов может привести к серьезным последствиям, включая утечку конфиденциальных данных, финансовые потери и репутационные риски. Для эффективной защиты необходимо регулярно анализировать угрозы, разрабатывать и внедрять соответствующие меры, а также постоянно повышать осведомленность персонала. Только комплексный подход позволит обеспечить надежную защиту информации от утечек по техническим каналам.

Список литературы:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Доктрина информационной безопасности, утвержденная Указом Президента РФ от 5 декабря 2016 года №646.
3. ГОСТ Р 50940-96 Защита информации. Средства защиты информации. Общие технические требования.
4. Сизоненко А.Б., Алиманов П.Е. Модель организационно-штатного обеспечения подразделений защиты информации / Вестник Воронежского института МВД России 2020 г.
5. Федеральный закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».
6. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. – М.: Горячая линия – Телеком, 2016. – 909 с.
7. Ищейнов, В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. Учебное пособие / В.Я. Ищейнов. – М.: Форум, 2018. – 188 с.
8. Рекомендации по стандартизации Р 50.1.056 – 2005 «Техническая защита информации. Основные термины и определения», утверждены Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479.