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

Енин Дмитрий Николаевич, 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

Носенко Валентин 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

СУЩЕСТВУЮЩИЕ ПРОГРАММНЫЕ СРЕДСТВА ПОДДРЕЖКИ ПРИНЯТИЯ РЕШЕНИИЙ ДОЛЖНОСТНЫМИ ЛИЦАМИ ПОДРАЗДЕЛЕНИЙ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ПРИ ВЫЯВЛЕНИИ ВОЗМОЖНЫХ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ.

Аннотация: Настоящая статья посвящена обзору существующих программных средств, применяемых для поддержки принятия решений должностными лицами технической защиты при выявлении возможных каналов утечки информации на объекте информатизации.

Ключевые слова: Технические каналы утечки информации, объект информатизации, система поддержки принятия решений, техническая защита.

Термины и определения:

Техническая защита информации – Деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [1].

Система поддержки принятия решений (СППР) – компьютерная автоматизированная система, целью которой является помощь людям, принимающим решения в сложных условиях для полного и объективного анализа предметной деятельности [7].

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.

Введение. В условиях растущих угроз информационной безопасности, вызванных развитием технологий и усложнением методов атак, эффективная защита объектов информатизации (ОИ) от утечки конфиденциальной информации является критически важной задачей. Одним из наиболее коварных способов утечки является использование технических каналов, которые эксплуатируют физические свойства устройств и окружающей среды. Для своевременного выявления и нейтрализации этих угроз подразделения технической защиты (ПТЗ) нуждаются в современных инструментах, обеспечивающих поддержку принятия решений (СППР).

Роль СППР в деятельности ПТЗ:

Процесс выявления технических каналов утечки информации (ТКУИ) является сложным и многогранным, требующим глубоких знаний, опыта и специального оборудования. СППР призваны автоматизировать и упростить этот процесс, предоставляя должностным лицам ПТЗ необходимую информацию, аналитические данные и инструменты для принятия обоснованных решений. Основные задачи СППР:

- **Сбор и анализ данных:** автоматизированный сбор информации об ОИ, включая его состав, топологию, технические характеристики оборудования, электромагнитное излучение, акустические свойства помещений и др.
- **Идентификация уязвимостей:** анализ собранных данных для выявления потенциальных уязвимостей, таких как ПЭМИН, наводки, акустические каналы, визуальное наблюдение и т. д.
- **Оценка рисков:** определение вероятности реализации угроз и потенциального ущерба от утечки информации.
- **Формирование рекомендаций:** выдача рекомендаций по устранению уязвимостей и реализации мер защиты.
- **Визуализация:** представление данных и результатов анализа в наглядной и понятной форме.
- **Отчетность:** Формирование отчетов о проведенном анализе и принятых мерах.

Существующие программные средства:

Программные средства, используемые для поддержки принятия решений в ПТЗ, можно разделить на несколько категорий:

1. Системы мониторинга и анализа электромагнитного излучения (СЭМИ):
   - Предназначены для обнаружения и анализа ПЭМИН, излучаемых электронными устройствами.
   - Включают в себя программное обеспечение для управления приёмным оборудованием, обработки полученных сигналов, анализа спектральных характеристик и идентификации источников излучения.
   - **Примеры:** ПО для управления спектроанализаторами, ПО для построения карт электромагнитного фона.
2. Системы анализа акустических характеристик:
   - Позволяют измерять и анализировать уровень шума и вибрации в помещениях.
   - Используются для выявления акустических и виброакустических каналов утечки.
   - **Примеры:** ПО для анализа звуковых записей, ПО для обработки данных с датчиков вибрации.
3. Системы моделирования и анализа защищенности ОИ:
   - Позволяют создавать цифровые модели объектов инфраструктуры и анализировать их уязвимости с учетом различных факторов, включая архитектуру, электромагнитную совместимость, акустические характеристики и т. д.
   - Используются для прогнозирования потенциальных каналов утечки и оценки эффективности мер защиты.
   - **Примеры:** САПР для проектирования защищенных объектов, ПО для моделирования распространения ЭМИ.
4. Системы управления информационной безопасностью (СУИБ):
   - Комплексные платформы, объединяющие функции управления рисками, анализа уязвимостей, контроля доступа, мониторинга событий безопасности и др.
   - Могут включать в себя модули для анализа ТКУИ и интеграции с другими специализированными средствами.
   - **Примеры:** решения от IBM, Oracle, SAP и др., а также специализированные решения по защите информации.

5. Специализированные средства анализа ТКУИ:

○ Инструменты, разработанные специально для выявления и анализа определенных видов технических каналов утечки.

○ **Примеры:** программное обеспечение для анализа наводок в электрических цепях, инструменты для перехвата и анализа RFID-сигналов, ПО для анализа изображений, полученных с помощью тепловизоров.

Принципы выбора программного обеспечения:

При выборе программных средств для обеспечения поддержки принятия решений в ПТЗ необходимо учитывать следующие факторы:

- **Функциональность:** Набор предоставляемых функций и возможностей.
- **Точность и надежность:** Достоверность получаемых результатов.
- **Простота использования:** Интуитивно понятный интерфейс и удобство работы.
- **Интеграция:** Возможность интеграции с другими системами и средствами защиты информации.
- **Стоимость:** Соотношение цены и качества.
- **Сертификация:** Наличие сертификатов соответствия требованиям безопасности.

Проблемы и перспективы развития:

Несмотря на наличие разнообразных программных средств, существует ряд проблем, которые необходимо учитывать при их использовании:

- **Сложность:** многие системы сложны в настройке и использовании, что требует от персонала высокой квалификации.
- **Высокая стоимость:** Специализированные решения могут быть дорогостоящими.
- **Ограниченные возможности:** некоторые средства не охватывают все виды ТКУИ.
- **Постоянное развитие угроз:** требуется постоянное обновление программного обеспечения и баз данных.

Перспективы развития СППР в области технической защиты связаны с:

- **Автоматизация процессов анализа:** использование искусственного интеллекта и машинного обучения для автоматизации задач по сбору данных, выявлению уязвимостей и оценке рисков.
- **Разработкой более интегрированных решений:** созданием единых платформ, объединяющих различные функции и инструменты для анализа ТКУИ.
- **Улучшение визуализации данных:** представление результатов анализа в наглядной и понятной форме для упрощения принятия решений.
- **Повышение точности и надежности результатов:** разработка более совершенных алгоритмов анализа и обработки данных.

Заключение:

Программные средства играют ключевую роль в обеспечении поддержки принятия решений должностными лицами подразделений технической защиты при выявлении возможных технических каналов утечки информации на объекте информатизации. Существует широкий спектр специализированных решений, позволяющих автоматизировать процессы сбора данных, идентификации уязвимостей, оценки рисков и формирования рекомендаций. Однако для эффективного использования этих средств требуется их грамотный выбор, настройка и применение, а также постоянное отслеживание новых угроз и развитие технологий защиты. Дальнейшее развитие программных средств в этой области связано с автоматизацией процессов анализа, интеграцией решений и улучшением визуализации данных, что позволит повысить эффективность защиты объектов информатизации от утечки информации по техническим каналам.

Список литературы:

1. 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.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне».

4. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» от 12.05.1999.

5. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 № 282.

6. Стародубцев А.А. Система поддержки принятия решений / Актуальные проблемы авиации и космонавтики 2016 г.

7. Карташов Г. П. Классификация систем поддержки принятия решений для использования в системе управления событиями и информацией о безопасности / Г.П. Карташов, Е. К. Корбин. – Текст: непосредственный // Молодой ученый. – 2023. – № 37 (484). – С. 9-11. –