Лекция 3. Комплексный подход к защите информации

1. Инженерно-техническая защита информации.
2. Криптографическая защита информации.
3. Программно-аппаратная защита информации.

Инженерно-технические средства защиты информации

Физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства.

Назначение инженерно-технических средств защиты информации

- защита территории и помещений КС от проникновения нарушителей;
- защита аппаратных средств КС и носителей информации от хищения;
- предотвращение возможности удаленного (из-за пределов охраняемой территории) видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств КС;

Назначение инженерно-технических средств защиты информации

- предотвращение возможности перехвата ПЭМИН, вызванных работающими техническими средствами КС и линиями передачи данных;
- организация доступа в помещения КС сотрудников организации;
- контроль над режимом работы персонала КС;
- контроль над перемещением сотрудников КС в различных производственных зонах;
- противопожарная защита помещений КС;
- минимизация материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий.

Технические средства охраны

Образуют первый рубеж защиты КС и включают в себя:

- средства контроля и управления доступом (СКУД);
- средства охранной сигнализации;
- средства видеонаблюдения (охранного телевидения, CCTV).

Методы и средства защиты информации от утечки по каналам ПЭМИН

Основным направлением является уменьшение соотношения «сигнал/шум» в этих каналах до предела, при котором восстановление информации становится принципиально невозможным. Возможные решения:

- снижение уровня излучений сигналов в аппаратных средствах КС;
- увеличение мощности помех в соответствующих этим сигналам частотных диапазонах.

Методы и средства защиты информации от утечки по каналам ПЭМИН

- Создание технических средств КС в «защищенном» исполнении, а также рациональный выбор места размещения этих средств относительно мест возможного перехвата ПЭМИН.
- Применение активных средств защиты в виде генераторов «сигналоподобных» помех или шума.

Генераторы шума

Методы и средства защиты информации от утечки по каналам ПЭМИН

- замена в информационных каналах КС электрических цепей волоконно-оптическими линиями;
- локальное экранирование узлов технических средств, являющихся первичными источниками информационных сигналов;
- включение в состав информационных каналов КС устройств предварительного шифрования обрабатываемой информации.

Средства обнаружения электронных подслушивающих устройств

- Нелинейные локаторы, которые с помощью специального передатчика в сверхвысокочастотном диапазоне радиоволн облучают окружающее пространство и регистрируют вторичный, переизлученный сигнал, поступающий от различных полупроводниковых элементов, находящихся как во включенном, так и в выключенном состоянии.

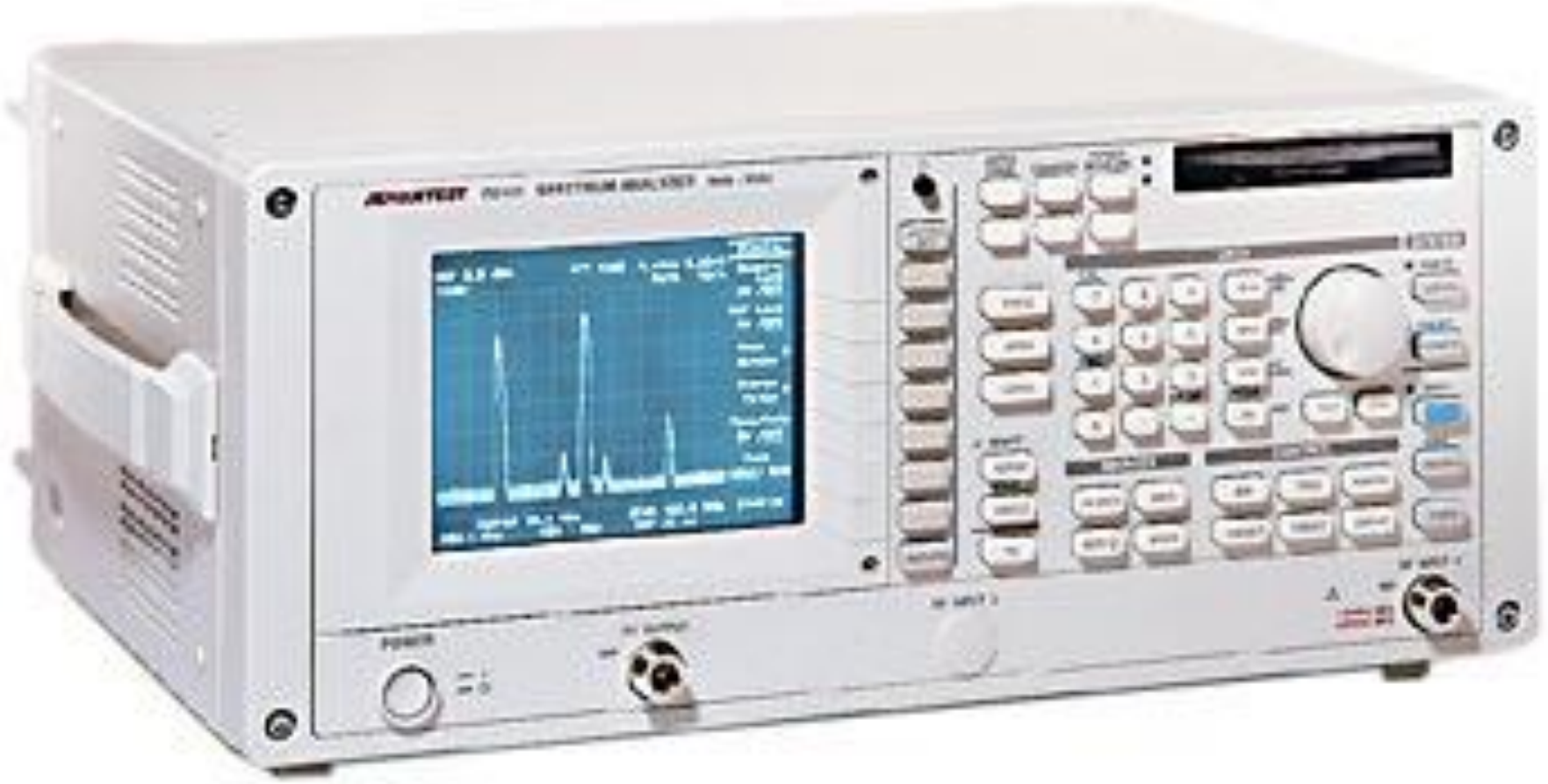
Нелинейный локатор

Средства обнаружения электронных подслушивающих устройств

- Нелинейные локаторы могут не выявить радиозакладное устройство, если оно вмонтировано в электронное устройство (системный блок компьютера, телевизор, телефонный аппарат и т.п.). В этом случае потребуется применение более сложных устройств контроля постороннего радиоизлучения – сканирующих приемников, компьютерных анализаторов спектра.

Сканирующий приемник

Анализатор спектра



Основы криптографической защиты информационных ресурсов

- К открытому тексту применяется функция шифрования, в результате чего получается шифротекст (или криптограмма).
- Для восстановления открытого текста из шифротекста к последнему применяется функция расшифрования.

Шифрование и расшифрование

Функции шифрования (E) и расшифрования (D) используют один или более дополнительных параметров, называемых ключом:

$$E_k$$

P (открытый текст)--> C (шифротекст)

$$D_{k'}$$

C (шифротекст) --> P (открытый текст)

$$C=E_k(P);\ P=D_{k'}(C)$$

Виды криптографических систем

- Если ключ шифрования K совпадает с ключом расшифрования K’, то такую криптосистему называют симметричной; если для шифрования и расшифрования используются разные ключи, то такую систему называют асимметричной.
- В симметричной криптосистеме ключ должен быть секретным; в асимметричной системе один из ключей может быть открытым.

Виды криптографических ключей

- Ключ симметричного шифрования обычно называют сеансовым (session key).
- Пару ключей асимметричного шифрования образуют открытый ключ (public key) и личный (или закрытый) ключ (secret key, private key).

Криптография и криптоанализ

- Науку о защите информации с помощью шифрования называют *криптографией*.
- Процесс получения открытого текста из шифротекста без знания ключа расшифрования называют обычно *дешифрованием* (или ««взломом» шифра), а науку о методах дешифрования – *криптоанализом*.
- Совместным изучением методов криптографии и криптоанализа занимается *криптология*.

Криптостойкость

Характеристика надежности шифротекста от вскрытия называется *криптостойкостью*. Криптостойкость шифра может оцениваться двумя величинами:

- минимальным объемом шифротекста, статистическим анализом которого можно его вскрыть и получить открытый текст без знания ключа;
- количеством MIPS-часов или MIPS-лет – времени работы условного криптаналитического компьютера производительностью один миллион операций в секунду, необходимой для вскрытия шифротекста.

Применение криптографических методов защиты информации

- Обеспечение конфиденциальности информации, передаваемой по открытым линиям связи или хранящейся на открытых носителях информации.
- Аутентификация, обеспечение целостности и неоспоримости передаваемой информации.
- Защита информационных ресурсов от несанкционированного использования.

Хеширование информации

- *Хешированием* информации называют процесс ее преобразования в хеш-значение фиксированной длины (дайджест, образ, хеш-код или просто хеш).

Понятие функции хеширования

- Односторонняя функция
- Для любого документа M длина его хеш-значения H(M) постоянна.
- Минимальная вероятность коллизий
- Сложность нахождения другого документа с тем же хеш-значением.

$$\neg\exists H^{-1} H^{-1}(H(M)) = M$$

$$p(H(M') = H(M) \mid M' \neq M) \leq p_{\max}$$

Применение функций хеширования

- Хранение образов паролей пользователей компьютерных систем в регистрационных базах данных.
- Генерация одноразовых паролей и откликов на случайные запросы службы аутентификации.
- Генерация сеансовых ключей из парольных фраз.
- Обеспечение подлинности и целостности электронных документов.

Аппаратные средства защиты информации

Электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не инженерно-техническим средствам защиты является именно обязательное включение в состав технических средств КС.

Основные аппаратные средства защиты информации

- устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.);
- устройства для хранения идентифицирующей пользователя информации (карты, генераторы одноразовых паролей, элементы Touch Memory и т. п.);
- устройства для шифрования информации;
- устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Аппаратные шифраторы

Вспомогательные аппаратные средства защиты информации

- устройства уничтожения информации на электронных носителях;
- устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Устройство для быстрого уничтожения информации на жестких магнитных дисках

Программные средства защиты информации

Специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций. К основным программным средствам защиты информации относятся:

- программы идентификации и аутентификации пользователей КС;
- программы разграничения доступа пользователей к ресурсам КС;
- программы шифрования информации;
- программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т.п.) от несанкционированного изменения, использования и копирования.

Идентификация и аутентификация

- Под *идентификацией*, применительно к обеспечению информационной безопасности КС, понимают однозначное распознавание уникального имени субъекта КС (проверка его регистрации в системе).
- *Аутентификация* при этом означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).

Вспомогательные программные средства защиты информации

- программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т.п.);
- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановить и доказать факт происшествия этих событий;
- программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);
- программы тестового контроля защищенности КС и др.

Преимущества и недостатки программных средств защиты информации

- Простота тиражирования.
- Гибкость.
- Простота использования.
- Неограниченные возможности развития.

- Расходование ресурсов компьютерных систем.
- Возможность обхода (из-за «пристыкованности»).
- Возможность злоумышленного изменения.