Запорожский национальный технический университет

Методы и технические средства обнаружения технических каналов утечки информации

Студенты гр. РТ-715
Ефименко М.М, Слива А.М

Научный руководитель
к.т.н., доц.Воскобойник В.А.

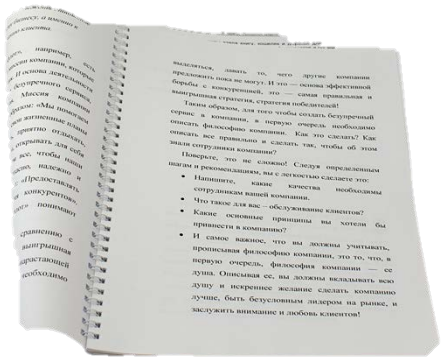
ПЛАН

1. Технические каналы утечки информации
2. Методы обнаружения
3. Технические средства обнаружения

Технические каналы утечки информации

Информация может быть представлена в различной форме и на различных физических носителях. Основными носителями информации, представляющими интерес с точки зрения защиты, являются:

- документальная;
- акустическая (речевая);
- телекоммуникационная и т.п.



Основными объектами защиты информации являются:

- ❖ информационные ресурсы, содержащие сведения, отнесенные к государственной тайне и конфиденциальную информацию;
- ❖ системы и средства, непосредственно обрабатывающие информацию, отнесенную к государственной тайне, а также конфиденциальную информацию. Эти средства и системы часто называют техническими средствами приема, обработки, хранения и передачи информации (ТСПИ);
- ❖ технические средства и системы, не относящиеся к средствам и системам информатизации (ТСПИ), но размещенные рядом с ними в одном помещении. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС).

Методы обнаружения

Получение доступа к аудиоинформации в подавляющем большинстве случаев сопряжено либо с внедрением специального технического средства, либо с перехватом сигналов (оптических, электромагнитных, виброакустических и т.д.). Наличие посторонних элементов является демаскирующим признаком. Демаскирующие признаки бывают следующие:

- инородное тело;
- следы установки;
- посторонние сигналы;

Каналами утечки информации являются:

- радиоканал;
- проводные коммуникации;
- оптический канал;
- виброакустический канал;
- высокочастотное навязывание.

Технические средства обнаружения

Поисковые мероприятия техническими средствами проводятся в местах, где возможна утечка конфиденциальной информации (кабинетах руководства, помещениях для переговоров, в загородных резиденциях, саунах, автомобилях) для своевременного обнаружения каналов утечки информации и ликвидации угрозы ее перехвата.

Задача поискового мероприятия:

- определение состояния информационной безопасности объекта;
- поиск каналов утечки информации;
- поиск установленных приборов и систем перехвата и передачи информации;
- выдача рекомендаций по оптимальным способам блокирования каналов утечки информации.

Поисковые мероприятия проводятся периодически по разработанным руководством службы безопасности календарным планам, или носят внеплановый (профилактический или превентивный) характер.

В случаях, когда становится очевидным, что на объекте имеется утечка информации, проводится конспиративная "чистка", наиболее трудоемкий вид поисковых мероприятий, требующий большой подготовительной работы сотрудников поискового подразделения. Основной задачей в этом случае является не только обнаружение каналов утечки информации (прослушивающих устройств), но и сохранение проводимых мероприятий в тайне. Плановые "чистки" проводятся периодически по графику.

Существуют четыре уровня "глубины чисток" (обусловленные набором применяющихся поисковых средств):

Первый уровень - обнаружение радиоизлучающих устройств в проверяемых помещениях и в смежных с ними. К ним относятся радиомикрофоны, телефонные радиопередатчики, установленные в телефонном аппарате или на линии.
Второй уровень - обнаружение устройства "первого уровня", а также передатчики, использующие в качестве канала передачи информации сеть 220В
Третий уровень - обнаружение изделий второго уровня, а также все типы кабельных микрофонных систем. Кроме того, выявляется оргтехника, работающая в режиме передачи за границы зоны охраны сигнала, содержащего полезную информацию.

Четвертый уровень - теоретически могут быть обнаружены все типы заносных и закладных электронных средств перехвата информации и естественные каналы ее утечки. При всей эффективности "чистки" четвертого уровня следует понимать все сложности, связанные с ее проведением (время, людские ресурсы, техническое обеспечение и т.д.). "Чистка" четвертого уровня проводится крайне редко: в основном, после переезда в новое здание или после капитального ремонта. Связано это с тем, что большинство типов подслушивающей техники, обнаруживающейся только на четвертом уровне, может быть установлено на объекте именно на этапе ремонта или реконструкции. Для этого требуется много времени и полная свобода передвижения по объекту.

Примеры приборов выявления

Современные технические средства обнаружения и выявления Устройств несанкционированного снятия информации:
Индикаторы поля:SELP SP 221 «Спутник», SELP SP 223 «Pandora», Утес, Вымпел, ST 107+, Bug Hunter.
Технические средства радиомониторинга: SEL SP-81R «Оракул», SEL SP-9000, Oskor-5000E, ПС-6000М, Омега, АКОР.
Частотомеры: Scout, Digital Scout, CUB, X-sweeper.
Контроль проводных линий: КПЛ, УЛАН-2, TALAN, ПДК 01.
Универсальные поисковые приборы: СРМ-700 «АКУЛА».
Обнаружители видеокамер:SEL SP-101 "Аркан", Оптик, Гранат, Hubble, Чистильщик.
Нелинейные локаторы: ЛЮКС, Лорнет, NR-900EMS, ORION NJE-4000, Буклет-2, Родник-23К.