ТЕМА № 3

«Дестабилизирующее воздействие и несанкционированный доступ к информации»

ЗАНЯТИЕ 2/3.

«КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ »

ЦЕЛЬ ЗАНЯТИЯ:

1. Изучить каналы утечки информации.
2. Обучить определять соотношения между каналами и источниками.
3. Воспитывать высокие морально-психологические и профессиональные качества, твердую и непоколебимую уверенность в своем оружии и военной технике, чувство превосходства своих ВС

Учебные вопросы.

1. Каналы утечки информации и источники воздействия на информацию, связанные с людьми.

2. Технические каналы утечки информации и источники воздействия на информацию.

1-й учебный вопрос

Каналы утечки информации и источники воздействия на информацию, связанные с людьми.

Самым распространенным, многообразным по методам несанкционированного доступа, а потому и самым опасным каналом является ***установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации.***(*первый канал*)

Методы несанкционированного доступа к информации:

- выведывание информации под благовидным предлогом (использование собеседника втемную);
- метод переманивания сотрудников;
- метода покупки конфиденциальной информации;
- принуждение к выдаче конфиденциальной информации шантажом;
- склонение к выдаче конфиденциальной информации.

С ростом промышленного шпионажа все более опасным каналом становится ***вербовка и внедрение агентов.****(второй канал)*

Третий канал — ***организация физического проникновения*** к носителям конфиденциальной информации ***сотрудников разведывательных служб*** включает два этапа:

- проникновение на территорию (в здания) охраняемого объекта;
- проникновение к носителям конфиденциальной информации.

При проникновении на территорию объекта возможно применение следующих ***методов***:

— использование подложного, украденного или купленного (в том числе и на время) пропуска;

— маскировка под другое лицо, если пропуск не выдается на руки;

— проход под видом внешнего обслуживающего персонала;

— проезд спрятанным в автотранспорте;
— отвлечение внимания охраны для прохода незамеченным (путем создания чрезвычайных ситуаций, с помощью коллеги и т. д.);
— изоляция или уничтожение охраны (в редких, чрезвычайных обстоятельствах);
— преодоление заграждающих барьеров (заборов), минуя охрану, в том числе и за счет вывода из строя технических средств охраны.

Проникновение к носителям конфиденциальной информации может осуществляться:

- путем взлома дверей хранилищ и сейфов (шкафов) или их замков, через окна;
- с отключением (разрушением) сигнализации, телевизионных средств наблюдения (если проникновение производится в нерабочее время);

методов.

- путем прохода в комнаты исполнителей работающих с конфиденциальными документами, в производственные и складские помещения для осмотра технологических процессов и продукции, а также в помещения, которых производится обработка информации (при проникновении в рабочее время);
- во время транспортировки носителей конфиденциальной информации , с использованием, в зависимости от вида, условий и маршрута транспортировки, соответствующих

2-й учебный вопрос:

«Технические каналы утечки информации и источники воздействия на информацию»

Подключение к средствам отображения, хранения, работки, воспроизведения и передачи информации, средства связи (*четвертый канал несанкционированного доступа к конфиденциальной информации)* может осуществляться лицами, находящимися на территории объекта и вне ее. Несанкционированное подключение, а следовательно, и несанкционированный доступ к конфиденциальной информации может производиться:

— с персонального компьютера с использованием телефонного набора или с несанкционированного терминала со взломом парольноключевых систем защиты или без взлома с помощью маскировки под зарегистрированного пользователя;

— с помощью программных и радиоэлектронных закладных устройств;

— с помощью прямого присоединения к кабельным линиям связи, в том числе с использованием параллельных телефонных аппаратов;

— за счет электромагнитных наводок на параллельно проложенные провода или методов высокочастотного навязывания.

Пятый канал — ***прослушивание речевой конфиденциальной информации*** чаще всего осуществляется по двум направлениям:

— подслушивание непосредственных разговоров лиц, допущенных к данной информации;

— прослушивание речевой информации, зафиксированной на носителе, с помощью подключения к средствам ее звуковоспроизведения.

Визуальный съем конфиденциальной информации (*шестой канал несанкционированного доступа к ней*) может осуществляться следующими методами:

— чтением документов на рабочих местах пользователей (в том числе с экранов дисплеев, с печатающих Устройств) в присутствии пользователей и при их отсутствии;

— осмотром продукции, наблюдением за технологическим процессом изготовления продукции;

— просмотром информации, воспроизводимой средствами видеовоспроизводящей техники и телевидения;

— чтением текста, печатаемого на машинке и размножаемого множительными аппаратами;

— наблюдением за технологическими процессами изготовления, обработки, размножения информации;

— считыванием информации в массивах других пользователей, в том числе чтением остаточной информации.

Перехват электромагнитных излучений (*седьмой канал*)

включает в себя перехват техническими средствами как функциональных сигналов, так и особенно побочных создаваемых техническими средствами отображения, хранения, обработки, воспроизведения, передачи информации средствами связи, охранной и пожарной сигнализации системами обеспечения функционирования этих средств техническими средствами технологических процессов на которых промышленных объектов, образцами вооружение и военной техники, вспомогательными электрическими радиоэлектронными средствами (электрическими часами бытовыми магнитофонами, видеомагнитофонами, радиоприемниками, телевизорами).

Этот канал имеет, по сравнению с другими каналами, преимущества:

- большой объем и высокая достоверность получаемой информации,
- оперативность ее получение,
- возможность съема в любое время,
- скрытность получения, возможность обнародования без угрозы перекрытия канала.

Методами, применяемыми при использовании *восьмого канала* — ***исследование выпускаемой продукции, производственных отходов и отходов процессов обработки информации*** — могут быть:

— приобретение и разработка (расчленение, выделение отдельных составных частей, элементов) выпускаемых изделий, их химический и физический анализ (обратный инжиниринг) с целью исследования конструкции, компонентов и других характеристик;

— сбор и изучение поломанных изделий, макетов изделий, бракованных узлов, блоков, устройств, деталей, созданных на стадии опытно-конструкторских разработок, а также руды и шлаков, позволяющих определить состав материалов, а нередко и технологию изготовления продукции;

— сбор и прочтение черновиков и проектов конфиденциальных документов, копировальной бумаги, красящей ленты печатающих устройств, прокладок, испорченных магнитных дискет.

Использование *девятого канала*— ***изучение доступных источников информации, из которых можно получить конфиденциальные сведения***, — осуществляется путем:

— изучения научных публикаций, содержащихся в специализированных журналах (сборниках);

— просмотра (прослушивания) средств массовой информации (газет, журналов, теле- и радиопередач);

— изучения проспектов и каталогов выставок;

— прослушивания публичных выступлений на семинарах, конференциях и других публичных мероприятиях;

— изучения формируемых специализированными коммерческими структурами банков данных о предприятиях.