Тема 12. Мероприятия по выявлению каналов утечки информации

Занятие 1. Характеристика особенностей мероприятий по выявлению каналов утечки информации на основе проведения специального обследования и специальной проверки

Учебные вопросы:

- 1. Организация и порядок проведения специальной проверки ТСПИ и ВТСС
- 2. Организация и порядок проведения специального обследования объекта информатизации

Литература

- Хорев А.А. Способы и средства защиты информации: Учеб. пособие. – М.: МО РФ, 2000.
- Бузов Г. А. и д.р. Защита от утечки информации по техническим каналам. М.: Горячая линия-Телеком, 2005.
- Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь. – М.: НОУ ШО Баярд, 2004.
- Торокин А.А. Основы инженерно-технической защиты информации. – М.: Гелиус, 2005.

Первый учебный вопрос: Организация и порядок проведения специальной проверки

Виды исследований по выявлению технических каналов утечки информации:

- специальные проверки (СП);
- специальные обследования (СО);
- специальные исследования (СИ).

Понятие специальная проверка

Специальная проверка - это комплекс инженерно-технических мероприятий, проводимых с использованием необходимых, в том числе и специализированных технических средств, направленных на исключение перехвата технической разведкой информации, содержащей сведения, составляющие государственную тайну, с помощью внедренных в защищаемые технические средства и изделия специальных электронных закладочных устройств.

- **Специальные проверки** технических средств и систем (ТСС) проводятся с целью:
- выявления возможно внедренных электронных средств съема информации в ТСС;
- выявления схемотехнических и иных доработок ТСС, приво дящих к усилению естественных свойств ТСС;
- выявления «программных» закладок в ТСС, имеющих процессорное управление.

Порядок проведения специальной проверки технических средств

- **Первый этап**: - Прием-передача технического средства, формирование исходных данных для составления программы проведения специальной проверки;
- **Второй этап**: - Разработка программы проведения специальной проверки технического средства;
- **Третий этап**: - Проведение технических проверок;
- **Четвертый этап**: - Анализ результатов специальной проверки, оформление отчетных документов.

Первый этап

- В орган проверки представляются:

1. Технические средства в полной комплектации, штатной упаковке, в исправном состоянии (по акту приема-передачи)
2. Исходные данные, необходимые для разработки программы проведения специальной проверки:

- данные о техническом средстве;
- данные о его планируемом применении;
- данные о месте размещения технического средства.

3. Дополнительные данные, способствующие составлению перечня специальных электронных устройств, возможно внедренных в техническое средство

В результате анализа исходных данных, конструктивно-технических принципов построения и на основе классификации специального электронного устройства определяется перечень естественных каналов утечки информации и возможно внедренных в техническое средство специальных электронных устройств.

Исходные данные, необходимые для разработки программы проведения специальной проверки

Данные о техническом средстве включают в себя:

- сведения о его назначении и полной комплектации;
- комплект документов на техническое средство;
- способ приобретения;
- сведения об организации или предприятии, в котором приобретено техническое средство.

Данные о планируемом применении должны отвечать на вопросы:

- планируется ли техническое средство для обработки закрытой информации (для размещения в помещении, где циркулирует закрытая речевая информация);
- есть ли высший гриф секретности обрабатываемой (обсуждаемой) информации;
- в составе какой системы (или самостоятельно) планируется применение технического средства;

к каким коммуникационным системам планируется его подключение.

Данные о планируемом месте размещения технических средств включают в себя:

- описание объекта, на котором планируется размещение технического средства; перечень охраняемых сведений объекта;
- минимальное расстояние до границы контролируемой зоны (КЗ);
- размещение посольств, представительств и иных мест постоянного или временного пребывания иностранных граждан по отношению к КЗ;
- возможность и периодичность пребывания иностранных делегаций на

Второй этап

- Составляется программа проведения специальной проверки технического средства, которая определяет порядок выявления демаскирующих признаков СЭУ и их непосредственное выявление

Третий этап

- Типовой набор операций при проведении технических проверок включает:
- дозиметрический контроль изделия в таре для обнаружения радиоактивных меток и радиоизотопных источников питания;
- вихретоковый контроль объектов (узлов) технических средств обработки и передачи информации, не содержащих металлических элементов;
- контроль тары, не имеющей полупроводниковых элементов;
- проведение радиоконтроля;
- проверка возможности осуществления высокочастотного навязывания элементам ТСПИ;
- разборка технического средства, осмотр его элементов и узлов с целью выявления отклонений в схемотехнических и конструктивных решениях;
- электротехнические измерения параметров элементов и узлов технических средств с целью выявления демаскирующих признаков СЭУ;
- контроль элементов и узлов технических средств, не содержащих полупроводниковых элементов, (нелинейная локация, рентгеноскопический или рентгенографический контроль);
- рентгенография или рентгеноскопия элементов и узлов технического средства с целью выявления схемных изменений в элементах и неразборных узлах технического средства;
- дешифрация рентгеновских снимков и проведение визуально-оптического контроля внешнего вида и внутренней структуры узлов и элементов технических средств;
- сборка технического средства и контроль работоспособностиция, утечка разглашение которой может нанести экономический ущерб предприятию.

Четвертый этап

- **После проведения специальной проверки:**

1. Проверенное техническое средство и оборудование маркируется (опечатывается) по специальной методике.

2. Формирование библиотеки эталонных рентгенограмм типовых элементов технических средств, фотографий узлов и формирование стендов (рабочих мест) по направлениям технического контроля.

3. По результатам анализа руководитель рабочей группы делает вывод об отсутствии (наличии) в составе технического средства СЭУ.

4. По результатам проведенных технических проверок оформляется акт проведения специальной проверки, где отражается перечень проверенных элементов и вид технических проверок, фамилия и инициалы лица, проводившего тот или иной вид проверки и заключение по результатам специальной проверки.

5. Акт оформляется в единственном экземпляре и остается у исполнителя.

6. Заключение оформляется в двух экземплярах, первый экземпляр направляется в адрес заказчика, второй остается у Исполнителя.

Акт и заключение утверждаются руководителем организации, проводившей специальную проверку.

При выявлении демаскирующих признаков СЭУ проводятся более детальные исследования с целью его выявления.

Второй учебный вопрос: Организация и порядок проведения специального обследования защищаемого помещения (объекта информатизации)

Специальные обследования защищаемых помещений - это комплекс инженерно-технических мероприятий, проводимых с использованием необходимых, в том числе и специализированных технических средств, проводимых с целью выявления возможно внедренных электронных средств съема информации в ограждающих конструкциях, предметах мебели и интерьера защищаемых помещений (ЗП).

Подготовка к проведению специальных обследований

1. Оценка обстановки, складывающейся в районе проведения поисковой операции :
   - Оценка противника;
   - Оценка условий.
2. Разработка порядка и последовательности проведения поисковой операции
3. Разработка план-графика выполнения поисковых работ

Оценка обстановки, складывающейся в районе проведения поисковой операции

Оценка противника - анализ причины, проведения специального обследование и модели противника в результате которого необходимо сделать промежуточные выводы, которые должны позволить получить предварительный облик противника:
- характер его потенциальных возможностей;
- расположение и вид закладных устройств (если они обнаружены до проведения поисковой операции).

Оценка условий:
- анализируется расположение объекта на местности с учетом окружающей его территории и размещенных на ней посторонних объектов;
- оценивается КЗ и возможности по снятию информации из-за ее пределов;
- обследуется сам исследуемый объект.

При непосредственном анализе объекта определяют:
- взаимное расположение контролируемых и смежных помещений, режимы их посещения;
- устанавливают факты и сроки ремонтных работ, монтажа и демонтажа коммуникаций, замены предметов мебели и интерьера;
- изготовляют планы помещений, на которые наносят все входящие и проходящие коммуникации;
- изучают конструктивные особенности ограждающих поверхностей, материалы покрытий.

Анализ противника и объекта

- Базируясь на выводах о возможном противнике и данных об объекте, определяют:

- виды и объем поисковых действий;
- состав измерительной техники и вспомогательного имущества;
- необходимое количество специалистов и подсобных рабочих;
- временной диапазон проведения операции.

Результаты оценки обстановки

1. Легенда проведения поисковой операции;
2. План прилегающей территории с указанием принадлежности и назначения строений;
3. Поэтажный план строения с обозначением смежных с обследуемым помещений;
4. Отчет об организациях или частных лицах, работающих в смежных помещениях;
5. Протокол, содержащий характеристики ограждающих поверхностей, материалов покрытий;
6. Схема жизнеобеспечивающих сооружений с привязкой к плану помещения;
7. Схема входящих и проходящих проводных коммуникаций;
8. План (фотографии) размещения мебели, предметов интерьера на объекте;
9. План-график работ с указанием ответственных исполнителей;
10. Перечень необходимой исследовательской аппаратуры.

Порядок и последовательность проведения специального обследования

Определение:

1. Ответственных за выполнение основных этапов работ;
2. Последовательность и сроки их выполнения;
3. Порядок материального обеспечения;
4. Порядок и последовательность действий при отклонениях и несоблюдении сроков решения основных вопросов;
5. Порядок взаимодействия между исполнителями;
6. Порядок управления и контроля за действиями подчиненных.

Разработка план-графика выполнения работ, в котором отражаются основные вопросы решения:

- начало и окончание основных работ;
- ответственные исполнители;
- последовательность выполнения основных этапов, их взаимосвязь между собой;
- организация контроля качества и сроков выполнения основных видов работ.

Выполнение поисковых мероприятий

Четыре вида проводимых исследований:

1. Радиообнаружение;
2. Осмотр помещения;
3. Обследование электрических и электронных приборов;
4. Проверка проводных коммуникаций.

Радиообнаружение

Идентификация подозрительных сигналов
Для решения подобных задач целесообразно применять автоматизированные программно-аппаратные комплексы, включающие приемник и персональную ЭВМ, работающую под управлением специального программного обеспечения. Более сложные системы имеют в своем составе модернизированные приемники или дополнительные устройства, повышающие быстродействие (блок аналого-цифровой обработки, блок быстрого преобразования Фурье) и расширяющие функциональные возможности (коррелляторы, контроллеры, коммутаторы и т.п.).

Осмотр помещений

Первичный осмотр. На этом этапе осуществляют визуальный контроль помещения и находящихся в нем предметов. Во избежание пропуска зоны или предмета осмотр проводят по определенной схеме, двигаясь по часовой стрелке и от периферии к центру. При наличии плана или фотографии предварительно сличают истинное размещение вещей и предметов с зафиксированным документально.

Техническая проверка. Аппаратурную проверку предметов мебели и интерьера проводят с применением нелинейного локатора и переносного рентгеновского аппарата на подготовленной площадке, предварительно проверенной на наличие помеховых сигналов.

Обследование электрических и электронных приборов

- Электрические приборы (настольные лампы, нагревательные приборы, электрические удлинители) перед проверкой включают в сеть и индикатором поля определяют наличие в них источников радиоизлучения.
- При установлении подозрительных излучений прибор проверяют с помощью комплекса радиообнаружения.
- Затем обесточивают, разбирают и осматривают.

Проверка проводных коммуникаций

- Осмотр каждой линии начинают с установления трассы ее прохождения в помещении, используя монтажные схемы и металлоискатели.
- Линии проверяют на наличие в них высокочастотных сигналов, модулированных информационным сообщением. Слаботочные линии дополнительно проверяют на присутствие в них информационных низкочастотных сигналов.

Подготовка отчетных материалов

- Протоколы с указанием мест срабатывания исследовательских приборов, участков вскрытий ограждающих поверхностей, описанием подозрительных предметов мебели и интерьера;
- Протоколы изъятия средств съема информации;
- Заключение о степени защищенности объекта от несанкционированного съема информации;
- Рекомендации по устранению **и** нейтрализации технических каналов утечки конфиденциальных сведений.