Тема 11. Мероприятия организации инженерно-технической защиты информации

Занятие 2. Мероприятия по контролю эффективности инженерно-технической защиты информации

Учебные вопросы:

- 1. Меры контроля эффективности защиты информации. Виды контроля эффективности инженерно-технической защиты информации.
- 2. Характеристика мер технического контроля эффективности защиты информации

Литература

- 1. Бузов Г. А. и д.р. Защита от утечки информации по техническим каналам. М.: Горячая линия-Телеком, 2005.
- 2. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь. – М.: НОУ ШО Баярд, 2004.
- 3. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Гелиус, 2005.
- 4. Зайцев и др. Технические средства и методы защиты информации. М.: Машиностроение 2009.

Первый учебный вопрос: Меры контроля эффективности защиты информации. Виды контроля эффективности инженерно-технической защиты информации.

- Определение ГОСТ 50922:
- **1. Мероприятие по контролю эффективности защиты информации** есть совокупность действий по разработке и/или практическому применению методов [способов] и средств контроля эффективности защиты информации.
- **2. Средство контроля эффективности защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации
- **3. Метод [способ] контроля эффективности защиты информации** - порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.


Мероприятия по контролю эффективности защиты информации
Методы контроля эффективности ЗИ
Средства контроля эффективности
Контроль состояния ЗИ
Контроль организации ЗИ
Контроль эффективности ЗИ
Мониторинг безопасности информации
Экспертиза документов по ЗИ
Организационный контроль
Технический контроль
Аудит ИБ
1. Проверка;
2. Анализ;
3. Наблюдение
4. Сравнение и учет
1. Инструментальный;
2. Инструментально-расчетный;
3. Расчетный
Аудиторская проверка информационной безопасности

- **Контроль состояния защиты информации** - проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.
- **А) Мониторинг безопасности информации**
- **Б) Контроль организации защиты информации**
- **В) Контроль эффективности защиты информации**

Мониторинг безопасности информации

- **Мониторинг безопасности информации**: Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью выявления его соответствия требованиям по безопасности информации.
- **Аудиторская проверка информационной безопасности в организации**: Периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организации установленных требований по обеспечению информационной безопасности.
- **Аудиторская проверка безопасности информации в информационной системе**: Проверка реализованных в информационной системе процедур обеспечения безопасности информации с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию

- **Контроль организации защиты информации** - проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.
- **ГОСТ Р 50922 – 2006 экспертиза документа по защите информации:** Рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение.

- **Контроль эффективности защиты информации** - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.
- **а) Организационный контроль эффективности защиты информации** - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.
- **б)Технический контроль эффективности защиты информации** - контроль эффективности защиты информации, проводимой с использованием средств контроля.

Алгоритм подготовки и проведения проверки

- *1. принятие решения о проведении проверки;*
- *2. подготовка перечня проверяемых вопросов;*
- *3. определение состава комиссии;*
- *4. определение сроков работы комиссии;*
- *5. подготовка и утверждение плана проверки;*
- *6. непосредственное проведение проверки;*
- *7. оформление результатов работы;*
- *8. выработка предложений и рекомендаций;*
- *9. доклад результатов проверки на месте;*
- *10. анализ недостатков с проверяемыми;*
- *11. доклад результатов лицу, назначившему проверку.*

Виды контроля

- **Предварительный контроль** проводится при любых изменениях состава, структуры и алгоритма функционирования системы защиты информации, в том числе:

- после установки нового технического средства защиты или изменения организационных мер;
- после проведения профилактических и ремонтных работ средств защиты;
- после устранения выявленных нарушений в системе защиты.

- **Периодический контроль** проводится выборочно (применительно к отдельным темам работ, структурным подразделениям или всей организации) по планам, утвержденным руководителем организации, а также вышестоящими органами.

  Периодический (ежедневный, еженедельный, ежемесячный) контроль должен проводиться также сотрудниками организации в части проверки наличия источников информации, с которыми они работают.

  Общий (в рамках всей организации) периодический контроль проводится временными внутренними и внешними комиссиями обычно 2 раза в год. Целью его является тщательная проверка работоспособности всех элементов и системы защиты информации в целом. Так как о времени работы комиссии сотрудникам организации (предприятия) заранее известно, то эти проверки выявляет в основном недостатки, не устраненные перед началом работы комиссии.

- **Постоянный контроль** осуществляется выборочно силами службы безопасности и привлекаемых сотрудников организации с целью объективной оценки уровня защиты информации и, прежде всего, выявления слабых мест в системе защиты организации. Так как объекты и время такого контроля сотрудникам не известны, то такой контроль, кроме того, оказывает психологическое воздействие на сотрудников организации, вынуждая их более тщательно и постоянно выполнять требования по обеспечению защиты информации.

Технический контроль эффективности защиты информации

- Цель технического контроля – получение объективной и достоверной информации о состоянии защиты объектов контроля и подтверждение того, что утечка информации с объекта невозможна, т.е. на объекте отсутствуют технические каналы утечки информации
- Технический контроль предназначен для:

- выявления возможных каналов утечки конфиденциальной информации;
- проверки соответствия и эффективности принятых мер защиты нормативным требованиям;
- разработки рекомендаций по совершенствованию принятых защитных мероприятий.

Способы проведения технического контроля эффективности технической защиты

- • *комплексный*, когда проверяется возможная утечка информации по всем опасным каналам контролируемого объекта;
- • *целевой*, когда проводится проверка по одному из интересующих каналов возможной утечки информации;
- • *выборочный*, когда из всего перечня технических средств на объекте для проверки выбираются только те, которые по результатам предварительной оценки с наибольшей вероятностью имеют опасные каналы утечки защищаемой информации.

Методы технического контроля

- • *инструментальные*, когда контролируемые показатели определяются непосредственно по результатам измерения контрольно-измерительной аппаратурой;
- • *инструментально-расчетные*, при которых контролируемые показатели определяются частично расчетным путем и частично измерением значений некоторых параметров физических полей аппаратными средствами;
- • *расчетные*, при которых контролируемые показатели рассчитываются по методикам, содержащимся в руководящей справочной литературе.

- Технический контроль проводится по отдельным физическим полям, создаваемых объектами информатизации, и состоит из:

- сбора исходных данных, характеризующих уязвимости объекта информатизации по отношению к воздействиям технической разведки;
- определения возможных типов и средств технической разведки;
- предварительного расчета зон разведдоступности;
- определения состава и подготовки к работе контрольно-измерительной аппаратуры;
- измерения нормируемых технических параметров защищаемого объекта по отдельным физическим полям на границе контролируемой зоны;
- определения эффективности принятых мер защиты и в отдельных случаях разработки необходимых мер усиления защиты.

- Технические меры контроля проводятся с использованием технических средств радио- и электрических измерений, физического и химического анализа и обеспечивают проверку:

- напряженности полей с информацией на границах контролируемых зон;
- уровней опасных сигналов и помех в проводах и экранах кабелей, выходящих за пределы контролируемой зоны;
- степени зашумления генераторами помех структурных звуков в ограждениях;
- концентрации демаскирующих веществ в отходах производства.