

Тема 2. Виды обеспечения системы информационной безопасности

Занятие 10. Инженерно- техническое обеспечение СОИБ ХС

УЧЕБНЫЕ ВОПРОСЫ:

- 1. Средства инженерно-технической защиты территорий и помещений**
- 2. Средства обнаружения и защиты технических каналов утечки информации**

Инженерно-техническое обеспечение СОИБ –

совокупность средств инженерно-технической защиты территорий и

- **Образец текста**
помещении хозяйствующего субъекта и средств обнаружения и защиты информации, организованная направленность применения которых состоит в создании системы охраны и защиты информации на объектах и элементах информационной системы хозяйствующего субъекта от угроз ее хищения, модификации или уничтожения

Структурная схема системы инженерно-технического обеспечения СОИБ ХС

ИНЖЕНЕРНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СОИБ ХС

Второй уровень декомпозиции –
НАПРАВЛЕНИЯ

В

**Инженерно-техническая защита
территорий и помещений ХС**

**Обнаружение и защита технических
каналов утечки информации**

Третий уровень декомпозиции –
СИЛЫ

П,

1 Служба безопасности;
2 IT-специалисты;
3 Специалисты внешних организаций
(аутсорсинг);
4 Специалисты госпожарнадзора;
5 Штатный (нештатный) пожарник
(пожарная команда)

1 Служба безопасности;
2 IT-специалисты;
3 Внешние эксперты (консалтинг);
4 Специалисты внешних организаций
(аутсорсинг);

Четвертый уровень декомпозиции –
СРЕДСТВА

**Инженерно-технические средства
физической системы защиты:**

- 1 Инженерно-технические средства подсистемы предупреждения угроз;
- 2 Инженерно-технические средства подсистемы обнаружения угроз;
3. Инженерно-технические средства подсистемы ликвидации угроз

**Технические средства обнаружения
(поиска) и защиты каналов утечки
информации:**

1. Средства обнаружения технических каналов утечки информации;
2. Средства защиты информации от утечек по техническим каналам;
3. Средства защиты компьютерной информации от НСД;
4. Средства защиты от утечки информации по материально-вещественному каналу

Основные задачи инженерно-технического обеспечения СОИБ ХС

1. **Обращение против проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или модификации;**
Образец текста
Второй уровень
Третий уровень
Четвертый уровень
2. **Защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении;**
Пятый уровень
3. **Предотвращение утечки информации по различным техническим каналам.**

- Под **подсистемой инженерно-технической защиты территорий и помещений** будем понимать совокупность инженерно-технических средств физической системы защиты, содержащей в своем составе средства, препятствующие физическому проникновению (доступу) злоумышленников на объекты за **второй уровень** конфиденциальной информации, а также осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных действий.
- Под **подсистемой обнаружения и защиты технических каналов утечки информации** будем понимать совокупность средств, применение которых обеспечивает выявление технических каналов утечки информации, защиту информации от утечек по техническим и материально-вещественному каналам, а также средства защиты компьютерной информации при несанкционированном доступе к ней.

Варианты защиты информации на основе инженерно-технического обеспечения

1. Источник и носитель информации локализованы в пределах границ объекта защиты и обеспечена защита от контакта с ними злоумышленника или дистанционного воздействия на них полеи его технических средств добывания;
Первый уровень
Второй уровень
Третий уровень
Четвертый уровень
2. Соотношение энергии носителя и помех на выходе приемника канала утечки такое, что злоумышленнику не удастся снять информацию с носителя с необходимым для ее использования качеством;
Пятый уровень
3. Злоумышленник не может обнаружить источник или носитель информации;
4. Вместо истинной информации злоумышленник получает ложную

Методы защиты информации на основе применения средств инженерно-технического обеспечения

- **Образец текста**
возникновению злоумышленника к источникам информации и воздействию на них стихийных сил природы;
- **Второй уровень**
Третий уровень
Четвертый уровень
Пятый уровень
Скрытие достоверной информации, посредством информационного и энергетического срытия;
- "подсовывание" злоумышленнику ложной информации, т.е. скрытие достоверной информации, посредством информационного срытия

Задачи решаемые с использованием инженерно-технических средств системы физической защиты

1. ~~Образец~~ регистрации предприятия и наблюдение за ней;
2. ~~Третий уровень~~ Охраны зданий, внутренних помещений ~~Четвертый уровень~~ и контроль за ними; ~~Пятый уровень~~
3. Охраны оборудования, продукции, финансов и информации;
4. Осуществления контролируемого доступа в здания и помещения.

Структурная схема подсистемы инженерно-технической защиты территорий и помещений

**Инженерно-техническая защита
территорий и помещений ХС**

Текста

Уровень

Уровень

Уровень

Уровень

Второй уровень декомпозиции -
НАПРАВЛЕНИЯ

Подсистема
предупреждения угроз

Подсистема
обнаружения угроз

Подсистема
ликвидации угроз

Третий уровень
декомпозиции - **СИЛЫ**

1. Сотрудники службы
безопасности

1. Дежурный состав
охраны службы
безопасности
2. Штатный или
нештатный пожарник
3. Специалисты
госпожарнадзора

1. Сотрудники службы
безопасности
(подразделение охраны)
2. Штатный или
нештатный пожарник

Четвертый уровень декомпозиции -
СРЕДСТВА

Инженерные средства
физической защиты

Средства контроля и
управления доступом

Средства охранной, охранно-
пожарной (пожарной)
сигнализации

Средства охранного
телевидения
(видеонаблюдения)

Средства охранного
дежурного освещения

Средства тревожной
сигнализации

Средства пожаротушения

Средства резервного
(аварийного)
электропитания

Подсистема предупреждения угроз

- Подсистема предупреждения угроз включает:
 - инженерные средства физической защиты;
 - средства контроля и управления доступом.
- **Инженерные средства физической защиты:**
 - естественные или искусственные преграды (барьеры);
 - особые конструкции периметров, проходов, оконных переплетов и дверных проемов зданий и помещений, а также сейфов и хранилищ;
 - зоны безопасности.
- **К средствам искусственных преград (барьеров) относятся:**
 - неровности поверхности земли (ровы, овраги, скалы);
 - труднопроходимый лес и кустарник;
 - водные преграды (каналы, реки, озера и сильно заболоченная местность);
- **К искусственным преградам (барьерам) относятся средства:**
 - бетонные или кирпичные заборы;
 - конструкции для ограничения скорости проезда транспортных средств;
 - решетки, сетчатые конструкции, металлические ограды и другие виды ограждений.
- **инженерные средства, создания дополнительных препятствий: защитная (колючая) проволока, острые металлические стержни или битое стекло, устанавливаемые поверх заборов;**
 - малозаметные проволочные сети для создания полосы отчуждения вдоль забора.
- **К особым конструкциям периметров, проходов, оконных и дверных переплетов помещений, сейфов и хранилищ относятся:**
 - деревянные или металлические двери (ворота);
 - окна, укрепленные различными способами;
 - металлические шкафы, сейфы и хранилища.

Система контроля и управления доступом

- Система управления доступом это программно-аппаратный комплекс, включающий в себя контроллеры СКУД, управляемые замки, считыватели, металлодетекторы, преграды в виде дверей, ворот, турникетов и шлюзовых кабин, а также компьютеры и программное обеспечение верхнего уровня, облегчающее настройку, мониторинг и оперативное управление правами доступа персонала.

Образец текста

- К основным средствам СКУД относятся:

- контроллер – электронный прибор (специализированный компьютер), в котором хранится информация о конфигурации, режимах работы системы, перечень лиц, имеющих право доступа на объект, а также уровень их полномочий;

Второй уровень

Третий уровень

- считыватель – устройство, подключаемое к контроллеру и позволяющее извлекать с него информацию личного идентификатора, как с "пропуска" пользователя;

Четвертый уровень

Пятый уровень

- К средствам системы управления доступом также относятся:

- преграда, одновременно являющаяся средством пропуска персонала или транспорта: дверь, турникет, шлюзовая кабина, шлагбаум и т.п.;

- исполнительный механизм для поддержания преграды в закрытом состоянии (нормальное состояние – доступ запрещен): замок для двери, запирающее устройство турникета, шлюзовой кабины, шлагбаума и т.п.;

- устройства контроля состояния преграды: датчики различных типов (например, герконовые);

- средства управления устройством запираения с модулем идентификации: контроллер со считывателем;

- идентификаторы: электронные пропуска, карты.

Состав основных средств обязательного и дополнительного оснащения системы контроля и управления доступом

- Образец
Второй уровень

Средства оснащения системы контроля и управления доступом

Средства обязательного оснащения

Пятый уровень

Контроллер

Исполнительные механизмы

Считыватель

Датчик положения двери

Средства дополнительного оснащения

Дверной доводчик

Аудио и видеодомофон

Блок резервного питания

Система дистанционного отпирания дверей

Подсистема обнаружения угроз

- средства охранной, охранно-пожарной (пожарной) сигнализации;
- средства охранного телевидения (видеонаблюдения);
- средства охранного оповещения.
- **Образец текста**
К средствам охранной и охранно-пожарной (пожарной) сигнализации относятся технические средства охраны объектов:
 - **Первый уровень**
извещатель (датчик) охранной и охранно-пожарной (пожарной) сигнализации – техническое устройство, формирующее электрический сигнал тревоги при воздействии на него или на создаваемые им поля внешних сил или объектов;
 - **Второй уровень**
шлейф охранной, охранно-пожарной (пожарной) сигнализации – канал связи образующий электрическую цепь, обеспечивающий передачу сигналов тревоги от извещателя (датчика) к приемно-контрольному прибору пункта или поста охраны и средствам тревожного оповещения;
 - **Третий уровень**
приемно-контрольные приборы (ПКП) – устройства предназначенные для приема обработки и регистрации сигналов тревоги, поступающих от извещателей (датчиков).

Система видеоконтроля

- передающие телевизионные камеры (видеокамеры);
- устройства отображения видеоинформации - мониторы;
- устройства обработки видеоинформации (коммутаторы, квадраторы, мультиплексоры);
- устройства регистрации информации (видеопринтеры, бытовые и специализированные видеомагнитофоны);
- кабели, обеспечивающие электрические связи элементов системы видеонаблюдения.
- **Средства телевизионного (видео) наблюдения обеспечивают:**
 - визуальный контроль за зонами и рубежами защиты;
 - наблюдение за нарушителями рубежей охраны, определение их количества, вооруженности, действий и намерений;
 - контроль за действиями лиц охраны и персонала организации;
 - запись видеоизображений для последующего обнаружения и опознавания злоумышленников, контроля и анализа действий сотрудников охраны.

Охранное дежурное освещение

- Охранное дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время как на территории объекта, так и внутри здания.
 - К основным средствам охранного дежурного освещения относятся:
 - лампы накаливания: вакуумные, криптоновые и галогенные лампы накаливания общего назначения мощностью до 1000 Вт;
 - разрядные лампы: газо- и паросветные, люминесцентные с пускорегулирующим устройством и электродосветные;
 - ИК-прожекторы.
- Светодиодные прожекторы и лампы.

Подсистема ликвидации угроз

Основными составными элементами подсистемы

ликвидации угроз являются:

• **Образец текста**
- Средства тревожной сигнализации.

Второй уровень
Средства звуковой сигнализации

Третий уровень
Средства тревожной световой сигнализации

- Средства пожаротушения.

Четвертый уровень

Пятый уровень

пенообразующие огнетушители;

механические средства (багры, топоры) для

разрушения очага пожара;

емкости с песком;

бочки с водой;

пожарные рукава и др.

- Средства резервного (аварийного) электропитания

Обнаружение и защита технических каналов утечки информации

Второй уровень декомпозиции - **НАПРАВЛЕНИЯ**

Подсистема обнаружения (поиска) технических каналов утечки информации

Подсистема защиты информации от утечек по техническим каналам

Подсистема предотвращения утечки информации по материально-вещественному каналу

Е Третий уровень декомпозиции - **СИЛЫ**

Т

1. Сотрудники службы безопасности;
2. IT-специалисты;
3. Внешние эксперты (консалтинг);
4. Специалисты внешних организаций (аутсорсинг);

1. Сотрудники службы безопасности
2. IT-специалисты;
3. Внешние эксперты (консалтинг);
4. Специалисты внешних организаций (аутсорсинг);

1. Сотрудники службы безопасности
2. IT-специалисты;
3. Ответственные сотрудники

Четвертый уровень декомпозиции - **СРЕДСТВА**

1. Средства методов физического поиска каналов утечки информации;
2. Средства методов инструментального (технического) контроля каналов утечки информации

1. Средства защиты информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ);
2. Средства защиты речевой информации в помещении;
3. Средства защиты телефонных линий

1. Средства защиты и экстренного уничтожения информации на бумажных носителях;
2. Средства защиты и экстренного уничтожения информации на машинных носителях

Средства обнаружения (поиска) каналов утечки информации

Второй уровень декомпозиции - **НАПРАВЛЕНИЯ**

Средства методов физического поиска

Средства методов инструментального (технического) контроля

2-ой уровень декомпозиции - **СИЛЫ**

Третий уровень декомпозиции - **СИЛЫ**

3-ий уровень декомпозиции - **СИЛЫ**

4-ый уровень декомпозиции - **СИЛЫ**

1. Служба безопасности;
2. IT-специалисты;
3. Внешние эксперты (консалтинг);
4. Специалисты внешних организаций (аутсорсинг);

1. Служба безопасности;
2. IT-специалисты;
3. Внешние эксперты (консалтинг);
4. Специалисты внешних организаций (аутсорсинг);

Четвертый уровень декомпозиции - **СРЕДСТВА**

Средства визуального поиска закладных устройств

Средства поиска каналов утечки информации за счет ПЭМИН

Средства обнаружения радиоизлучений закладных устройств

Средства обнаружения неизлучающих закладных устройств

Средства визуального осмотра помещений

Специальные измерительные устройства и приемники

1. Обнаружители поля
2. Радиоприемные устройства
3. Универсальные поисковые приборы
4. Автоматизированные поисковые комплексы

1. Обнаружители пустот
2. Аппаратура обнаружения элементов закладок
3. Аппаратура контроля проводных телефонных линий

Технические средства обнаружения закладных устройств методами физического поиска

- **Вспомогательное досмотровое оборудование:**
 - Третий уровень
 - **электрические фонари;**
 - Четвертый уровень
 - **досмотровые зеркала;**
 - Пятый уровень
- волоконно-оптические технические приборы – эндоскопы.

Технические средства для проведения мероприятий специальных проверок, обследований и исследований

- **Образец текста**
инструментального (технического) контроля, относительно методов выявления ТКУИ, можно разделить на три составные части:
Первый уровень
Второй уровень
Третий уровень
Четвертый уровень
Пятый уровень
1. Средства поиска каналов утечки информации за счет побочного электромагнитного излучения и наводок (ПЭМИН);
 2. Средства обнаружения радиоизлучений закладных устройств;
 3. Средства обнаружения неизлучающих закладных устройств.

Средства поиска каналов утечки информации за счет побочного электромагнитного излучения и наводок (ПЭМИН);

- **Образцовые микровольтметры;**
- **Второй уровень анализаторы спектра;**
Третий уровень
- **Специальные измерительные комплексы для проведения измерений уровней ЭМИ;**
Пятый уровень
- **обнаружители диктофонов**

Средства обнаружения радиоизлучений закладных устройств

1. Обнаружители поля:

- детекторные индикаторы электромагнитного излучения;

- интерсепторы;

- радиочастотомеры;

2. Радиоприемные устройства:

- бытовые радиоприемники;

- анализаторы спектра;

- сканирующие приемники;

- специальные высокоскоростные поисковые приемники

3. Универсальные поисковые приборы

Состав обязательных элементов комплексов:

- широкодиапазонного перестраиваемого по частоте приемника (сканера);

- блока распознавания закладок;

- блока акустической локации;

- процессора, осуществляющего обработку сигналов и управление приемником.

4. Автоматизированные поисковые комплексы

простейшие типовые поисковые программно-аппаратные комплексы;

– специализированные поисковые программно-аппаратные комплексы.

Средства обнаружения неизлучающих закладных устройств

1. Обнаружители пустот:

- различные ультразвуковые приборы, в том числе

- медицинские; **Образцы текста**

- специальные обнаружители пустот (тепловизоры).

2. Аппаратура обнаружения элементов закладок:

- нелинейные резонаторы;

- металлодетекторы;

- рентгеновские установки.

3. Аппаратура контроля проводных телефонных линий:

- устройства контроля напряжения линий;

- устройства анализа несимметрии линий;

- устройства анализа нелинейности параметров линий;

- устройства анализа неоднородности телефонных линий
(кабельные радары).

Средства защиты от технических каналов утечки информации

Второй уровень декомпозиции - **НАПРАВЛЕНИЯ**

Средства защиты информации, обрабатываемой ТСПИ

Средства защиты акустической информации в выделенных помещениях

Средства защиты телефонных аппаратов и двухпроводных линий

Третий уровень декомпозиции - **СИЛЫ**

1. Служба безопасности;
2. IT-специалисты;
3. Внешние эксперты (консалтинг);
4. Специалисты внешних организаций (аутсорсинг);

1. Служба безопасности;
2. IT-специалисты;
3. Внешние эксперты (консалтинг);
4. Специалисты внешних организаций (аутсорсинг);

1. Служба безопасности;
2. IT-специалисты;
3. Внешние эксперты (консалтинг);
4. Специалисты внешних организаций (аутсорсинг);

Четвертый уровень декомпозиции - **СРЕДСТВА**

Пассивные методы защиты

Активные методы защиты

Пассивные методы защиты

Активные методы защиты

Пассивные методы защиты

Активные методы защиты

1. Средства ослабления побочных электромагнитных излучений ТСПИ и их наводок;
2. Средства исключения (ослабления) просачивания информационных сигналов ТСПИ в цепи электропитания

1. Средства систем пространственного зашумления
2. Средства систем линейного зашумления

1. Средства звукоизоляции выделенных помещений

1. Средства создания виброакустических помех
2. Средства подавления диктофонов
3. Средства подавления (нейтрализации) акустических закладок

1. Средства ограничения, фильтрации и отключения источников опасных сигналов в оконечном оборудовании слаботочных линий.
2. Средства блокирования радиозакладок

1. Средства линейного зашумления телефонных аппаратов
2. Средства зашумления и уничтожения радиозакладок
3. Средства криптографической защиты телефонных линий

1. Средства ослабления побочных электромагнитных излучений ТСПИ и их наводок:

- экранирование технических средств;
- заземление технических средств;
- фильтрация информационных сигналов

2. Средства исключения (ослабления)

просачивания информационных сигналов ТСПИ в цепи электропитания:

- средства систем пространственного зашумления;
- средства систем линейного зашумления

Экранирование технических средств

1. Электростатическое;
2. Магнитостатическое;
3. • **Электромагнитное**

Экранирование

- Второй уровень

- источники ПЭМИ, Третий уровень
- Четвертый уровень

- монтаж проводов и соединительные линии;
- помещения;

Характеристика степени ослабления высокочастотных электромагнитных полей различными зданиями

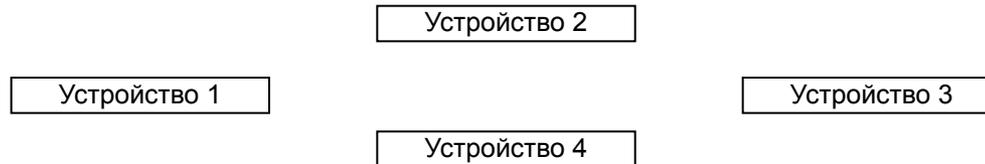
Тип здания	Степень экранирования, дБ		
	100 МГц	500 МГц	1000 МГц
Кирпичное здание с толщиной стен 1,5 кирпича	13 ... 15	15 ... 17	16 ... 19
Железобетонное здание с ячейкой арматуры 15 x 15 см и толщиной стен 16 см	20 ... 25	18 ... 19	15 ... 17

Системы заземления

1. Общего заземления;
 2. Заземляющего кабеля;
 3. Шин и проводов, соединяющих заземлитель с объектами;
 - Второй уровень
 - Третий уровень
 - Четвертый уровень
 - Штатный уровень
- Для создания контуров заземления наиболее часто используют следующие схемы:
- одноточечного последовательного и параллельного соединения устройств;



- многоточечного соединения устройств;



- гибридного соединения устройств.

Фильтрация информационных сигналов

- **Разделительные трансформаторы** – обеспечивают ослабление информационного сигнала и тем самым способствует предотвращению проникновения сигналов по проводникам
 - **Помехоподавляющие фильтры** – предназначены для пропуска без ослабления сигналов, частоты которых находятся в пределах рабочего диапазона и ослабления нежелательных сигналов, частоты которых находятся вне участков этого частотного диапазона.
- Различают фильтры верхних и нижних частот, полосовые и заграждающие фильтры.

- Средства пространственного зашумления предназначены для исключения перехвата ПЭМИ по образцу текста электромагнитному каналу.
- Средства линейного зашумления предназначены для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС.
- К ним относятся устройства генерирующие помехи типа «белого шума» или «синфазной помехи».

Звукоизоляция выделенных помещений

Звукоизоляция выделенных помещений

проводится с целью исключения перехвата акустической (речевой) информации по прямому акустическому (через щели, окна, двери, технологические проемы, вентиляционные каналы и т. д.) и вибрационному (через ограждающие конструкции, трубы и т.д.) каналам.

Образец текста

Второй уровень

Третий уровень

Четвертый уровень

Пятый уровень

Активные методы защиты речевой информации направлены на:

- создание маскирующих акустических (вибрационных) помех;
 - подавление диктофонов в режиме записи;
 - создание прицельных радиопомех акустическим радиозакладкам (в том числе – средствам мобильной радиосвязи, используемым в качестве радиомикрофона).
1. Средства виброакустической маскировки - специальные генераторы белого и розового шума
 - Третий уровень
 2. Средства подавления диктофонов – портативные (переносные) и стационарные
 - Четвертый уровень
 - Портативные подавители диктофонов изготавливаются в обычном кейсе, а стационарные монтируются в месте проведения конфиденциальных переговоров под крышкой стола или в ближайшем шкафу.
 3. Средства подавления (нейтрализации) акустических закладных устройств относятся следующие виды технических средств:
 - средства постановки прицельной помехи;
 - системы пространственного электромагнитного зашумления;
 - помехоподавляющие фильтры низких частот и системы линейного зашумления;
 - средства блокирования работы сотовых телефонов.