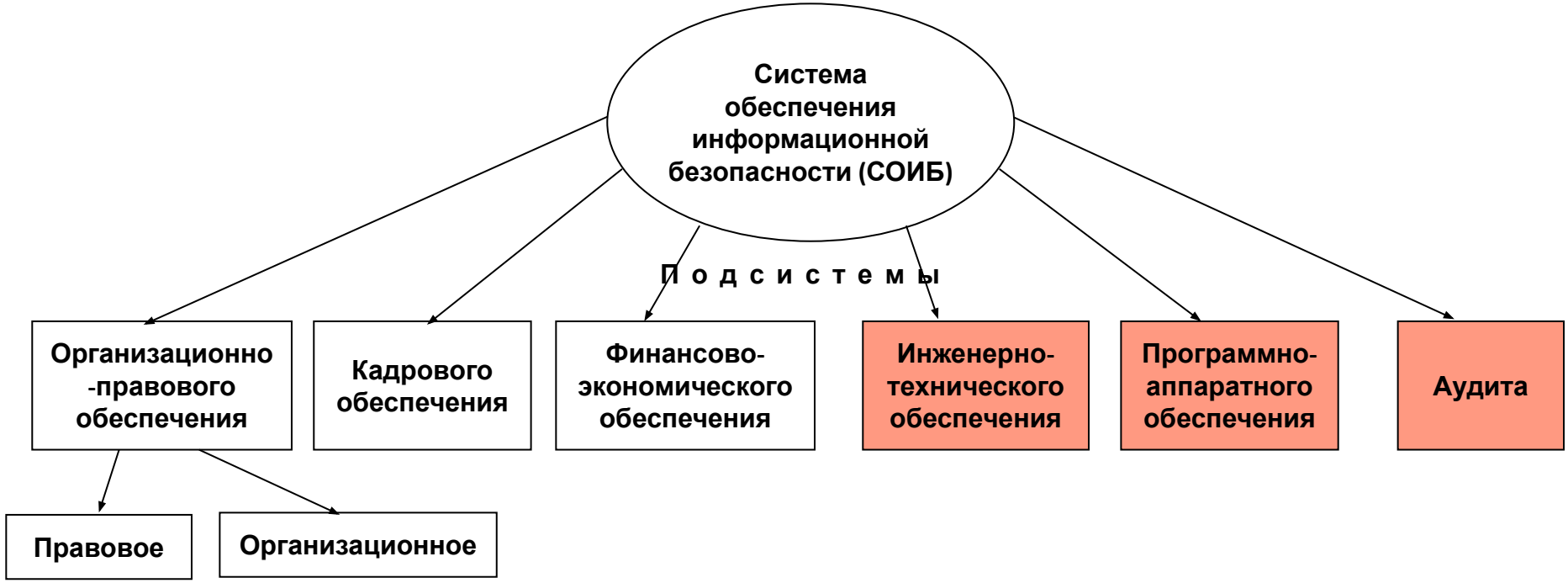
- ***Система обеспечения информационной безопасности*** (СОИБ) – функциональная подсистема системы комплексной безопасности, объединяющая силы, средства и объекты защиты информации, организованные и функционирующие по правилам, установленным правовыми, организационно-распорядительными и нормативными документами по защите информации

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Н а п р а в л е н и я

Анализ финансово-экономической деятельности	Моделирование экономических и финансовых процессов	Моделирование экономических и финансовых рисков

С р е д с т в а

- экономические показатели; - финансовые показатели;	- модели TCO, ROI и др.;	- модели оценки экономических и финансовых рисков

УЧЕБНЫЕ ВОПРОСЫ:

1. Инженерно-техническое обеспечение информационной безопасности
2. Программно-аппаратное обеспечение информационной безопасности
3. Аудит информационной безопасности

Первый учебный вопрос:

Инженерно-техническое обеспечение информационной безопасности

Инженерно-техническое обеспечение СОИБ – совокупность средств инженерно-технической защиты территорий и помещений 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

ИНЖЕНЕРНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СОИБ

НАПРАВЛЕНИЯ

Инженерно-техническая защита территорий и помещений

Обнаружение и защита технических каналов утечки информации

СИЛЫ

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);

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

1. Воспрещение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или модификации
2. Защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении
3. Предотвращение утечки информации по различным техническим каналам

- **Подсистема инженерно-технической защиты территорий и помещений** – это совокупность инженерно-технических средств физической системы защиты, содержащей в своем составе средства, препятствующие физическому проникновению (доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации, а также осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных действий

- **Подсистема обнаружения и защиты технических каналов утечки информации** – это 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 механическая преграда от контакта с ними злоумышленника или дистанционного воздействия на них полей его технических средств добывания

2. Соотношение энергии носителя и помех на выходе приемника канала утечки такое, что злоумышленнику не удается снять информацию с носителя с необходимым для ее использования качеством

3. Злоумышленник не может обнаружить источник или носитель информации

4. Вместо истинной информации злоумышленник получает ложную

СРЕДСТВА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ТЕРРИТОРИЙ И ПОМЕЩЕНИЙ

Методы защиты информации на основе применения средств инженерно-технического обеспечения

- воспрепятствование непосредственному проникновению злоумышленника к источникам информации и воздействию на них стихийных сил природы;
- скрытие достоверной информации, посредством информационного и энергетического срытия;
- "подсовывание" злоумышленнику ложной информации, т. е. скрытие достоверной информации, посредством информационного скрытия

Задачи решаемые с использованием инженерно-технических средств системы физической защиты

1. Охраны территории предприятия и наблюдение за ней
2. Охраны зданий, внутренних помещений и контроль за ними
3. Охраны оборудования, продукции, финансов и информации
4. Осуществления контролируемого доступа в здания и помещения

Структурная схема подсистемы инженерно-технической защиты территорий и помещений

ПОДСИСТЕМА ПРЕДУПРЕЖДЕНИЯ УГРОЗ

1. Инженерные средства физической защиты;
2. Средства контроля и управления доступом.

1. Инженерные средства физической защиты:

- естественные и искусственные преграды (барьеры);
- особые конструкции периметров, проходов, оконных переплетов и дверных проемов зданий и помещений, а также сейфов и хранилищ;
- зоны безопасности

К средствам естественных преград (барьеров) относятся:

- неровности поверхности земли (рвы, овраги, скалы);
- труднопроходимый лес и кустарник;
- водные преграды (каналы, реки, озера и сильно заболоченная местность)

К искусственным преградам (барьерам) относятся:

- 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

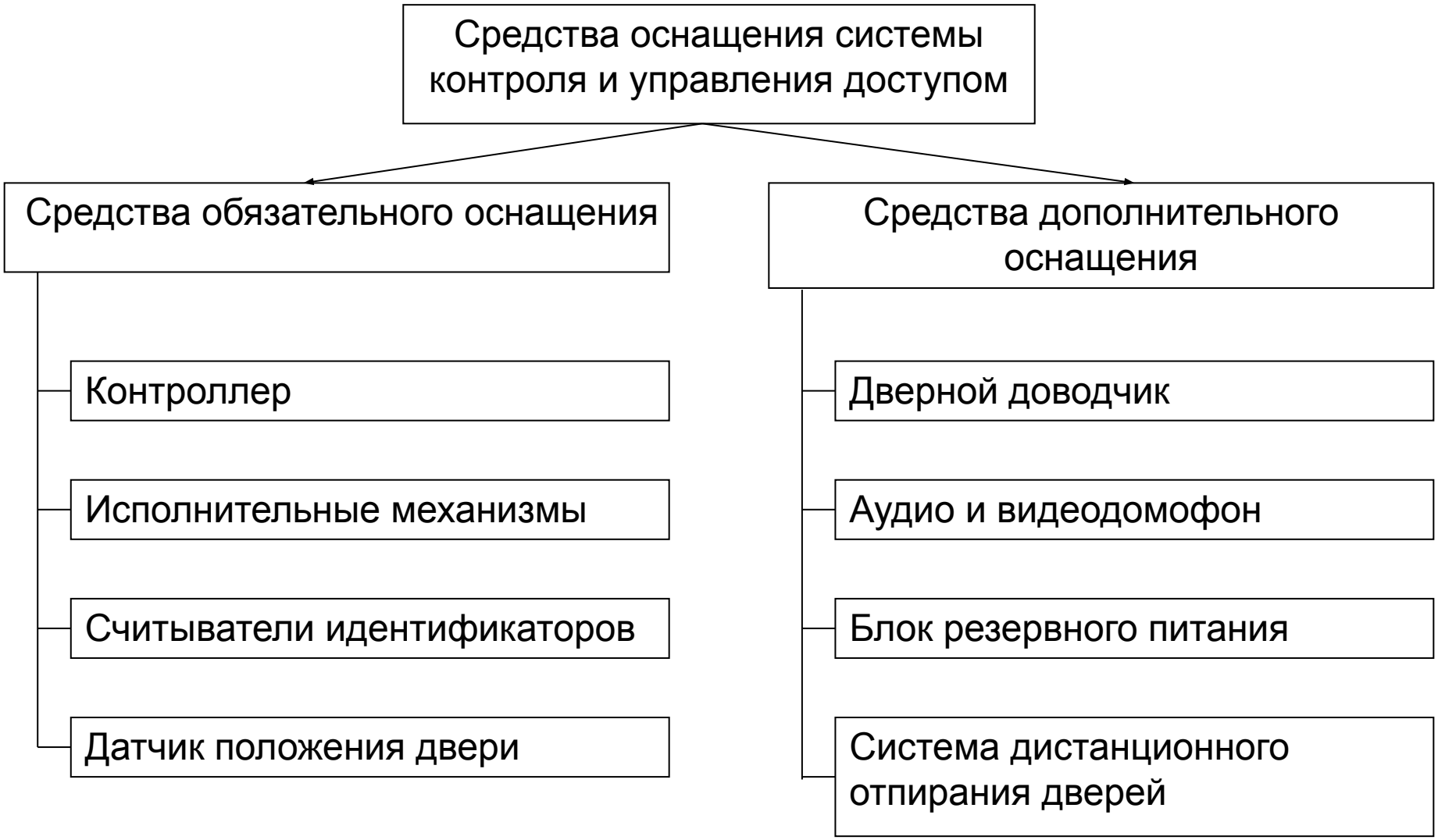
2. Система контроля и управления доступом (СКУД)

- **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.

К основным средствам СКУД относятся:

- ✔ контролер – 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;
- ✔ считыватель – устройство, подключаемое к контроллеру и позволяющее извлекать с него информацию личного идентификатора, как с "пропуска" пользователя;
- ✔ 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 запирания с модулем идентификации: контроллер со считывателем;
- ✔ идентификаторы: электронные пропуска, карты

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



ПОДСИСТЕМА ОБНАРУЖЕНИЯ УГРОЗ

- средства охранной, охранно-пожарной (пожарной) сигнализации;
- средства охранного телевидения (видеонаблюдения);
- средства охранного освещения

Средства охранной и охранно-пожарной (пожарной) сигнализации :

- извещатель (датчик) охранный и охранно-пожарный (пожарный) – техническое устройство, формирующее электрический сигнал тревоги при воздействии на него или на создаваемые им поля внешних сил или объектов;
- шлейф охранной, охранно-пожарной (пожарный) 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;
- приемно-контрольные приборы (ПКП) – устройства предназначенные для приема обработки и регистрации сигналов тревоги, поступающих от извещателей (датчиков)


ИЗВЕЩАТЕЛИ
(датчики)
По назначению
- для отдельных объектов;
- для закрытых помещений;
- для открытых пространств;
- пожарные
По принципу обнаружения
По виду зоны обнаружения
- точечная защита;
- защита по линии;
- защита по площади;
- защита по объему
Контактные
Акустические
Оптико-электронные
Микроволновые (радиоволновые)
Вибрационные
Емкостные
Тепловые (пожарные)
Ионизационные (пожарные)
Комбинированные

Система видеоконтроля

•передающие телевизионные камеры (видеокамеры);
•устройства отображения видеоинформации - мониторы;
•устройства обработки видеоинформации (коммутаторы, квадраторы, мультиплексоры);
•устройства регистрации информации (видеопринтеры, бытовые и специальные 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

Схема системы видеоконтроля

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

Для освещения объектов телевизионного (видео) наблюдения целесообразно использовать лампы накаливания

Основные составные элементы подсистемы ликвидации угроз

- средства тревожной сигнализации;
- средства пожаротушения;
- средства резервного (аварийного) электропитания

СРЕДСТВА ОБНАРУЖЕНИЯ И ЗАЩИТЫ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Обнаружение и защита технических каналов утечки информации

НАПРАВЛЕНИЯ

Подсистема обнаружения (поиска) технических каналов утечки информации	Подсистема защиты информации от утечек по техническим каналам	Подсистема предотвращения утечки информации по материально-вещественному каналу

СИЛЫ

1. Сотрудники службаыбезопасности; 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

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

НАПРАВЛЕНИЯ

Средства методов физического поиска

Средства методов инструментального (технического) контроля

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);

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:

- электрические фонари;
- досмотровые зеркала;
- волоконно-оптические технические приборы (эндоскопы)

Технические средства для проведения мероприятий специальных проверок, обследований и исследований

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

- селективные микровольтметры;
- анализаторы спектра;
- специальные измерительные комплексы для проведения измерений уровней ЭМИ;
- 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.

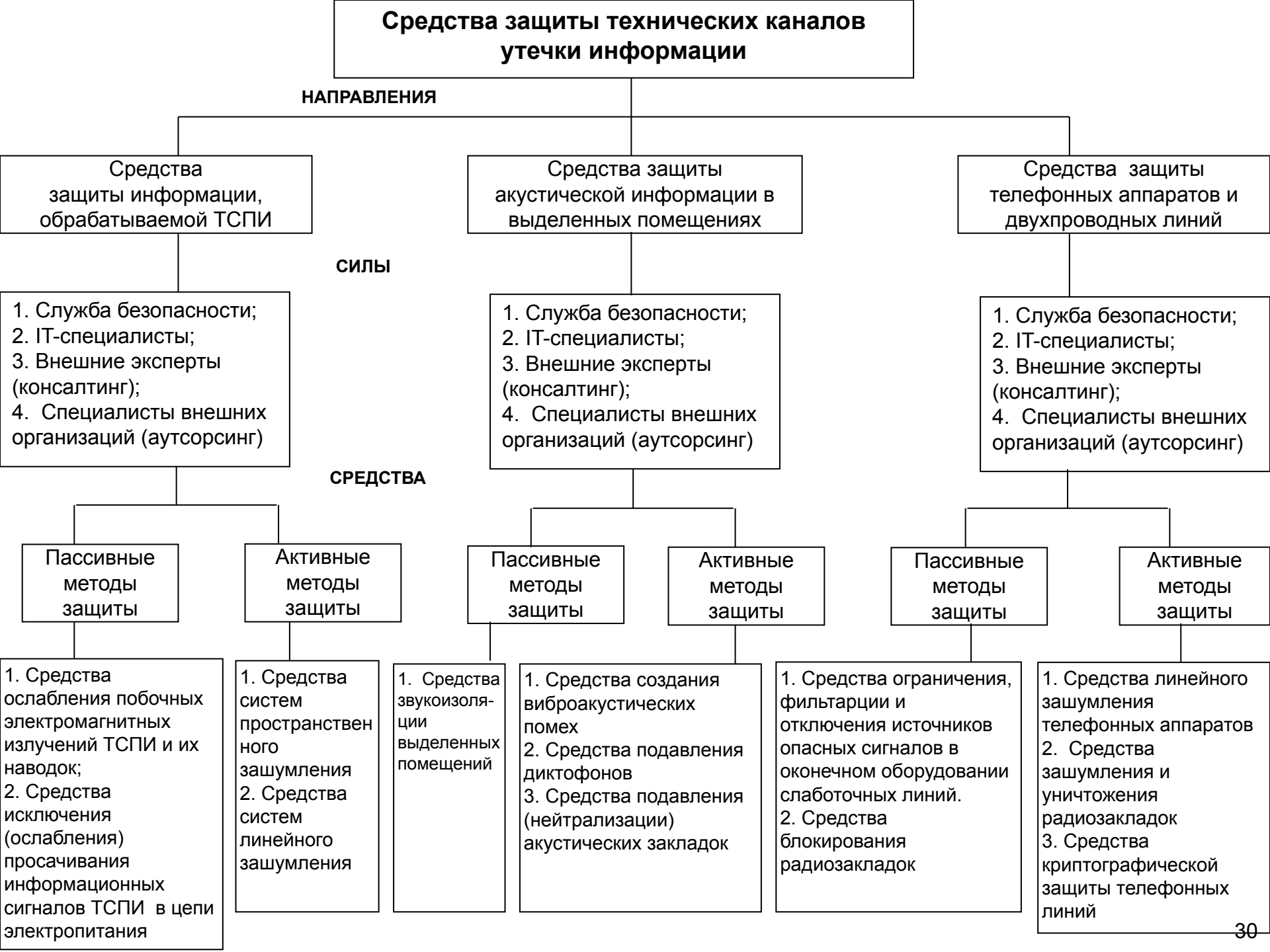
4. **Автоматизированные поисковые комплексы**
- простейшие типовые поисковые программно-аппаратные комплексы;
- специализированные поисковые программно-аппаратные комплексы

Средства обнаружения неизлучающих закладных устройств

1.**Обнаружители пустот:**
- различные ультразвуковые приборы, в том числе медицинские;
- специальные обнаружители пустот (тепловизоры).

2. **Аппаратура обнаружения элементов закладок:**
- нелинейные локаторы;
- 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 технических каналов утечки информации
НАПРАВЛЕНИЯ
Средства защиты информации, обрабатываемой ТСПИ
Средства защиты акустической информации в выделенных помещениях
Средства защиты телефонных аппаратов и двухпроводных линий
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)
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

Технические способы защиты

пассивные технические способы защиты:

- установка систем ограничения и контроля доступа на объектах размещения ТСПИ и выделенных помещениях
- экранирование ТСПИ и соединительных линий средств
- заземление ТСПИ и экранов соединительных линий приборов
- звукоизоляция выделенных помещений
- встраивание в вспомогательные технические средства и системы (ВТСС), обладающие «микрофонным» эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров
- ввод автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ
- монтаж в цепях электропитания ТСПИ, а также в электросетях выделенных помещений помехоподавляющих фильтров

активные технические способы защиты:

- пространственное зашумление, создаваемое генераторами электромагнитного шума
- постановку прицельных помех, генерируемых на рабочих частотах радиоканалов подслушивающих устройств специальными передатчиками
- постановку акустических и вибрационных помех, генерируемых приборами виброакустической защиты
- подавление диктофонов устройствами направленного высокочастотного радиоизлучения;
- зашумления электросетей, посторонних проводников и соединительных линий ВТСС, имеющих выход за пределы контролируемой зоны
- создание режимов теплового разрушения электронных устройств

Экранирование технических средств

Виды экранирования:

- электростаическое;
- магнитостатическое;
- электромагнитное

Экранируются:

- источники ПЭМИ
- монтажные провода 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 х 15 см и толщиной стен 16 см	20 … 25	18 … 19	15 … 17

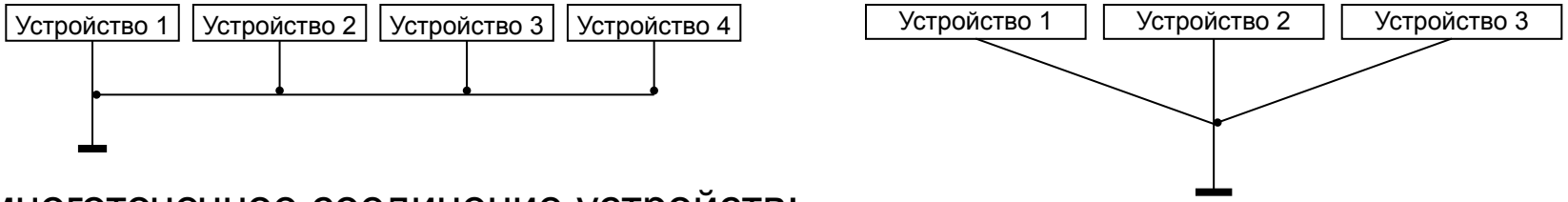
Системы заземления

Элементы заземления

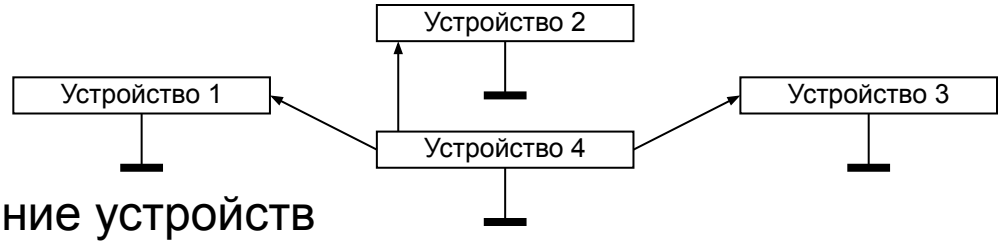
1. Общее заземление
2. Заземляющей кабель
3. Шины и провода, соединяющие заземлитель с объектами

- Для создания контуров заземления наиболее часто используют следующие схемы:

- одноточечное последовательное и параллельное соединение устройств:



- многоточечное соединение устройств:



- гибридное соединение устройств

Фильтрация информационных сигналов

- **Разделительные трансформаторы** – обеспечивают ослабление информационного сигнала и тем самым способствует предотвращению проникновения сигналов по проводникам

- **Помехоподавляющие фильтры** – предназначены для пропускания 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

- Различают фильтры: верхних и нижних частот, полосовые и заграждающие фильтры

- Помехоподавляющие фильтры типа ФП, ФСП устанавливают в осветительную и розеточную сеть в месте их выхода из выделенных помещений

- Средства пространственного зашумления предназначены для исключения перехвата ПЭМИ по 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»

Основные характеристики систем пространственного зашумления

Тип (модель)	Наименование характеристик			
	Диапазон частот, МГц	Спектральная плотность мощности шума, дБ	Вид антенны	Конструкция
ГШ-1000М	0,1 … 1000	40 … 75	Рамочная жесткая	Переносной
ГШ-К-1000М	0,1 … 1000	40 … 75	Рамочная мягкая	Бескорпусной
СМОГ	0,00005 … 1000	55 … 80	Подставки под принтер	Бескорпусной
ГНОМ-3	0,01 … 1000	45 … 75	Рамочная гибкая	Стационарный

Основные характеристики систем пространственного и линейного зашумления

Наименование характеристик	Тип (модель)	
	ГРОМ-ЗИ-4	ГНОМ-2С
Диапазон частот, МГц	20 … 1000	0,01 … 1000
Спектральная плотность мощности шума, дБ	40 … 90	50 … 80
Вид антенны	Телескопическая	Рамочная
Конструкция	Переносной	Стационарный

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.

Звукоизоляция выделенных помещений в зависимости от присвоенных категорий должна быть не менее норм приведенных ниже на слайде в таблице

Нормы звукоизоляции выделенных помещений

Частота, Гц	Звукоизоляция выделенного помещения, дБ		
	1 категории	2 категории	3 категории
500	53	48	43
1000	56	51	46
2000	56	51	46
4000	55	50	45

Звукоизоляция специальных дверей

Конструкция двери	Звукоизоляция (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Дверь звукоизолирующая облегченная	18	30	39	42	45	43
Дверь звукоизолирующая облегченная с зазором более 200 мм	25	42	55	58	60	60
Дверь звукоизолирующая тяжелая	24	36	45	51	50	49
Дверь звукоизолирующая тяжелая, двойная с зазором более 300 мм	34	46	60	60	65	65
Дверь звукоизолирующая тяжелая, двойная с облицовкой тамбура	45	58	65	70	70	70

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)

Технические средства защиты речевой информации

1. Средства виброакустической маскировки - специальные генераторы белого и розового шума

2. Средства подавления диктофонов – портативные (переносные) и стационарные. Портативные подавители диктофонов изготавливаются в обычном кейсе, а стационарные монтируются в месте проведения конфиденциальных переговоров под крышкой стола или в ближайшем шкафу

3. Средствам 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

Пассивные методы защиты оконечного оборудования слаботочных линий от микрофонного эффекта и ВЧ-навязывания:

- ограничение опасных сигналов;
- фильтрация опасных сигналов;
- отключение источников (преобразователей) опасных сигналов

Способы защиты телефонных линий:

- подача в линию во время разговора маскирующих низкочастотных сигналов звукового диапазона, или ультразвуковых колебаний;
- поднятие напряжения в линии во время разговора;
- подача в линию маскирующего низкочастотного сигнала при положенной трубке;
- генерация в линию с последующей компенсацией на определенном участке телефонной линии сигнала речевого диапазона с известным спектром;
- подача в линию импульсов напряжением до 1500 В для выжигания электронных устройств и блоков их питания.

Методы защиты телефонных разговоров с использованием активных средств:

- метод синфазной низкочастотной маскирующей помехи;
- метод высокочастотной маскирующей помехи;
- метод “ультразвуковой” маскирующей помехи;
- метод повышения напряжения;
- метод «обнуления»;
- метод низкочастотной маскирующей помехи;
- компенсационный метод;
- метод «выжигания»

Защита информации с применением **криптографических средств** защиты направлена на исключение ее получения злоумышленником, даже при условии полного перехвата информационных сигналов

Достоинства технических средств криптографической защиты:

- обеспечивают наивысшую степень защиты телефонных переговоров
- защита происходит на всем протяжении линии связи
- могут быть использованы как в кабельных, так и беспроводных системах связи

Недостатки технических средств криптографической защиты:

- необходимость установки однотипного оборудования на всех абонентских пунктах
- потеря времени, необходимого для синхронизации аппаратуры и обмена ключами в начале сеанса защищенного соединения

Второй учебный вопрос:

Программно-аппаратное обеспечение информационной безопасности

Программно-аппаратное обеспечение СОИБ

- ***Программно-аппаратное обеспечение СОИБ*** **– совокупность возможностей системного программного обеспечения (операционных систем и оболочек), прикладного программного обеспечения (СУБД, текстовых, табличных редакторов и др.), специального программного обеспечения в виде компьютерных служебных приложений, а также специальных технических устройств, выполняющих функции защиты информации в информационной системе объекта**

Направления деятельности программно-аппаратного обеспечения СОИБ

- **Программная защита информации**, под которой будем понимать совокупность возможностей программного обеспечения (как системного, так и прикладного) современных информационных и автоматизированных систем ХС по защите хранящейся и обрабатывающейся в них информации

- **Программно-аппаратная защита информации**, которая представляет собой совокупность возможностей аппаратных (физических) устройств современных информационных и автоматизированных систем ХС, а также установленного на них, или взаимодействующего с ними программного обеспечения по защите информации, хранящейся и обрабатывающейся в данных системах

Подсистема программно-аппаратного обеспечения СОИБ

НАПРАВЛЕНИЯ

Программная защита информации

СИЛЫ

1. Специалисты IT-подразделения
2. Внешние организации (специалисты), осуществляющие аутсорсинговую деятельность: поставка, установка, сопровождение ПО и др.;
3. Внешние организации (специалисты), осуществляющие консалтинговую деятельность
4. Специалисты службы безопасности

СРЕДСТВА

1. Средства защиты информации, встроенные в системное ПО:
- средства аутентификации;
- средства контроля и управления доступом;
- средства администрирования;
- средства аудита;
- средства файловой системы.
2. Средства защиты информации, встроенные в прикладное ПО (приложения);
- средства аутентификации;
- защита от модификации.
3. Средства электронной цифровой подписи и мандатного доступа
4. Антивирусное программное обеспечение.
5. Программное обеспечение для защиты от спама
6. Программное обеспечение для защиты от шпионских программ
7. Программное обеспечение для шифрования и кодирования информации
8. Программы архивирования информации
9. Программные сканеры безопасности
10. Программные межсетевые экраны

Программно-аппаратная защита информации

1. Специалисты IT-подразделения
2. Внешние организации (специалисты), осуществляющие аутсорсинговую деятельность: поставка, установка, сопровождение и др.;
3. Внешние организации (специалисты), осуществляющие консалтинговую деятельность
4. Специалисты службы безопасности

1. Средства вычислительной техники в защищенном (специальном) исполнении
2. Средства аутентификации (аппаратные ключи, смарт-карты, брелоки и др.).
3. Системы резервного копирования.
4. Средства криптографической защиты.
5. Средства маршрутизации и VPN
6. Межсетевые экраны

Классификация программных средств защиты информации

Средства защиты информации, встроенные в операционную систему

- ***Аутентификация***
- ***Авторизация***
- ***Аудит***

Аутентификация

Аутентификация (от лат. «установление подлинности»), механизм, предотвращающий доступ к сети нежелательных лиц и разрешающий вход для легальных пользователей

Приемы доказательства аутентичности:

а) аутентифицируемый может продемонстрировать знание некоего общего для обеих сторон секрета – как правило, слова - пароля;

б) аутентифицируемый может продемонстрировать, что он владеет неким уникальным предметом (физическим ключом), в качестве которого может выступать, например, электронная магнитная карта (смарт-карта), устройства, типа Touch-memory, брелоки и др.;

в) аутентифицируемый может доказать свою идентичность, используя собственные уникальные биохарактеристики: рисунок радужной оболочки глаза или отпечатки пальцев, которые предварительно были занесены в базу данных аутентификатора

Авторизация

- *Авторизация.* Цель процедуры авторизации состоит в том, чтобы предоставить каждому легальному пользователю именно те виды доступа и к тем ресурсам, которые были для него определены администратором системы

Формы предоставления правил доступа:

- избирательный доступ;
- мандатный доступ

Аудит

- *Аудит.* Аудит, осуществляемый встроенными средствами операционной системы, заключается в фиксации в системном журнале событий, связанных с доступом к защищаемым системным ресурсам

Аудит используется и для того, чтобы контролировать даже неудачные попытки проникновения в систему

Система аудита рассматривается в качестве последнего рубежа в борьбе с нарушениями

Средства защиты информации, встроенные в пользовательские приложения

Встроенные механизмы защиты системы управления базами данных (СУБД) Microsoft Access:

1. Защита файлов баз данных, которая заключается в реализации следующих возможностей:
- задать пароль, который в последующем позволит выполнить какие-либо действия над файлом базы данных только после его ввода;
- задать разрешения на работу над базой данных в целом или на ее элемент (таблицу, запрос, отчет и др.) конкретному пользователю или группе пользователей;
- закодировать файл базы данных под другим именем и, в последующем, раскодировать его
2. Наличие служебных программ, выполняющих следующие дополнительные защитные функции:
- создание резервной копии базы данных;
- сжатие и восстановление базы данных

Средства защиты информации, встроенные в пользовательские приложения
(продолжение)

Средства защиты текстового редактора Microsoft Word, позволяют реализовать следующие функции:

- ввести ограничение на форматирование, путем уменьшения перечня разрешенных стилей форматирования текстового документа;
- ввести ограничение на редактирование, путем разрешения указанного способа или нескольких способов редактирования (только чтение, запись исправлений, ввод данных и др.) текстового документа или его части;
-установить перечень пользователей или групп пользователей, для которых установлены разрешения на выполнение некоторых операций над документом

Средства защиты табличного редактора Microsoft Excel:

- «защитить лист», при этом можно указать перечень разрешенных действий над рабочим листом и задать пароль;
- «разрешить изменение диапазонов», в этом случае можно защитить от изменений некоторый, определенный пользователем, диапазон ячеек;
- «защитить книгу», при этом можно защитить от изменений структуру рабочей книги, а также интерфейс рабочего окна;
- «защитить книгу и дать общий доступ». Эта команда предоставляет общий доступ к рабочей книге с запретом на отмену режима ее модификации

Средства защиты информации, поставляемые в виде отдельных программных модулей, оболочек, сред

•Межсетевой экран (firewall, брандмауэр) - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных

Типы межсетевых экранов:

-межсетевые экраны прикладного уровня;

-межсетевые экраны с пакетной фильтрацией;

-гибридные межсетевые экраны

Оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся ***в блокировке запрещенного трафика***

Межсетевые экраны прикладного уровня

- Межсетевые экраны прикладного уровня (прокси-экраны) это программные пакеты, базирующиеся на операционных системах общего назначения (Windows NT или Unix) или на аппаратной платформе межсетевых экранов. Межсетевой экран обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен.
- В межсетевом экране прикладного уровня каждому разрешаемому протоколу должен соответствовать свой собственный модуль доступа (лучшим модулем доступа считаются тот, который специально построен для разрешаемого протокола.
- МЭ используют модули доступа для входящих подключений. Модуль доступа в межсетевом экране принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений.
- Межсетевой экран скрывает адреса систем, расположенных по другую сторону от него. Так как все соединения инициируются и завершаются на интерфейсах межсетевого экрана, внутренние системы сети не видны напрямую извне, что позволяет скрыть схему внутренней адресации сети.

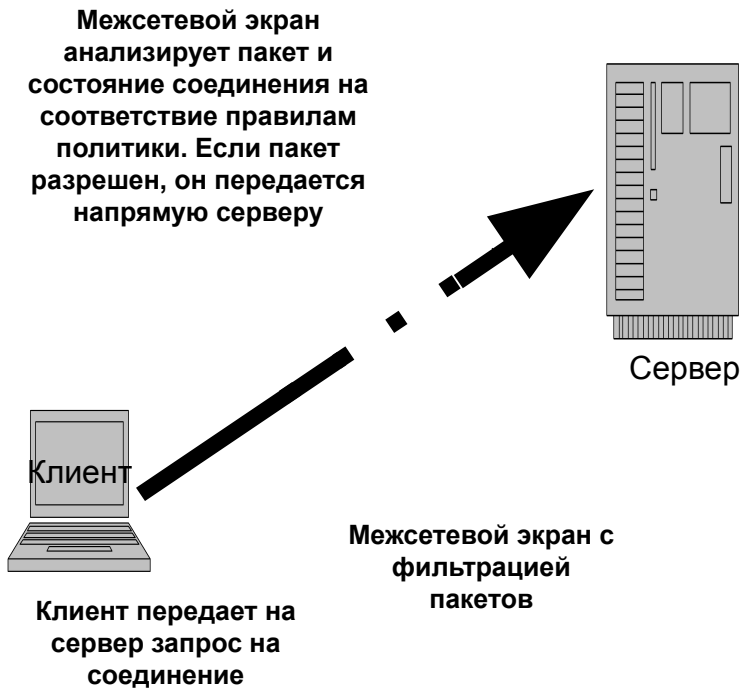
Порядок соединения модуля доступа межсетевого экрана прикладного уровня

Межсетевые экраны с пакетной фильтрацией

- Межсетевые экраны с пакетной фильтрацией могут также быть программными пакетами, базирующимися на операционных системах общего назначения (таких как Windows NT и Unix) либо на аппаратных платформах межсетевых экранов. Межсетевой экран имеет несколько интерфейсов, по одному на каждую из сетей, к которым подключен экран. Доставка трафика из одной сети в другую определяется набором правил политики. Если правило не разрешает явным образом определенный трафик, то соответствующие пакеты будут отклонены или аннулированы межсетевым экраном.
- Правила политики усиливаются посредством использования фильтров пакетов. Фильтры изучают пакеты и определяют, является ли трафик разрешенным, согласно правилам политики и состоянию протокола (проверка с учетом состояния).
- При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране, а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет и состояние соединения правилами политики. Если это так, пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.
- Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом, работающим через IP

Межсетевые экраны с фильтрацией пакетов имеют возможность поддержки большего объема трафика, т. к. в них отсутствует нагрузка, создаваемая дополнительными процедурами настройки и вычисления, имеющими место в программных модулях доступа.

Межсетевые экраны, работающие только посредством фильтрации пакетов, не используют модули доступа, и поэтому трафик передается от клиента непосредственно на сервер



Гибридные межсетевые экраны

•Гибридные межсетевые экраны это устройства двух вариантного исполнения:

-в первом случае это межсетевой экран прикладного уровня который в дополнение к своему функционалу реализует метод поддержки протоколов необходимых системе безопасности при работе сетевых администраторов, для которых не существует определенных модулей доступа;

-во втором случае это межсетевые экраны с пакетной фильтрацией в которые добавили некоторые модули доступа использование которых позволяет обеспечить более высокий уровень безопасности некоторых широко распространенных протоколов

Средства создания виртуальных защищенных сетей (VPN)

•VPN (Virtual Private Network - виртуальная частная сеть) представляет собой логическую сеть, создаваемая поверх другой сети, например корпоративной (интранет)

•Под *инкапсуляцией* в компьютерных сетях понимают метод их согласования, применимый только для согласования транспортных протоколов. Инкапсуляция (тунель) может быть использована, когда две сети с одной транспортной технологией необходимо соединить через сеть, использующую другую транспортную технологию

•VPN состоит из двух частей: внутренняя (подконтрольная) сеть, которых может быть несколько, и внешняя сеть, по которой проходит инкапсулированное соединение, обычно это - Интернет

Основные функциональные возможности VPN:

1.Кодирование межсетевых потоков;
2.Создание периметра безопасности;
3.Выборочное кодирование трафика;
4.Управление ключевой системой;
5.Регистрация событий, мониторинг и управление межсетевыми потоками;
6.Защита соединений с мобильными клиентами

Средства обнаружения и предотвращения атак

•Программные системы обнаружения атак - IDS (Intrusion Detection System) – это системы которые на основе шаблонных и сигнатурных методов способны обнаруживать такие категории атак, как аномалии и злоупотребления.

Системы обнаружения атак:

-обнаружение атак на уровне сети (network-based) на основе анализа сетевого трафика;

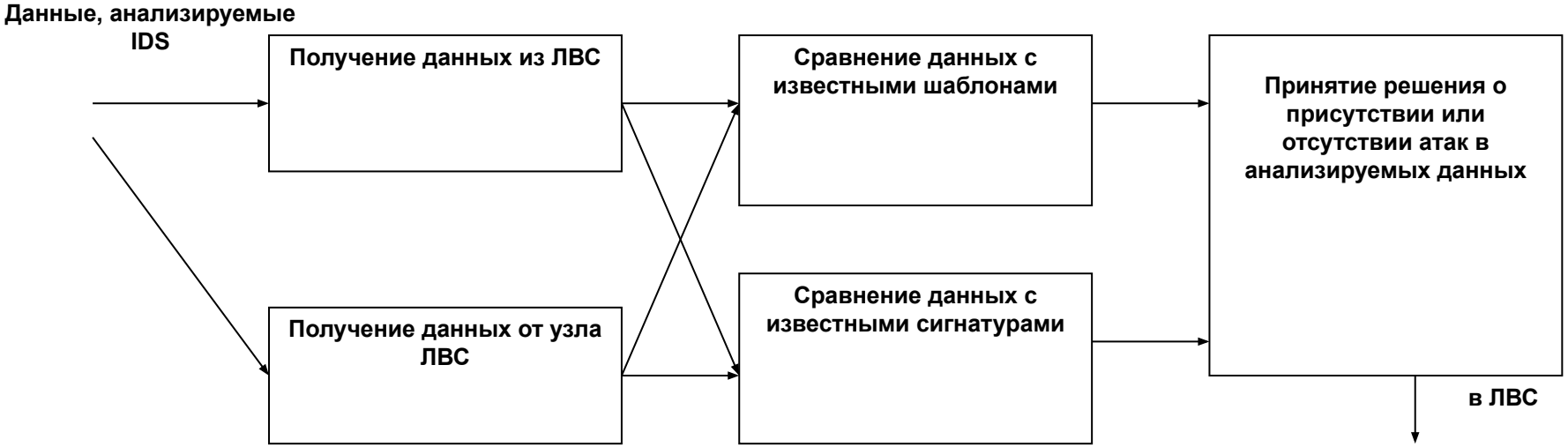
-обнаружение атак на уровне хоста (host-based) на основе анализа например данных регистрационного журнала операционной системы

Средства обнаружения атак:

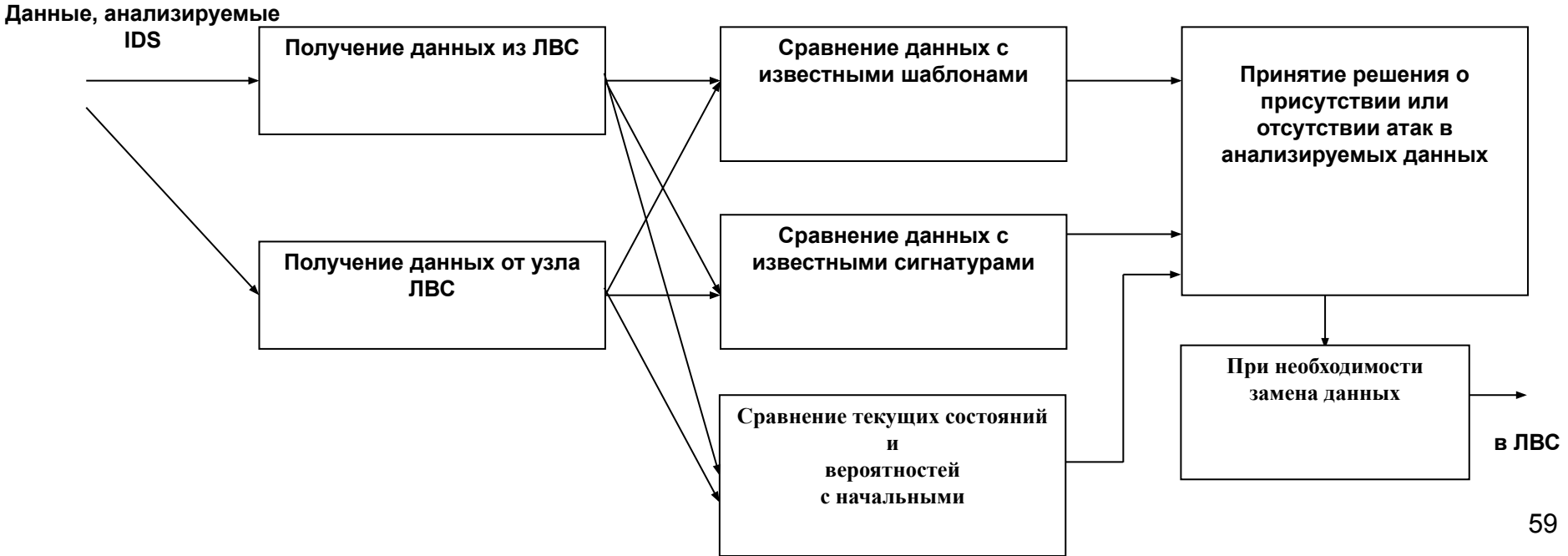
- сканеры безопасности;

-сетевые анализаторы

Общая схема обнаружения сетевых атак современными IDS



Структурная схема обнаружения и предотвращения сетевых атак



Средства защиты от компьютерных вирусов

№ пп	Название компании	Название и версия антивирусного ПО	Интегральный оказатель эффективности	Занимаемое место
1	AVIRA	AntiVir PE Premium	99,45%	2
2	G DATA Security	AntiVirusKit (AVK)	99,31%	3
3	Alwil Software	avast! Professional	95,24%	11
4	GriSoft	AVG Anti-Malware	97,75%	6
5	Softwin	BitDefender Prof.+	97,51%	10
6	Doctor Web	Dr. Web (BETA**)	89,87%	17
7	MicroWorld	eScan Anti-Virus	97,53%	9
8	Fortinet	FortiClient	89,98%	16
9	Frisk Software	F-Prot Anti-Virus	92,20%	13
10	F-Secure	F-Secure Anti-Virus	97,57%	8
11	Kaspersky Labs	Kaspersky AV	98,46%	5
12	McAfee	McAfee VirusScan+	93,15%	12
13	Microsoft	Microsoft OneCare	90,37%	15
14	ESET	NOD32 Anti-Virus	97,60%	7
15	Norman ASA	NormanVirusControl	90,93%	14
16	Symantec	Norton Anti-Virus	98,80%	4
17	AEC	TrustPort AV WS	99,64%	1

Классический механизм обнаружения вирусов, основан на сравнении исследуемого программного кода с образцами программных кодов известных вирусов;

В современном антивирусном ПО используются новые антивирусные технологии – *проактивные методы защиты*:

- поведенческий блокиратор;
- эвристический анализатор;

Критерии выбора антивирусной защиты:

1. Надежность работы антивируса, для оценки которой можно использовать результаты независимых тестирований.
2. Простота использования антивируса (наличие понятного интерфейсе программы, отсутствие сложных настроек, возможность обеспечения базового уровня защищенности при использовании всех настроек «по умолчанию», наличие режима автоматического запуска и др);
3. Интегрированные решения (использование кроме антивирусной защиты фильтров для защиты от спама, межсетевых экранов, запрет посещения опасных сетевых ресурсов и др);
4. Комплексность защиты (применение в дополнение к технологическим и организационные решения.
5. Качество защиты

Программно-аппаратная защита

Программно-аппаратная защита информации представляет собой совокупность возможностей аппаратных устройств современных информационных и автоматизированных систем объекта, а также установленного на них, или взаимодействующего с ними программного обеспечения по защите информации, хранящейся и обрабатывающейся в данных системах

Виды программно-аппаратных средств защиты:

1. Средства вычислительной техники в защищенном (специальном) исполнении
2. Средства аутентификации (аппаратные ключи, смарт-карты, брелоки и др.)
3. Системы резервного копирования
4. Средства криптографической защиты
5. Средства маршрутизации и VPN
6. Межсетевые экраны

Программно-аппаратные средства аутентификации

- Современные программно-аппаратные средства аутентификации основаны на использовании электронных ключей или, так называемых, eToken

- Данные устройства представляют собой персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с технологиями цифровых сертификатов и электронной цифровой подписи (ЭЦП)

- EToken выпускаются в виде нескольких устройств: USB-ключ, смарт-карта, брелок, которые имеют встроенный модуль флэш-памяти объемом от 512 до 4096 Мб

Программно-аппаратные средства криптографической защиты

Состав типового программно-аппаратного комплекса:

-программное обеспечение;

-аппаратный модуль

Типовые функции средств:

- «прозрачное», т.е. незаметное для пользователя шифрование информации;
- шифрование данных в соответствии с международными и национальными стандартами;
- защиту программно-аппаратных ресурсов компьютера от несанкционированного доступа (НСД);
- идентификацию и аутентификацию пользователя при запуске компьютера до запуска BIOS;
- контроль целостности загружаемой ОС;
- блокировку запуска компьютера при НСД;
- регистрацию событий НСД;
- аппаратную блокировку от несанкционированной загрузки операционной системы с гибкого диска, CD-ROM диска, DVD-диска и с USB Flash-диска

Средства маршрутизации и VPN, сетевое экранирование

•Маршрутизатор или роутер (от англ. router) представляет собой сетевое устройство, которое принимает решение о порядке и маршруте пересылки пакетов сетевого уровня (третий уровень в многоуровневой модели OSI) между различными сегментами сети на основании информации о ее топологии, а также определённых правил

Функции защиты информации:

1. Контроль доступа, фильтрация портов
2. Ограничение/фильтрация содержания
3. Защищенные сети – VPN
4. Журналирование

Третий учебный вопрос:

Аудит информационной безопасности

Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности

Основные направления деятельности в области аудита информационной безопасности

1. Аттестация объектов информатизации по требованиям безопасности информации:
   - ✔ аттестация автоматизированных систем, средств связи, обработки и передачи информации;
   - ✔ аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
   - ✔ аттестация технических средств, установленных в выделенных помещениях

2. Контроль защищенности информации ограниченного доступа:
   - ✔ выявление технических каналов утечки информации и способов несанкционированного доступа к ней;
   - ✔ контроль эффективности применяемых средств защиты информации

Основные направления деятельности в области аудита информационной безопасности (продолжение)

3. Специальные исследования технических средств на наличие побочных электромагнитных излученийи наводок (ПЭМИН):

- ✔ персональные ЭВМ, средства связи и обработки информации;
- ✔ локальные вычислительные системы;
- ✔ оформления результатов исследований в соответствии с требованиями ФСБ и ФСТЭК

4. Проектирование объектов в защищенном исполнении:

- ✔ разработка концепции информационной безопасности;
- ✔ проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;
- ✔ проектирование помещений, предназначенных для ведения конфиденциальных переговоров

Виды аудита информационной безопасности

- Внешний аудит
- Внутренний аудит

Внешний аудит – это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Внешний аудит рекомендуется (а для ряда финансовых учреждений и акционерных обществ требуется) проводить регулярно

Внутренний аудит – представляет собой непрерывную деятельность, которая осуществляется на основании документа, обычно носящего название «Положение о внутреннем аудите», и в соответствии с планом, подготовка которого осуществляется подразделением внутреннего аудита и утверждается руководством организации. Аудит безопасности информационных систем является одной из составляющих ИТ – аудита

Цели аудита информационной безопасности

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационных систем;
- оценка текущего уровня защищенности информационных систем;
- локализация узких мест в системе защиты информационных систем;
- оценка соответствия информационных систем существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности информационных систем

Дополнительные задачи аудита информационной безопасности

- разработка политик безопасности и других организационно-распорядительных документов по защите информации и участие в их внедрении в работу организации;
- постановка задач для IT-персонала, касающихся обеспечения защиты информации;
- участие в обучении пользователей и обслуживающего персонала информационных систем вопросам обеспечения информационной безопасности;
- участие в разборе инцидентов, связанных с нарушением информационной безопасности;
- прочие задачи

Основные этапы аудита информационной безопасности

- инициирование процедуры аудита;
- сбор информации аудита;
- анализ данных аудита;
- выработку рекомендаций;
- подготовку аудиторского отчета

Инициирование процедуры аудита информационной безопасности

Должны быть решены следующие организационные вопросы:

- права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о внутреннем (внешнем) аудите;
- аудитором должен быть подготовлен и согласован с руководством план проведения аудита;
- в положении о внутреннем аудите должно быть закреплено, в частности, что сотрудники компании обязаны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию;
- должны быть определены границы проведения обследования

Сбор информации аудита информационной безопасности

- ✔ документация на информационную систему;
- ✔ информация об организационной структуре пользователей информационной системы и обслуживающих подразделений;
- ✔ существующие риски и требования безопасности, предъявляемые к информационной системе;
- ✔ распределение механизмов безопасности по структурным элементам и уровням функционирования информационной системы

Анализ данных аудита информационной безопасности

Первый подход – самый сложный, базируется на анализе рисков

Второй подход – самый практичный, опирается на использовании стандартов информационной безопасности

Третий подход – наиболее эффективный, предполагает комбинирование первых двух

Выработка рекомендаций информационной безопасности

рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности

Подготовка аудиторского отчета

Отчет должен содержать следующие пункты:

1. Описание целей проведения аудита
2. Характеристику обследуемой ИС
3. Границы проведения аудита и используемых методов
4. Результаты анализа данных аудита
5. Выводы
6. Рекомендации по устранению существующих недостатков и совершенствованию системы защиты

Литература:

1. В.Г.Олифер, Н.А.Олифер Сетевые операционные системы, - СПб.: Питер, 2002
2. Independent comparatives of Anti-Virus Software, [Электронный документ], Http://www.av-comparatives.org
3. Касперский Е. Компьютерное зловредство, - СПб.: Питер, 2007