

Лекция 11. Управление безопасностью ИС.

Учебные вопросы

1. Задачи администрирования безопасности ИС
2. Обеспечение информационной безопасности
3. Модель многослойной защиты
4. Шифрование
5. Протоколирование и аудит

Основные задачи администрирования безопасности ИС

- **Основная цель организации администрирования безопасности ИС** – реализация на процедурном уровне задачи обеспечения политики информационной безопасности.
- **Инструменты администрирования** – программные и аппаратные средства, обеспечивающие выполнение политики безопасности.

Политика безопасности

- **Политика безопасности** – совокупность документированных решений, принимаемых на различных уровнях руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.
- Политика безопасности вырабатывается на основе анализа рисков защищенности системы.

Программа безопасности верхнего уровня

- Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации.
- Цели программы:
 - Управление рисками (оценка рисков, выбор эффективных решений);
 - Координация деятельности в области информационной безопасности
 - Стратегическое планирование
 - Контроль деятельности в области информационной безопасности.
- Контроль деятельности в области ИБ должен гарантировать, во-первых, что действия организации не противоречат законам, во-вторых, что состояние безопасности в организации соответствует требованиям и реагировать на случаи нарушений.

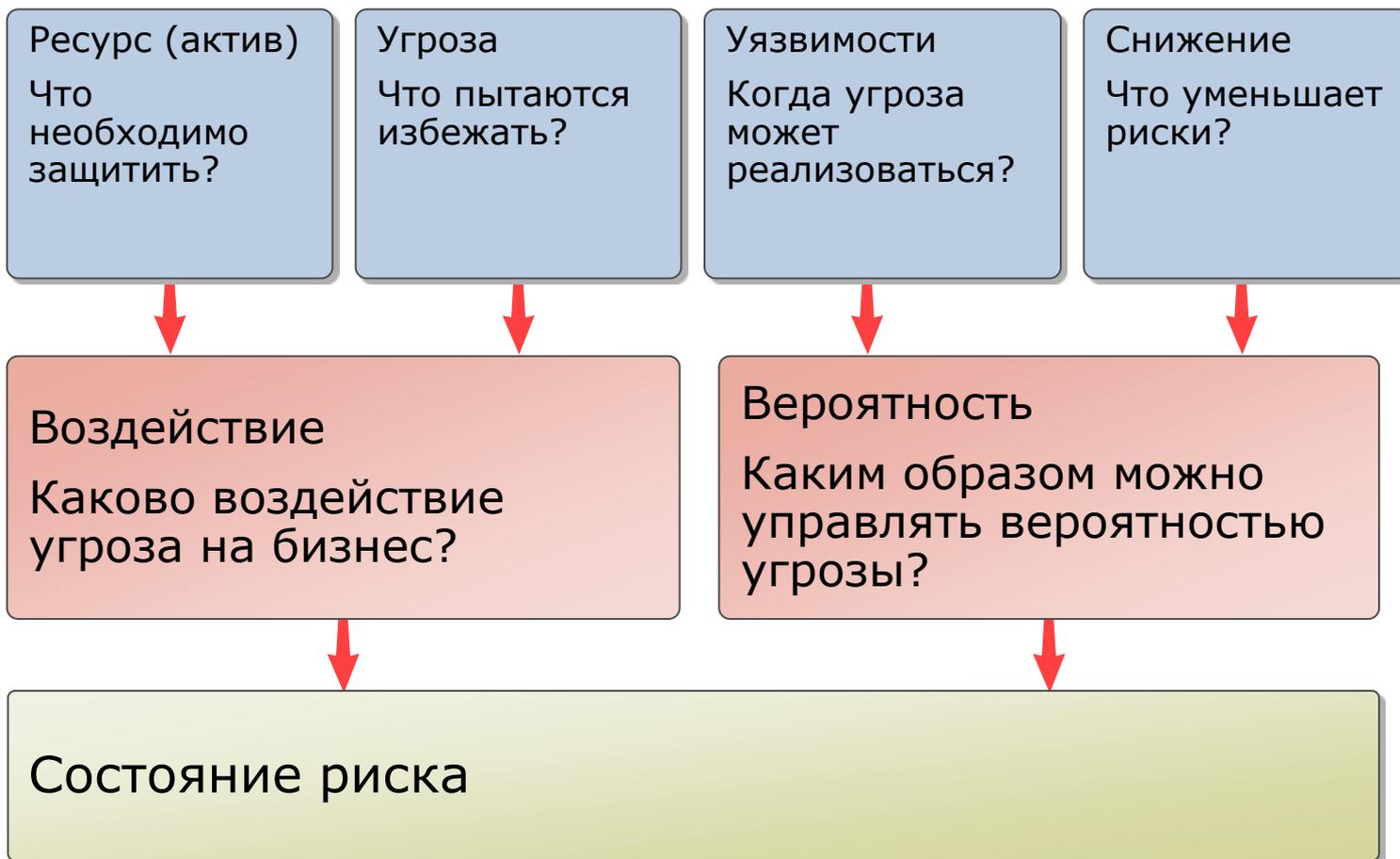
Программы безопасности процедурного (служебного) уровня

- Цель программы процедурного уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов.
- На нижнем уровне осуществляется выбор механизмов защиты, технических и программных средств.
- Ответственность за реализацию программ нижнего уровня обычно несут администраторы соответствующих сервисов.

Процесс управления рисками



Схема рисков



Обеспечение информационной безопасности

- Обеспечение безопасности информации в ИС подразумевает построение подсистем, входящих в **систему обеспечения безопасности информации – СОБИ**.
- СОБИ строится как иерархическая, многоуровневая система.
- Комплексный подход, применяемый при построении СОБИ, предусматривает наличие нескольких уровней защиты, которые определяют требования по обеспечению безопасности информации на всех этапах ее обращения в КИС.

Подсистемы системы информационной безопасности

- **Подсистема поддержки доверенной информационной среды (ДИС)** предназначена для поддержания целостной программно-аппаратной среды ИС, обеспечения гарантий доверительности пользователей ИС к предоставляемой системой информации и сервисам.
- **Подсистема аутентификации и идентификации** предназначена для проведения процедур аутентификации/идентификации сетевых сущностей, входящих в состав ИС, на всех этапах обработки и обращения информации в ИС. Подсистема тесно взаимодействует с подсистемой контроля доступа.

Подсистемы системы информационной безопасности

- **Подсистема контроля доступа** предназначена для управления и контроля за доступом пользователей к АРМ, серверам, прикладным системам, системным и сетевым сервисам и др., входящим в состав КИС, на базе многоуровневой Политики безопасности.
- **Подсистема защиты потоков** предназначена для создания доверенных каналов связи между структурными составляющими КИС.
- **Подсистема аудита и регистрации** осуществляет сбор и хранение информации об общем состоянии программных и технических компонентов, функционирующих отдельно или входящих в состав подсистем безопасности, и предназначена для предварительного анализа данной информации.

Подсистемы системы информационной безопасности

- **Подсистема управления** – предназначена для оперативного управления как отдельными составляющими СОБИ, так и системой в целом, в соответствии с Политикой безопасности.
- Подсистема включает в себя механизмы:
 - анализ информации с консолей мониторинга средств защиты;
 - система поддержки принятия решения об оперативном усилении/ослаблении политики безопасности в отдельных элементах или узлах СОБИ и противодействия внешним и внутренним атакам;
 - управление отдельными средствами и комплексами защиты информации и др.

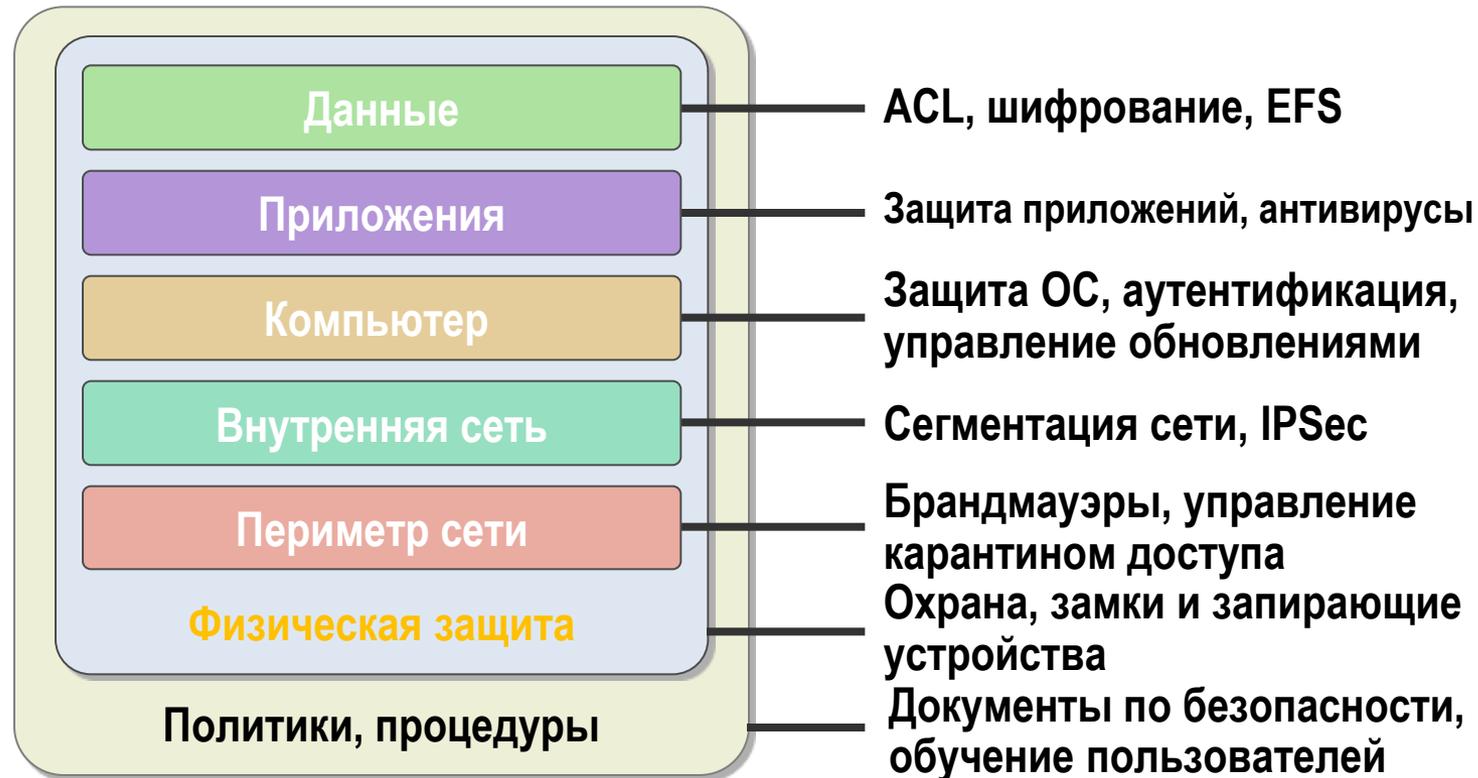
Наборы подсистем защиты

- СОБИ для каждой организации представляет собой различный набор подсистем (решений), который не является стандартным и различен в зависимости от бизнес-задач, решаемых информационной системой.
- Однако можно выделить несколько базовых подсистем, составляющих СОБИ корпоративной информационной системы практически любой организации:
 - Подсистема безопасного подключения корпоративной сети к Интернет;
 - Подсистема защиты корпоративной электронной почты;
 - Подсистема защиты от вредоносных программ и компьютерных вирусов;
 - Подсистема защиты внутренних и внешних информационных потоков;
 - Подсистема предотвращения вторжений;
 - Подсистема защиты информации персональных компьютеров от НСД;
 - Подсистема контроля целостности программной среды;
 - Подсистема резервного копирования и восстановления данных.

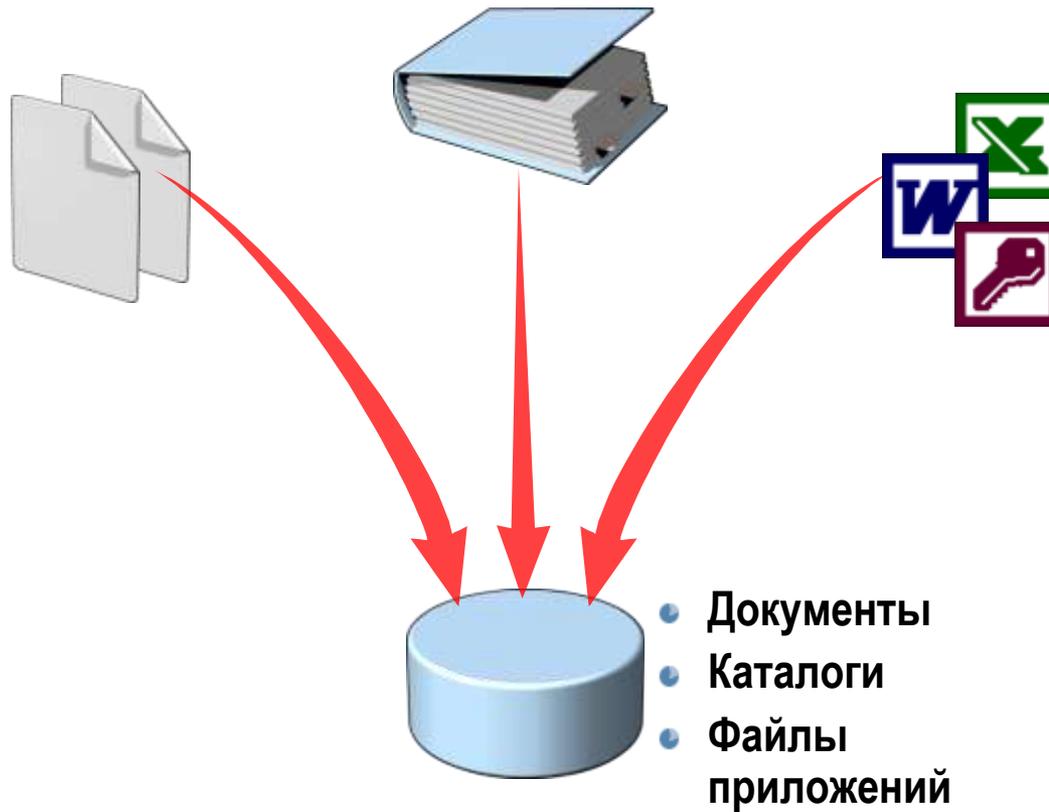
Модель многослойной защиты

Использование многослойной модели защиты позволяет:

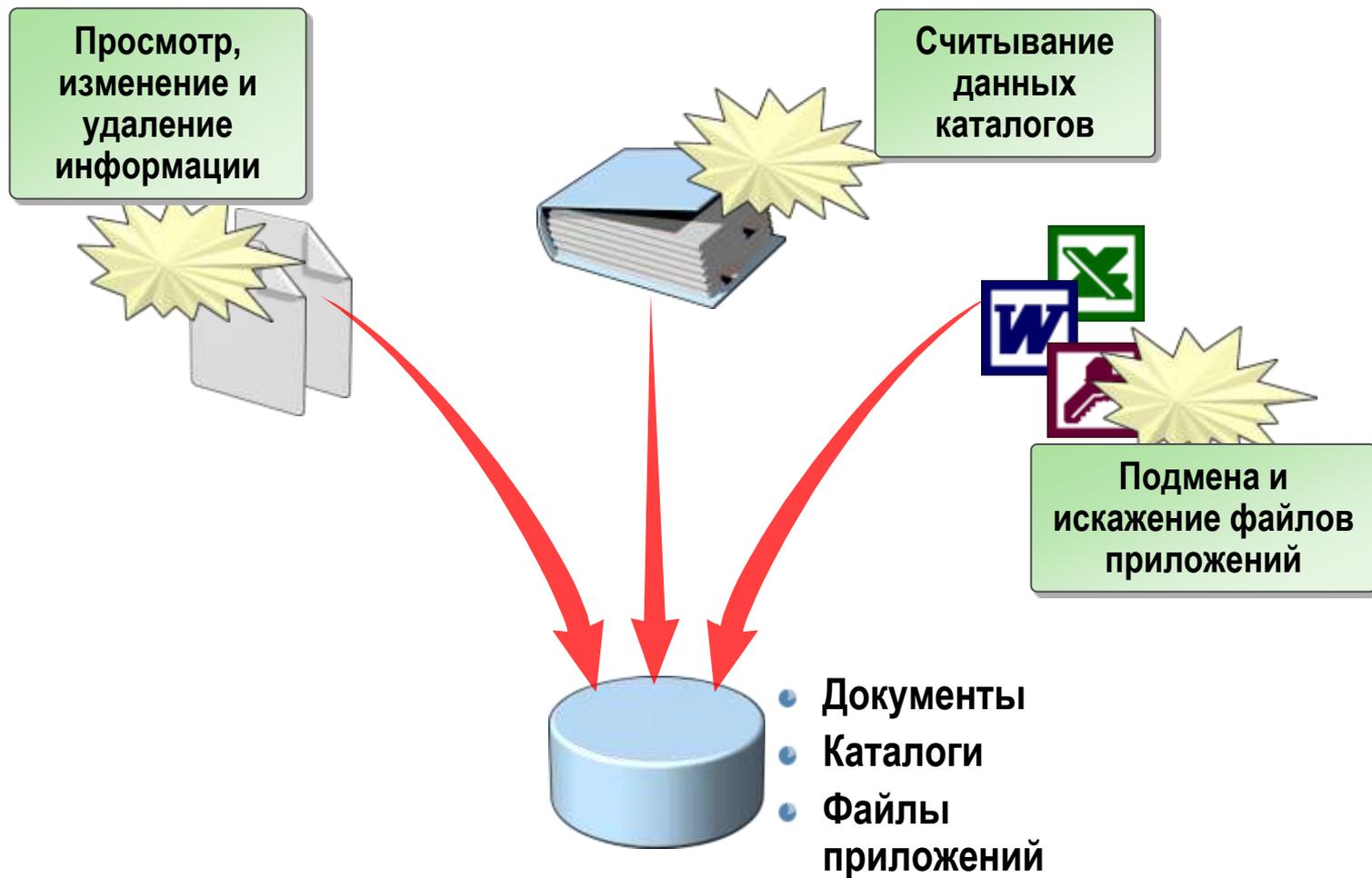
- Уменьшить шанс успеха атаки
- Увеличить вероятность обнаружения атаки



Описание уровня данных



Угрозы безопасности на уровне данных



Задачи администрирования - уровень данных

- На уровне данных задача администрирования – управление доступом к данным.
- Политики управления доступом – дискреционная, мандатная, ролевая.
- Инструменты управления доступом – списки прав доступа (ACL), метки доступа, биты защиты и т.п.
- Доступ к данным регулируется на уровне файловой системы – доступ к файлам, на уровне объектов БД – доступ к таблицам, представлениям.
- Шифрование данных – установка и администрирование РКІ (инфраструктура открытых ключей).
- Обеспечение регулярного резервного копирования.

Управление доступом

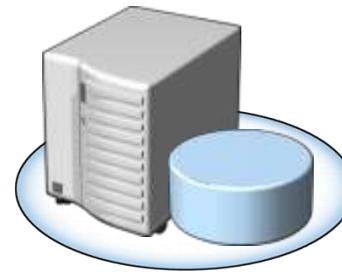
- Управление доступом на уровне данных в ОС Windows эффективно выполняется на носителях с файловой системой **NTFS**.
- Файловая система NTFS обеспечивает поддержку хранения списков прав доступа (ACL) и механизм их использования при выдаче разрешений и запретов на операции с файлами и каталогами.

Описание уровня приложений

- Данный уровень включает как клиентскую, так и серверную часть приложения



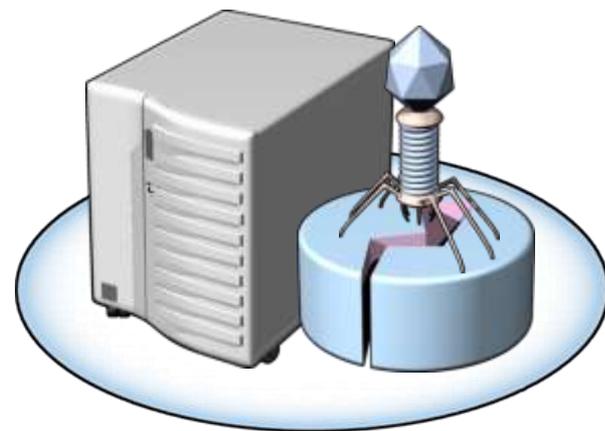
**Клиентские приложения:
Microsoft Outlook, Microsoft
Office Suite**



**Серверные приложения: Web
Servers, Exchange Server, SQL
Server**

Угрозы уровня приложений

- Потеря функциональности приложения
- Исполнение вредоносного кода
- Чрезмерная нагрузка на приложение – DoS атака
- Нежелательное использование приложения



Задачи администрирования - уровень приложений

- На уровне приложений основные задачи администрирования – определение прав пользователей на запуск и управление процессами.
- Установление прав доступа к прикладным программам и процессам.
- Управление групповыми политиками на ограничение использования ПК.

Описание уровня хоста

- Включает отдельные ПК пользователей сети
- Часто играет специальную роль в ИС
- Обеспечение ИБ хоста требует баланса между защищенностью и удобством работы пользователя



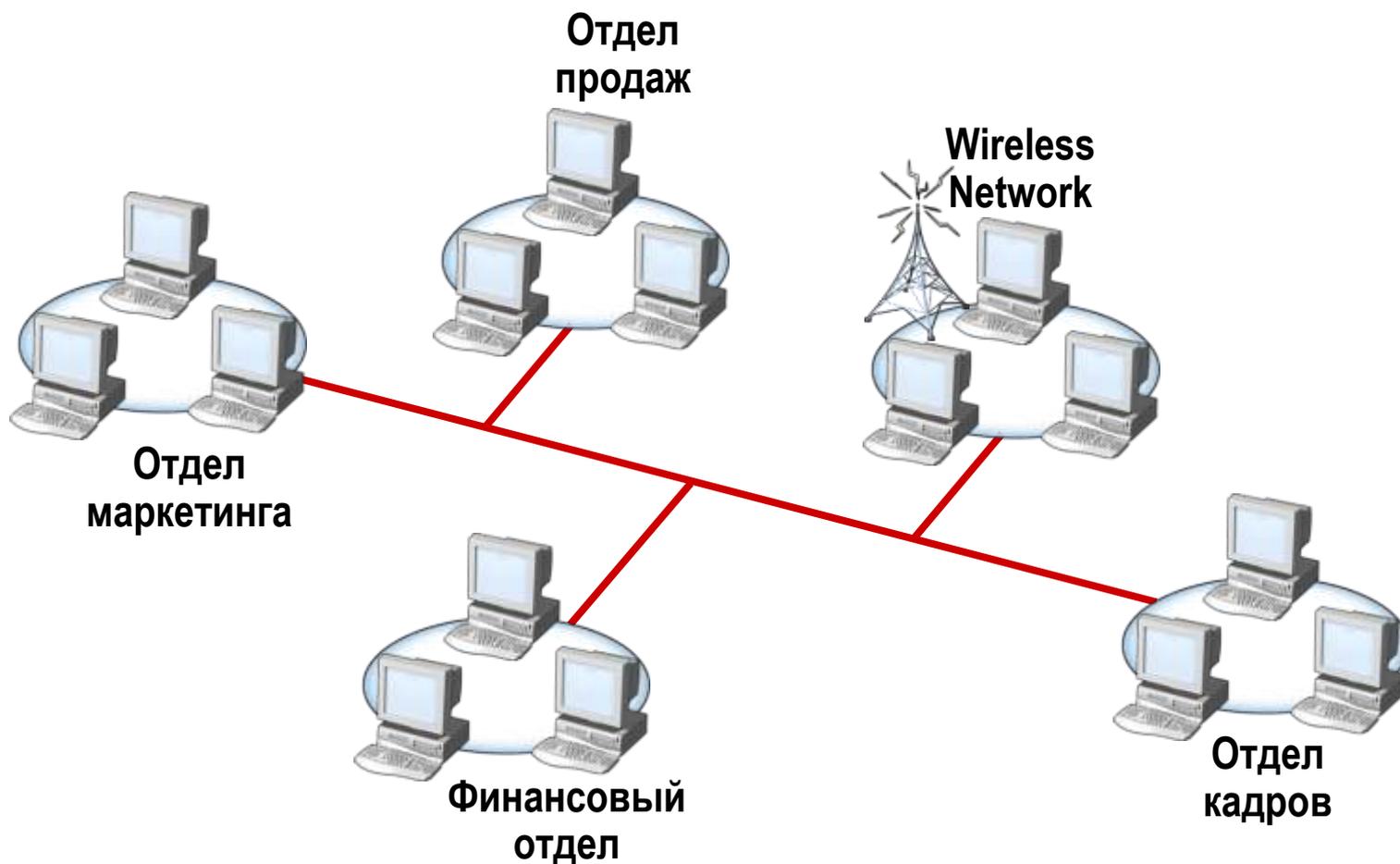
Уязвимости уровня хоста



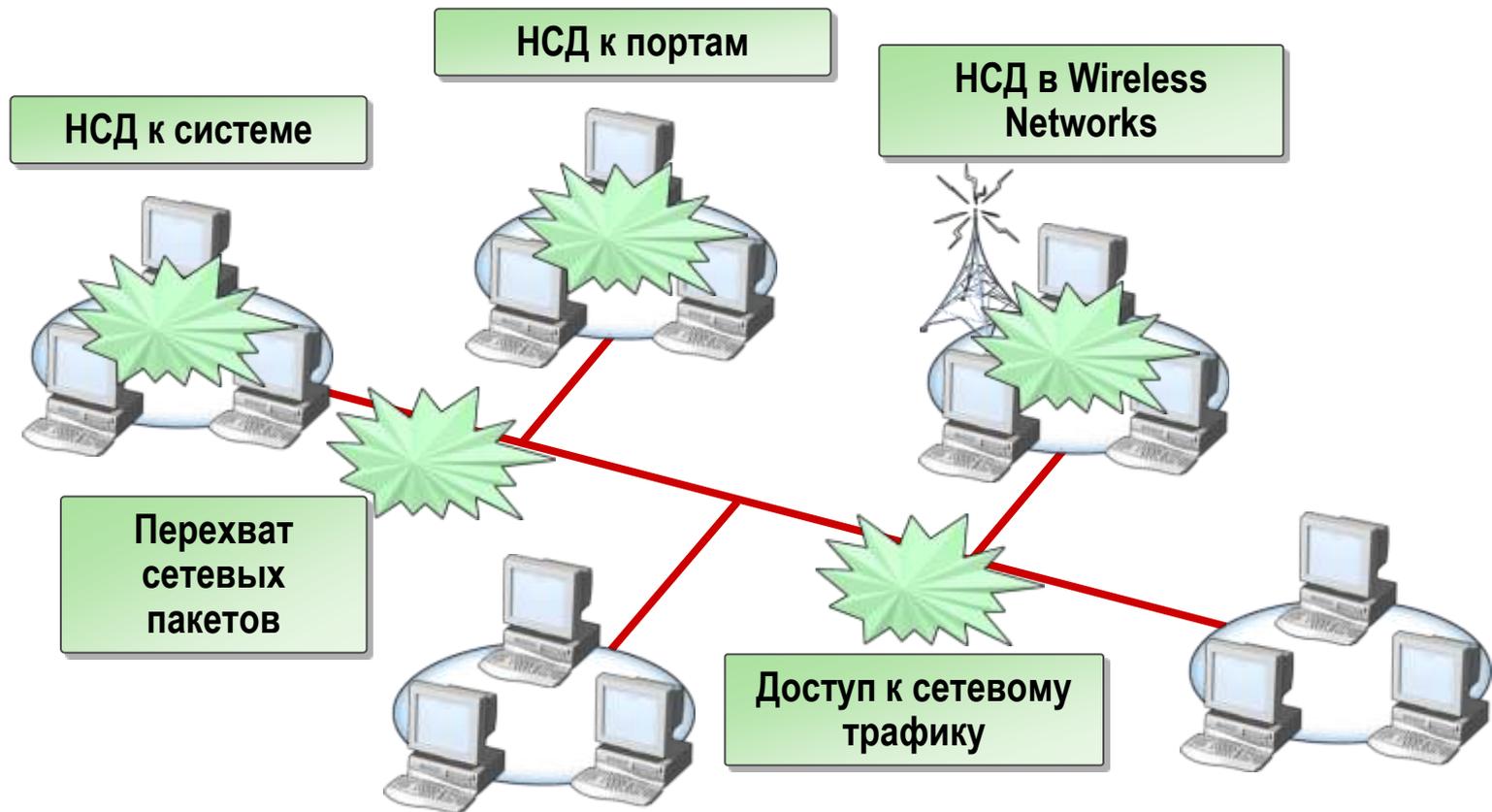
Задачи администрирования - уровень хоста

- На уровне хоста основные задачи администрирования – определение прав пользователей на работу с компьютером (разграничение входа).
- Определение ограничений на выполнение программ и приложений в вычислительной системе.

Описание уровня ЛВС



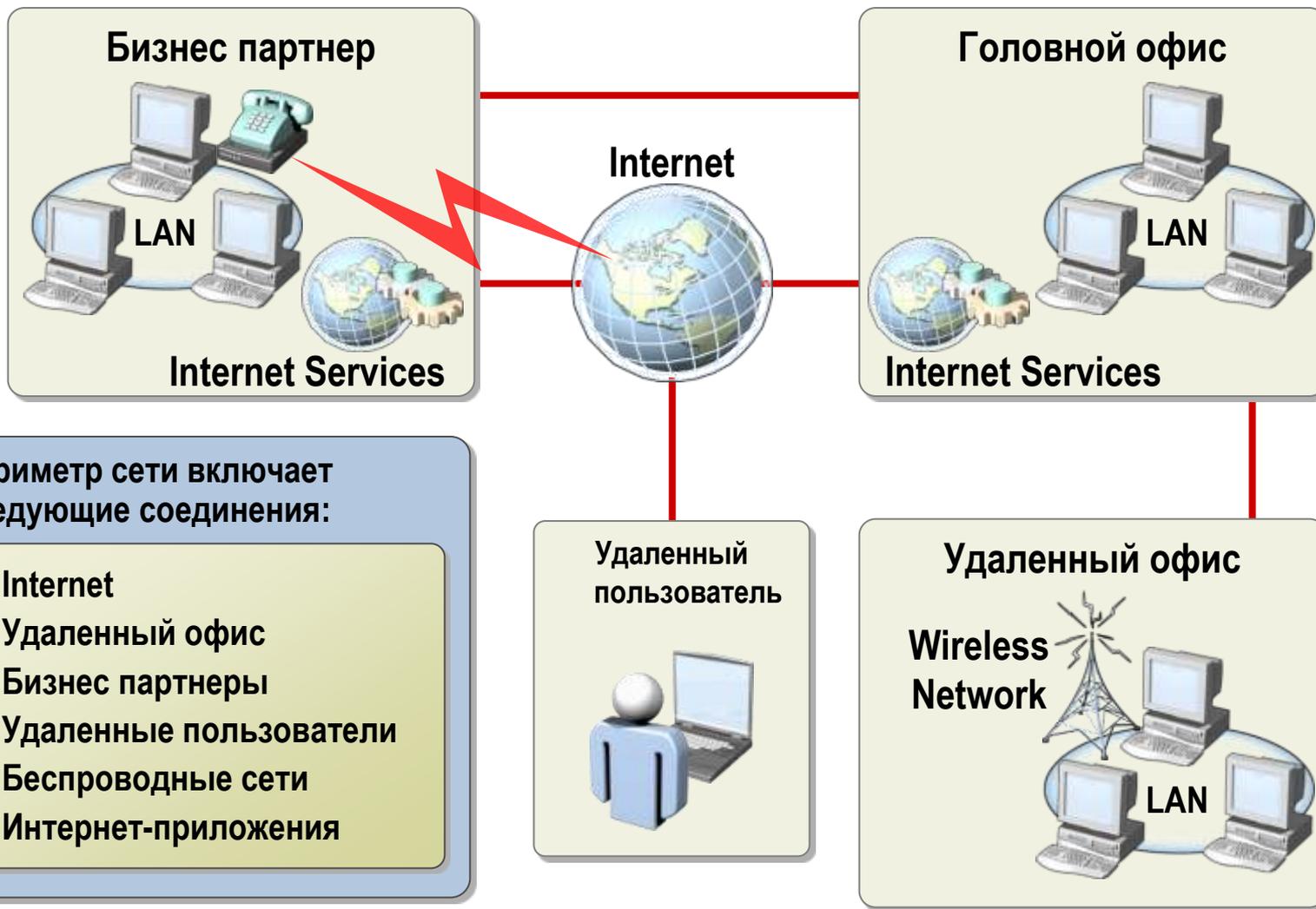
Угрозы безопасности уровня ЛВС



Задачи администрирования - уровень локальной сети

- На уровне локальной сети основные задачи администрирования – определение прав пользователей на работу в сети (многофакторная аутентификация).
- Использование инфраструктуры открытых ключей (PKI) для шифрования трафика.
- Использование служб каталогов для публикации ресурсов и разграничения прав доступа.
- Сегментация сети и администрирование сетевых служб.

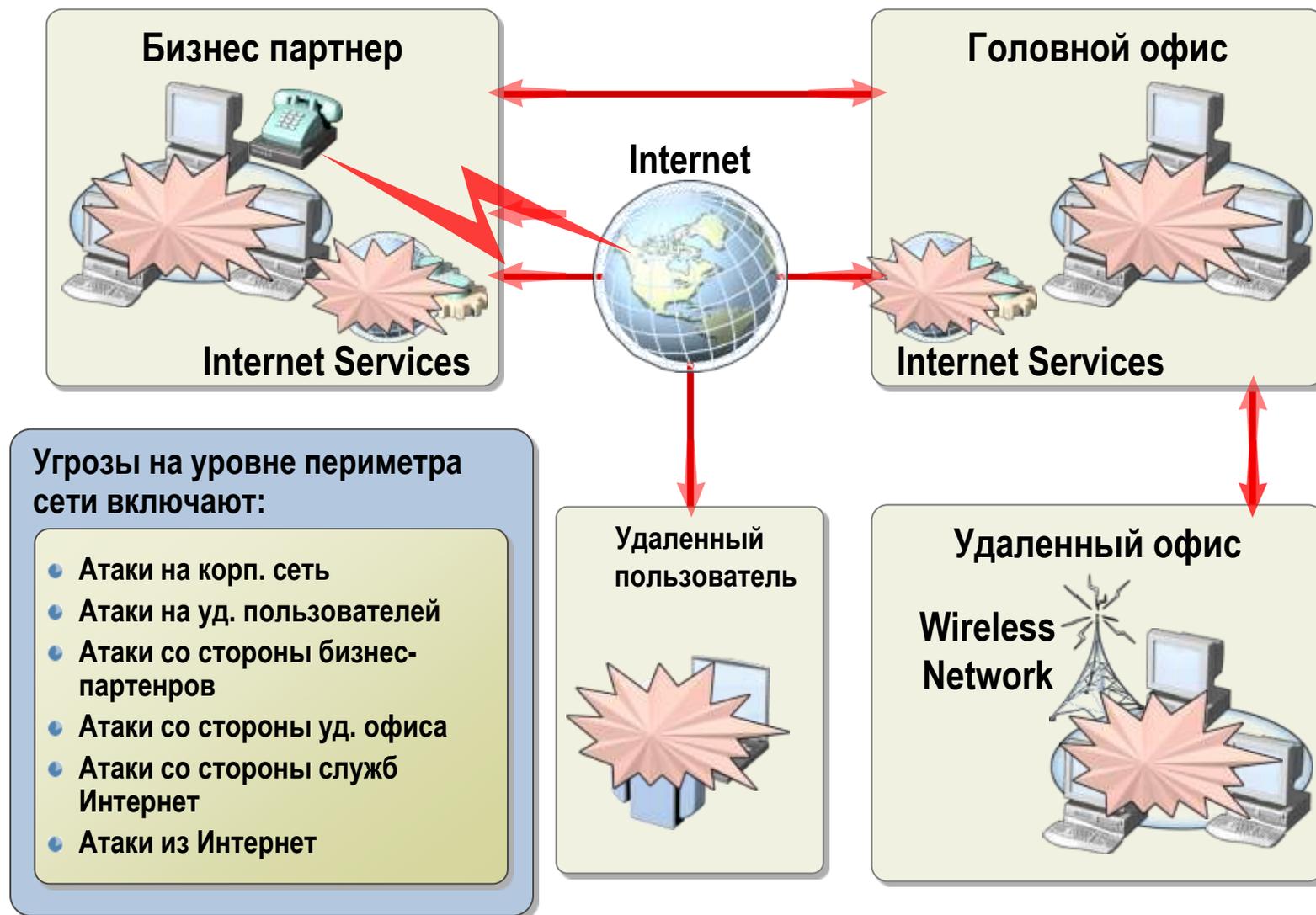
Описание уровня периметра сети



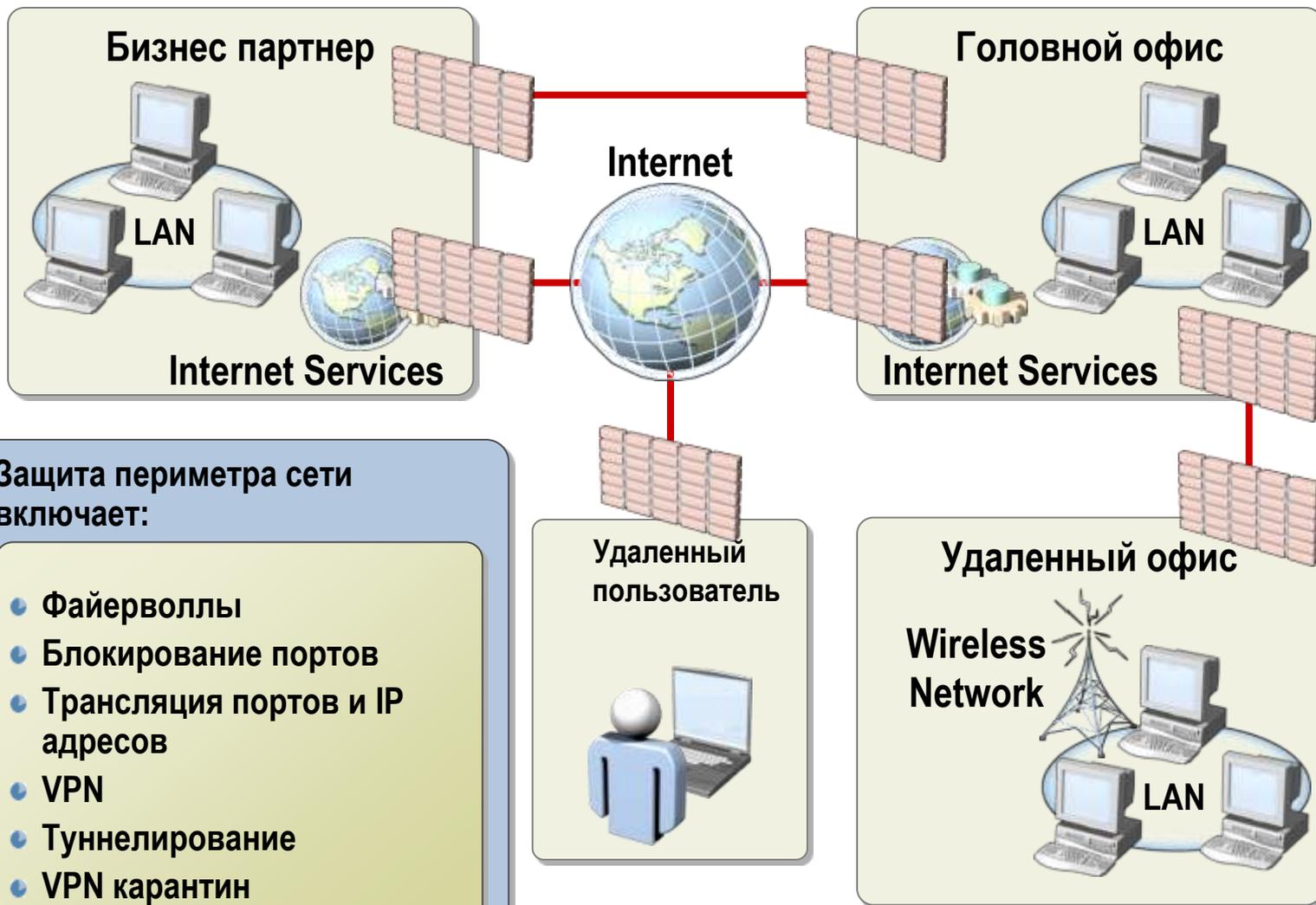
Периметр сети включает следующие соединения:

- Internet
- Удаленный офис
- Бизнес партнеры
- Удаленные пользователи
- Беспроводные сети
- Интернет-приложения

Угрозы на уровне периметра сети



Защита на уровне периметра сети



Защита периметра сети включает:

- Файерволлы
- Блокирование портов
- Трансляция портов и IP адресов
- VPN
- Туннелирование
- VPN карантин

Задачи администрирования - уровень периметра сети

- На уровне периметра сети основные задачи администрирования – определение прав пользователей доступ в сеть Интернет из локальной сети и доступ к локальной сети из Интернет.
- Использование инфраструктуры открытых ключей – РКІ для шифрования трафика.
- Администрирование инфраструктурных сетевых служб для работы в сети Интернет.
- Администрирование веб-сервисов.

Шифрование

- **Шифрование** – использование криптографических сервисов безопасности.
- Процедура шифрования – преобразование открытого текста сообщения в закрытый.
- Для обеспечения конфиденциальности преобразованного сообщения используются специальные параметры преобразования – **ключ шифрования**.

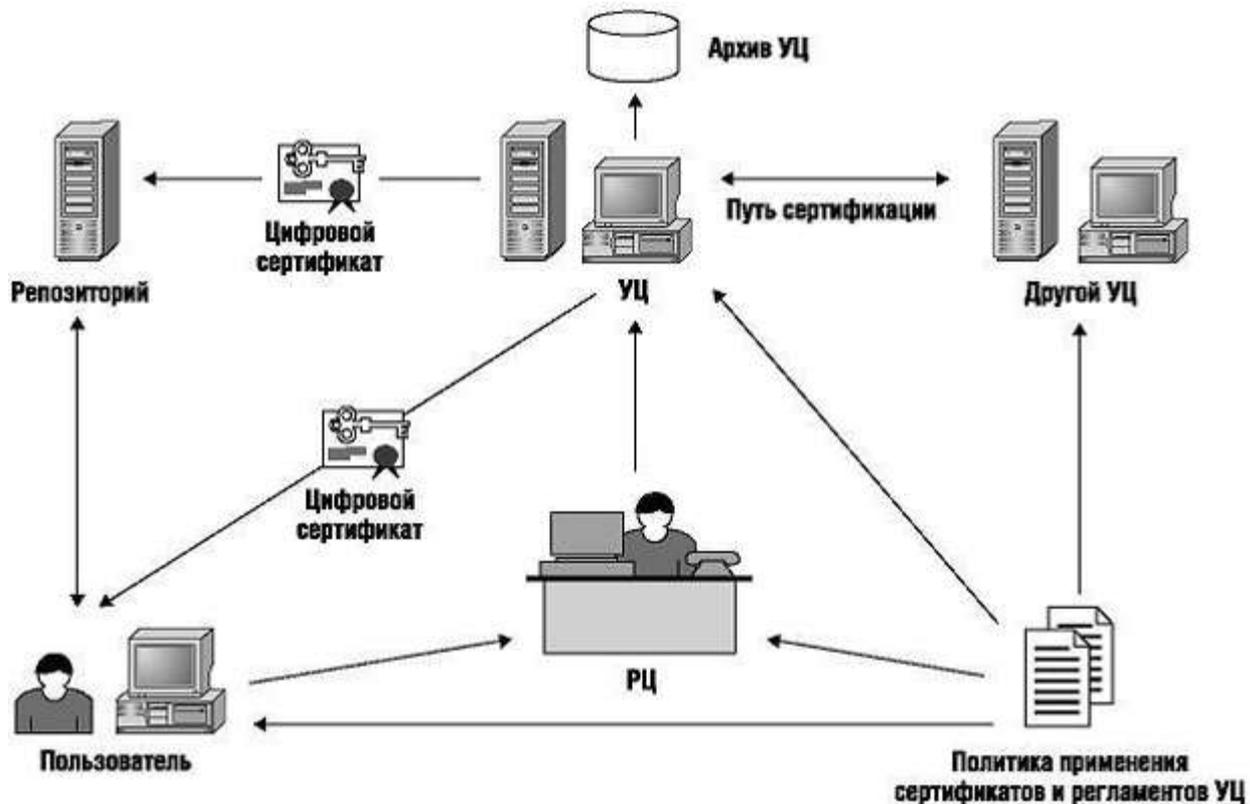
Симметричное шифрование

- В процессе шифрования и дешифрования используется один и тот же параметр – секретный ключ, известный обеим сторонам.
- Примеры симметричного шифрования:
 - ГОСТ 28147-89
 - DES
 - Blow Fish
 - IDEA
- Достоинство симметричного шифрования
 - Скорость выполнения преобразований
- Недостаток симметричного шифрования
 - Известен получателю и отправителю, что создает проблемы при распространении ключей и доказательстве подлинности сообщения

Ассиметричное шифрование

- В криптографических преобразованиях используется два ключа. Один из них несекретный (открытый) ключ используется для шифрования. Второй, секретный ключ для расшифровывания.
- Примеры несимметричного шифрования:
 - RSA
 - Алгоритм Эль-Гамала
- Недостаток асимметричного шифрования
 - низкое быстродействие алгоритмов (из-за длины ключа и сложности преобразований)
- Достоинства:
 - Применение асимметричных алгоритмов для решения задачи проверки подлинности сообщений, целостности и т.п.

Инфраструктура открытых ключей



Элементы инфраструктуры открытых ключей

- Удостоверяющий центр - главный управляющий компонент PKI - выполняет следующие основные функции:
 - формирует собственный секретный ключ; если является головным УЦ, то издает и подписывает свой сертификат, называемый **самоизданным** или **самоподписанным**;
 - выпускает (то есть создает и подписывает) сертификаты открытых ключей подчиненных удостоверяющих центров и конечных субъектов PKI; может выпускать кросс-сертификаты, если связан отношениями доверия с другими PKI;
 - поддерживает реестр сертификатов (базу всех изданных сертификатов) и формирует списки CAC с регулярностью, определенной регламентом УЦ;
 - публикует информацию о статусе сертификатов и списков CAC.

Репозиторий

- Репозиторий - специальный объект инфраструктуры открытых ключей, база данных, в которой хранится реестр сертификатов (термин "реестр сертификатов ключей подписей" введен в практику Законом РФ "Об электронной цифровой подписи").
- Репозиторий упрощает управление системой и доступ к ресурсам, предоставляет информацию о статусе сертификатов, обеспечивает хранение и распространение сертификатов, управляет внесениями изменений в сертификаты.
- К репозиторию предъявляются следующие требования:
 - простота и стандартность доступа;
 - регулярность обновления информации;
 - встроенная защищенность;
 - простота управления;
 - совместимость с другими хранилищами (необязательное требование).

Серверные компоненты PKI



Шифрование данных на носителях информации

- **Шифрованная файловая система** (Encrypting File System, EFS) позволяет безопасно хранить данные.
- EFS делает это возможным благодаря шифрованию данных в выбранных файлах и папках файловой системы NTFS.
 - EFS разработана для безопасного хранения данных на локальных компьютерах. Поэтому она не поддерживает безопасную передачу файлов по сети.

Шифрование данных

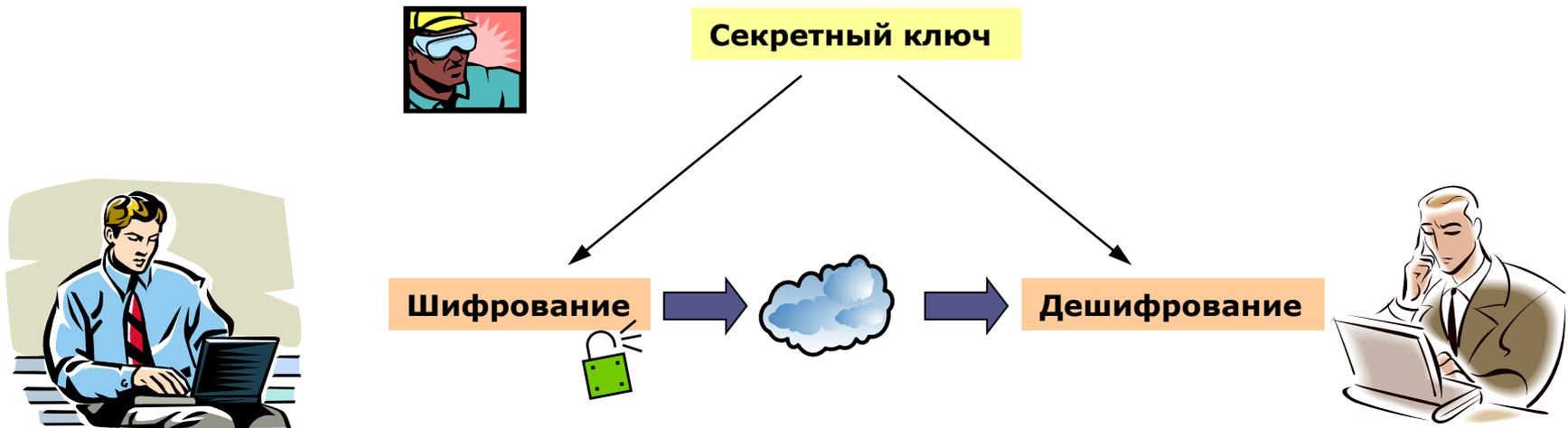
- *Шифрование* файлов происходит следующим образом:
 - Каждый файл имеет уникальный *ключ шифрования файла*, который позже используется для расшифровки данных файла.
 - Ключ шифрования файла сам по себе зашифрован — он защищен **открытым ключом** пользователя, соответствующим сертификату EFS.
 - Ключ шифрования файла также защищен открытым ключом каждого дополнительного пользователя EFS, уполномоченного расшифровывать файлы, и ключом каждого **агента восстановления**.
- Сертификат и закрытый ключ системы EFS могут быть выданы несколькими источниками. Сюда входит автоматическое создание сертификатов и выдача сертификатов центрами сертификации (ЦС) корпорации Майкрософт или сторонними центрами сертификации

Расшифровывание данных

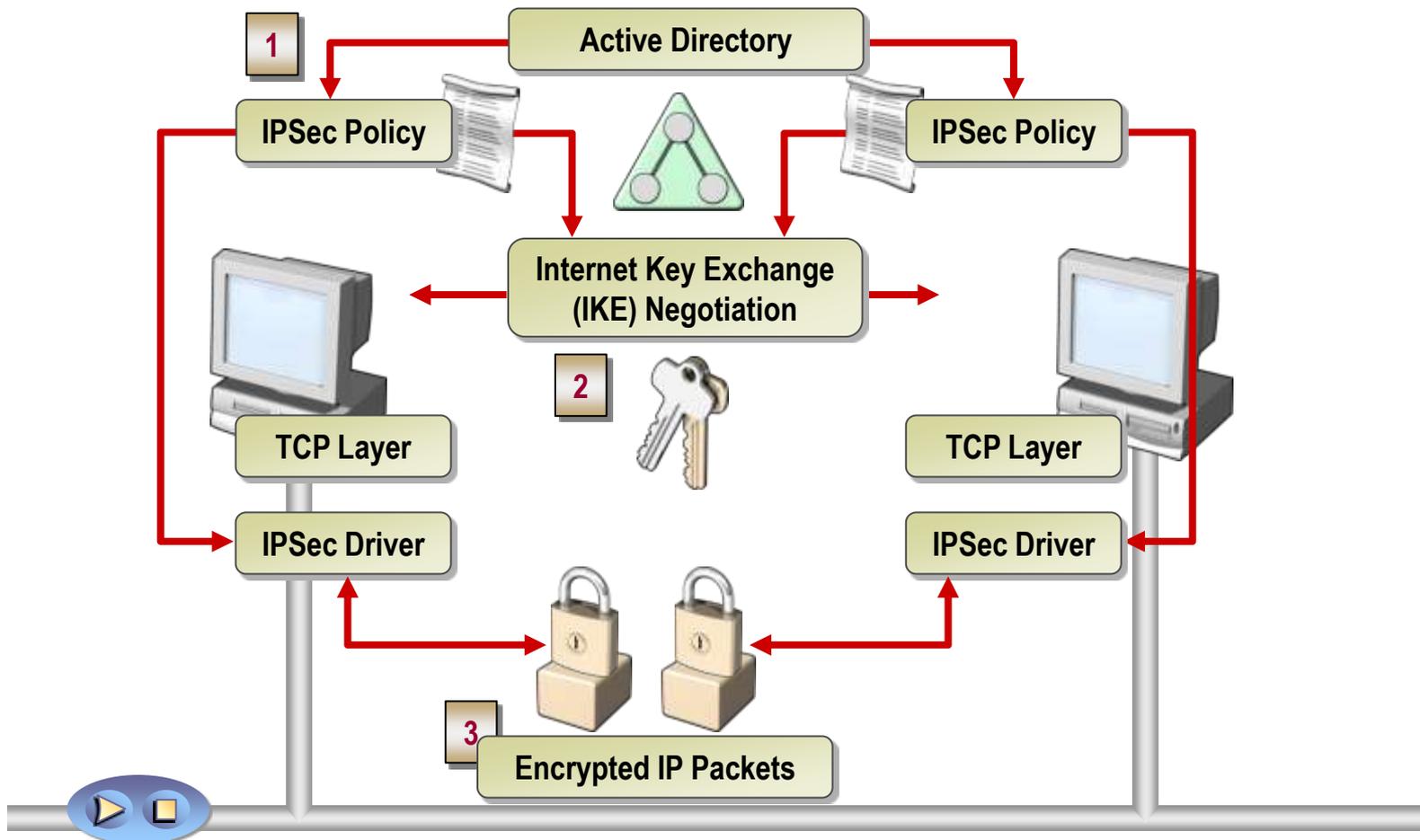
- *Расшифровка* файлов происходит следующим образом:
 - Для расшифровки файла необходимо сначала расшифровать его ключ шифрования. Ключ шифрования файла расшифровывается, если **закрытый ключ** пользователя совпадает с открытым.
 - Не только пользователь может расшифровать ключ шифрования файла. Другие назначенные пользователи или агенты восстановления также могут расшифровать ключ шифрования файла, используя собственный закрытый ключ.
- Закрытые ключи содержатся в защищенном хранилище ключей, а не в диспетчере учетных записей безопасности (Security Account Manager, SAM) или в отдельном каталоге.

Шифрование сетевого трафика (протокол IPSec)

- Для **шифрования** данных в протоколе IPSec может быть применен любой симметричный алгоритм шифрования.
- В **симметричных схемах шифрования** конфиденциальность основана на том, что отправитель и получатель обладают общим, известным только им, параметром функции шифрования.
- Этот параметр называется **секретным ключом**. Секретный ключ используется как для шифрования текста, так и для его дешифрования.



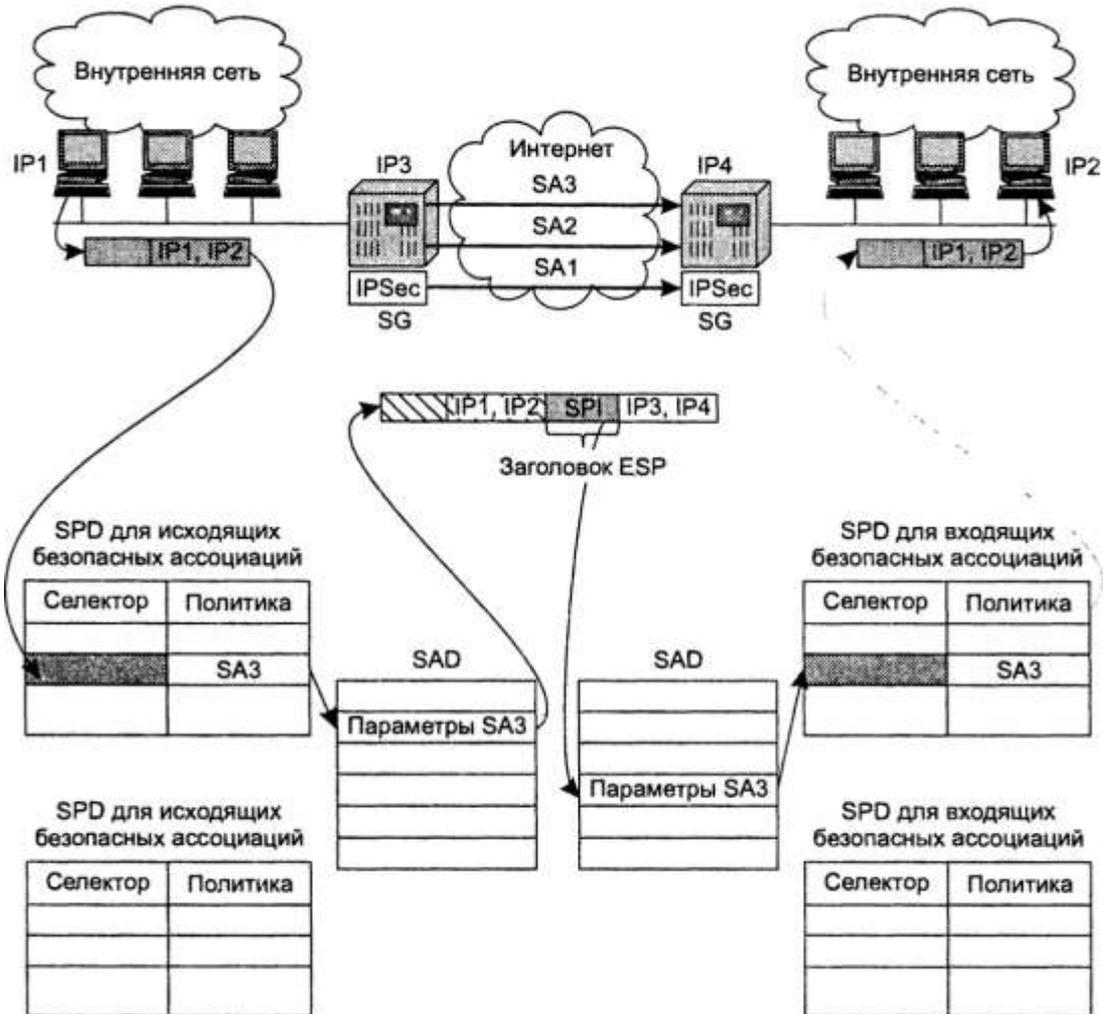
Защита трафика средствами IPSec



Базы данных SAD И SPD

- Протокол IPSec, работающий на хосте или шлюзе, определяет способ защиты, который он должен применить к трафику на основании использования в каждом узле, поддерживающем IPSec, двух типов баз данных:
 - **безопасных ассоциаций** (Security Associations Database, SAD);
 - **политики безопасности** (Security Policy Database, SPD).
- Наборы текущих параметров, определяющих все активные ассоциации, хранятся на обоих конечных узлах защищенного канала в виде баз данных безопасных ассоциаций (SAD). Каждый узел IPSec поддерживает две базы SAD — одну для исходящих ассоциаций, другую для входящих.
- Другой тип базы данных — база данных политики безопасности (SPD) — определяет соответствие между IP-пакетами и установленными для них правилами обработки.

Использование баз данных SPD и SAD



Структура БД SPD

- Записи SPD состоят из полей двух типов — полей селектора пакета и полей политики защиты для пакета с данным значением селектора.
- Селектор в SPD включает следующий набор признаков, на основании которых можно с большой степенью детализации выделить защищаемый поток:
 - IP-адреса источника и приемника могут быть представлены как в виде отдельных адресов (индивидуальных, групповых или широковещательных), так и диапазонами адресов, заданными с помощью верхней и нижней границ либо с помощью маски;
 - порты источника и приемника (то есть TCP- или UDP-портов);
 - тип протокола транспортного уровня (TCP, UDP);
 - имя пользователя в формате DNS или X.500;
 - имя системы (хоста, шлюза безопасности и т. п.) в формате DNS или X.500.

Работа политики безопасности IPSec

- Для каждого нового пакета, поступающего в защищенный канал, IPSec просматривает все записи в базе SPD и сравнивает значение селекторов этих записей с соответствующими полями IP-пакета.
- Если значение полей совпадает с каким-либо селектором, то над пакетом выполняются действия, определенные в поле политики безопасности данной записи.
- Политика предусматривает одну из следующих возможностей:
 - передача пакета без изменения,
 - отбрасывание,
 - обработка средствами IPSec.
- В последнем случае поле политики защиты должно содержать ссылку на запись в базе данных SAD, в которую помещен набор параметров безопасной ассоциации для данного пакета.
- На основании заданных параметров безопасной ассоциации к пакету применяется соответствующий протокол шифрования и секретные ключи.

Создание политики защиты средствами IPSec

- Если к исходящему пакету нужно применить некоторую политику защиты, но указатель записи SPD показывает, что в настоящее время нет активной безопасной ассоциации с требуемой политикой, то IPSec создает новую ассоциацию с помощью протокола IKE, помещая новые записи в базы данных SAD и SPD.
- Базы данных политики безопасности создаются и администрируются либо пользователем (этот вариант больше подходит для хоста), либо системным администратором (вариант для шлюза), либо автоматически (приложением).

Обработка пакетов IPSec

- Как *принимающий* узел IPSec определяет способ обработки прибывшего пакета?
 - При шифровании многие ключевые параметры пакета, отраженные в селекторе, оказываются недоступными – следовательно невозможно определить соответствующую запись в базах данных SAD и SPD и, следовательно, тип процедуры, которую надо применить к поступившему пакету.
 - Для решения этой проблемы в заголовках AH и ESP используется **поле SPI**.
 - В это поле помещается указатель на строку базы данных SAD, в которой записаны параметры соответствующей безопасной ассоциации.
 - Поле SPI заполняется протоколом AH или ESP во время обработки пакета в отправной точке защищенного канала.
 - Когда пакет приходит в конечный узел защищенного канала, из его внешнего заголовка ESP или AH извлекается значение SPI, и дальнейшая обработка пакета выполняется с учетом всех параметров заданной этим указателем ассоциации.

Протоколирование и аудит

- **Протоколирование** – сбор и накопление информации о событиях ИС (внешних, внутренних, клиентских)
- **Аудит** – анализ накопленной информации, проводимый оперативно или периодически.

Протоколирование и аудит

- Позволяет решить следующие задачи:
 - Обеспечение подотчетности пользователей и администраторов ИС
 - Обеспечение реконструкции последовательности событий
 - Обнаружение попыток нарушений ИБ
 - Предоставление информации для выявления и анализа проблем

Протоколирование и аудит

- События, рекомендуемые для протоколирования:
 - Вход/выход в систему;
 - Обращение к удаленной системе или сервису;
 - Выполнение операций с файлами и информационными массивами;
 - Изменение привилегий пользователя или иных атрибутов безопасности.

Протоколирование и аудит

- При протоколировании рекомендуют записывать следующую информацию:
 - Дата и время события
 - Уникальный идентификатор субъекта – инициатора события
 - Результат события
 - Источник запроса
 - Имена объектов
 - Описание изменений, внесенных в базу данных защиты

Активный аудит

- Задачи активного аудита – выявление подозрительной активности и управление средствами автоматического реагирования на нее
- Активность противоречащую политике безопасности разделяют:
 - Атаки, направленные на незаконное получение полномочий
 - Действия, выполняемые в рамках полномочий, но нарушающие политику безопасности (злоупотребление полномочиями)

Активный аудит

- Методы активного аудита:
 - Сигнатурный – на основе определения сигнатуры атаки (совокупность условий при которых считается, что атака имеет место) – велики ошибки первого рода (неумение обнаруживать неизвестные атаки);
 - Статистический – на основе анализа выполняемых действий субъектов – велики ошибки второго рода (ложное срабатывание).

Рекомендации по безопасности

- ✓ Использование комплексной многоуровневой защиты
- ✓ Использование принципа минимизации привилегий пользователей
- ✓ Использование средств мониторинга и аудита
- ✓ Проведение обучение пользователей процедурам ИБ
- ✓ Обобщение опыта противодействия угрозам ИБ
- ✓ Разработка и проверка плана противодействия угрозам ИБ
- ✓ Использование защищенных сервисов и систем