Обеспечение информационной безопасности, определения

- ***Информация*** в теории компьютерной безопасности определяется как сведения в некоторой предметной области, необходимые для оптимизации принимаемых решений. *(в отличии от вероятностного подхода к определению информации Шеннона, здесь учитывается полезность сведений, и .т.п. свойства)*

- ***Автоматизированная система*** обработки информации (АС) – организационно-техническая система, совокупность взаимосвязанных компонентов: технических средств, программного обеспечения, информации и персонала.

- ***Угроза*** – это потенциальная возможность ущерба ресурсу, как со стороны злоумышленника, так и со стороны различных катастроф: пожаров, наводнений, землетрясений.

- ***Информационная безопасность АС*** – совокупность условий работоспособного состояния АС, при котором АС способна противостоять внутренним и внешним угрозам, а ее функционирование не создает угроз для АС и внешней среды.

Свойства информации и АС

- Из *конфиденциальности* (англ. confidential: доверительный, «по секрету») информации следует необходимость введения ограничений на доступ
- *Целостность* – существование информации в неискаженном виде
- *Доступность* – своевременный и беспрепятственный доступ
- Безопасность обеспечена, если поддерживаются необходимые уровни К, Ц и Д.

Цель создания системы защиты информации

- Организации создают системы защиты информации, чтобы защитить свои ресурсы от угроз.
- Ресурсы включают: производственные секреты, служебную переписку, базы данных клиентов, информацию о транзакциях и т.д.
- Угроза – это ***потенциальная возможность ущерба*** ресурсу, как со стороны злоумышленника, так и со стороны различных катастроф: пожаров, наводнений, землетрясений.

Основные виды угроз для АС

1. Нарушение конфиденциальности
2. Нарушение целостности
3. Угроза отказа служб

Прим. В англоязычных источниках – т.н. триада CIA (Confidentiality, Integrity, Availability)

4. Угроза раскрытия параметров АС

Методы реализации угроз и принципы обеспечения информационной безопасности

- Угрозы и методы обеспечения защиты реализуются на разных уровнях:
  - Уровень носителей информации
  - Уровень средств взаимодействия с носителем
  - Уровень представления информации
  - Уровень содержания информации

Уровни квалификации атакующих и характерные причины атак

- Низкий уровень
  - Привлечение внимания к себе
  - Опасны тем, что не представляют всех последствий
- Средний уровень
  - Желание заявить о себе в своем сообществе
  - Мщение уволенных/отстраненных сотрудников
  - Часто атакуют известные ресурсы для получения наибольшей огласки, обсуждают свои атаки в форумах
- Высокий уровень
  - Шпионаж, терроризм, получение вознаграждения
  - Методы часто включают введение в заблуждение пользователей и администраторов (social engineering), составление тактических планов атаки
  - Открыто не обсуждают свои атаки

Методология построения систем защиты информации в АС

- Идентификация угроз
- Анализ рисков (создание плана УР)
- Разработка подсистем безопасности для различных угроз
- Разработка ответных мер для возможных нарушений ИБ

Разработка систем безопасности

- Разработка систем безопасности использует концепцию **управления рисками**, чтобы определить соответствующее риску противодействие.
- Данные, собранные в ходе определения адекватных противодействий, с точки зрения управления рисками, также полезны для аргументации важности информационной защиты и затрат на обеспечение безопасности.

Концепции систем безопасности

- «Глубокая» (многоуровневая) защита – определяет использование совместных технологических и организационных мер на нескольких уровнях противодействия угрозам
- «Минимальных привилегий»
- «Минимальной поверхности атаки»

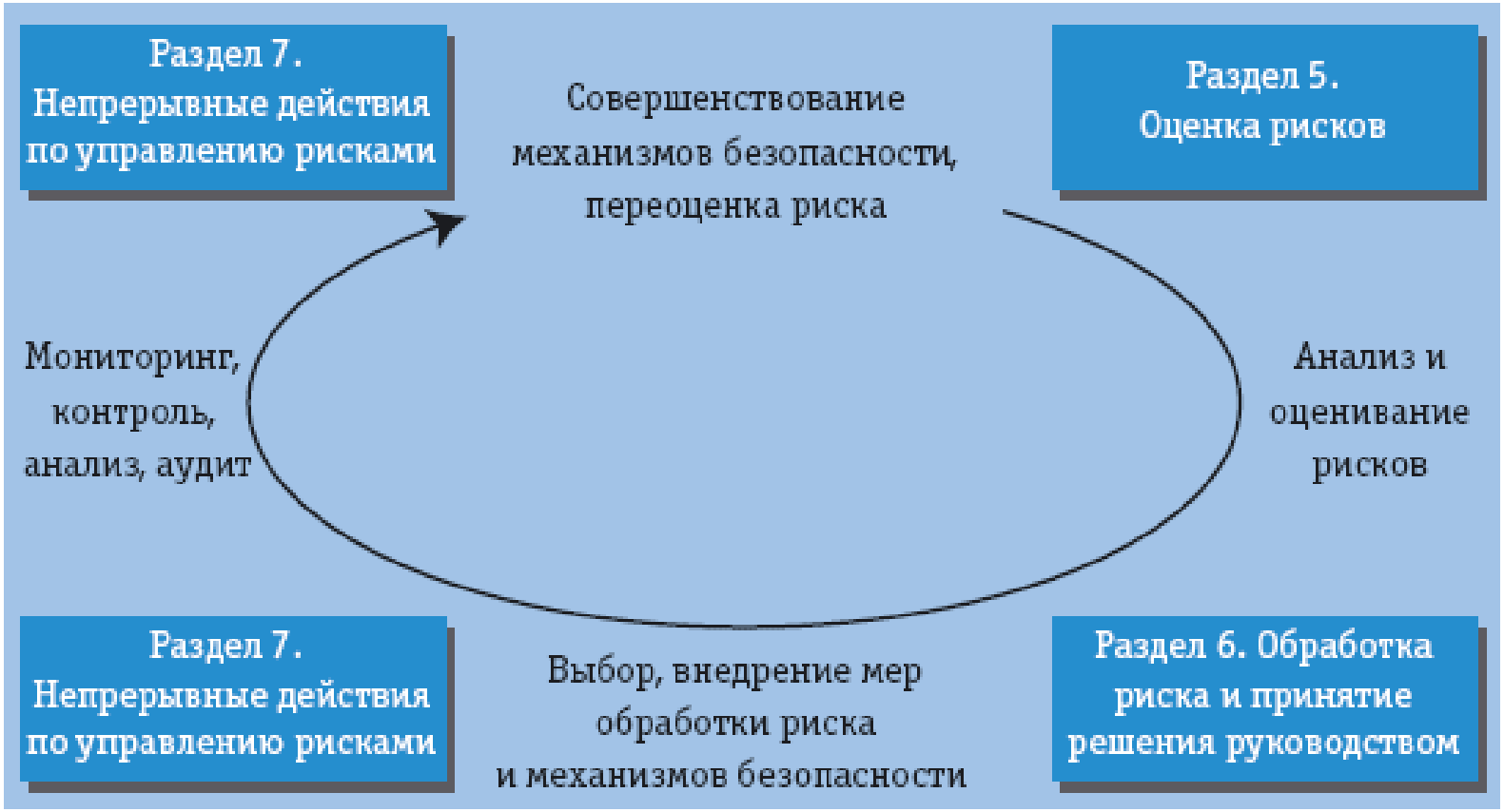
Фазы решения проблем ИБ системы

- Планирование:
  - команда, угрозы (STRIDE sections/life-cycle), план УР
- Создание:
  - политики и процедуры (создание и внедрение), тренинг администраторов и пользователей, внедрение мер противодействия угрозам
- Управление:
  - мониторинг и управление безопасностью (обнаружение вторжений и реагирование), каждодневное управление, оптимизация политик и процедур.

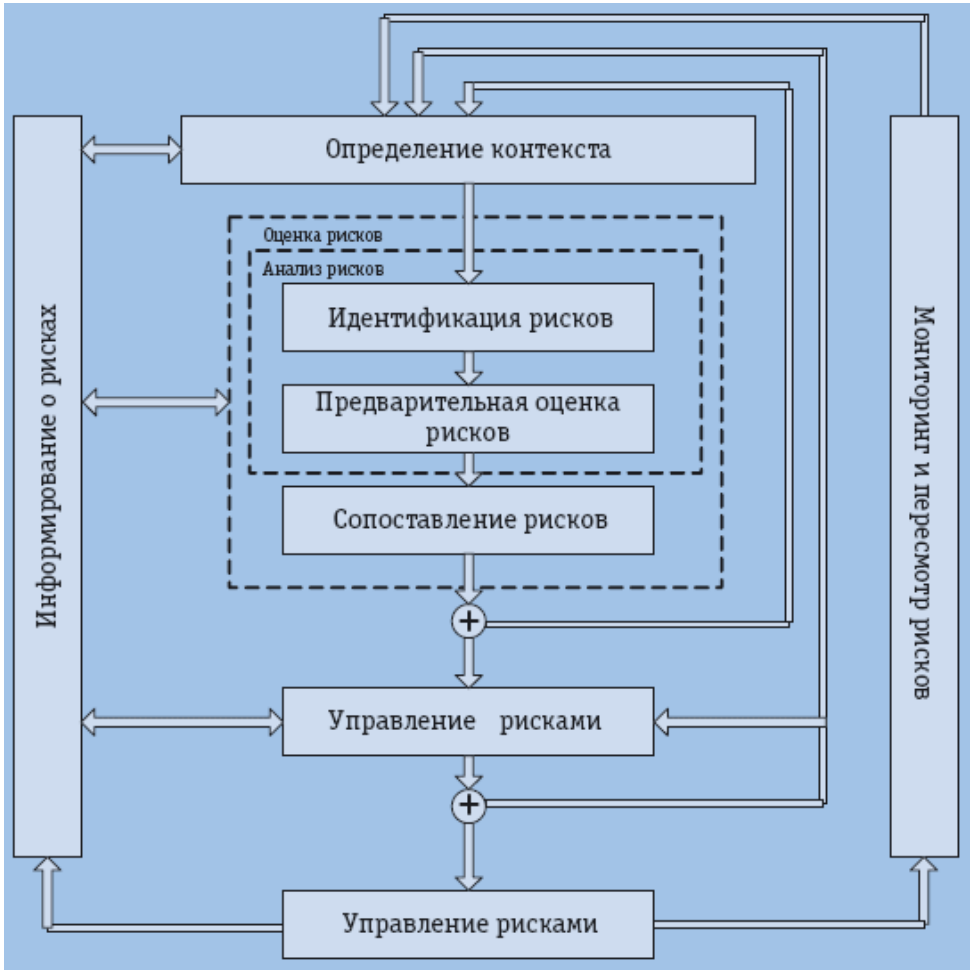
План управления рисками, стадии

- Идентификация
  - Для каждой угрозы – RS (возможно несколько для каждого ресурса).
- Анализ
  - RS: условия возникновения, последствия, оценка урона: количественно (100-бальная шкала PxI, годовые потери, и т.п.), качественно.
- Планирование УР
  - 4 стратегии: принять, уменьшить, передать, избежать.
  - Должен быть назначен ответственный за каждый риск.
- Разработка методов отслеживания изменений рисков
  - Измерение частоты появления, успеха противодействия.
- Меры по управлению
  - Когда и как изменять план УР, актуализировать его.

Фазы управления рисками стандарта ISO 27005



Модель управления рисками ISO 27005



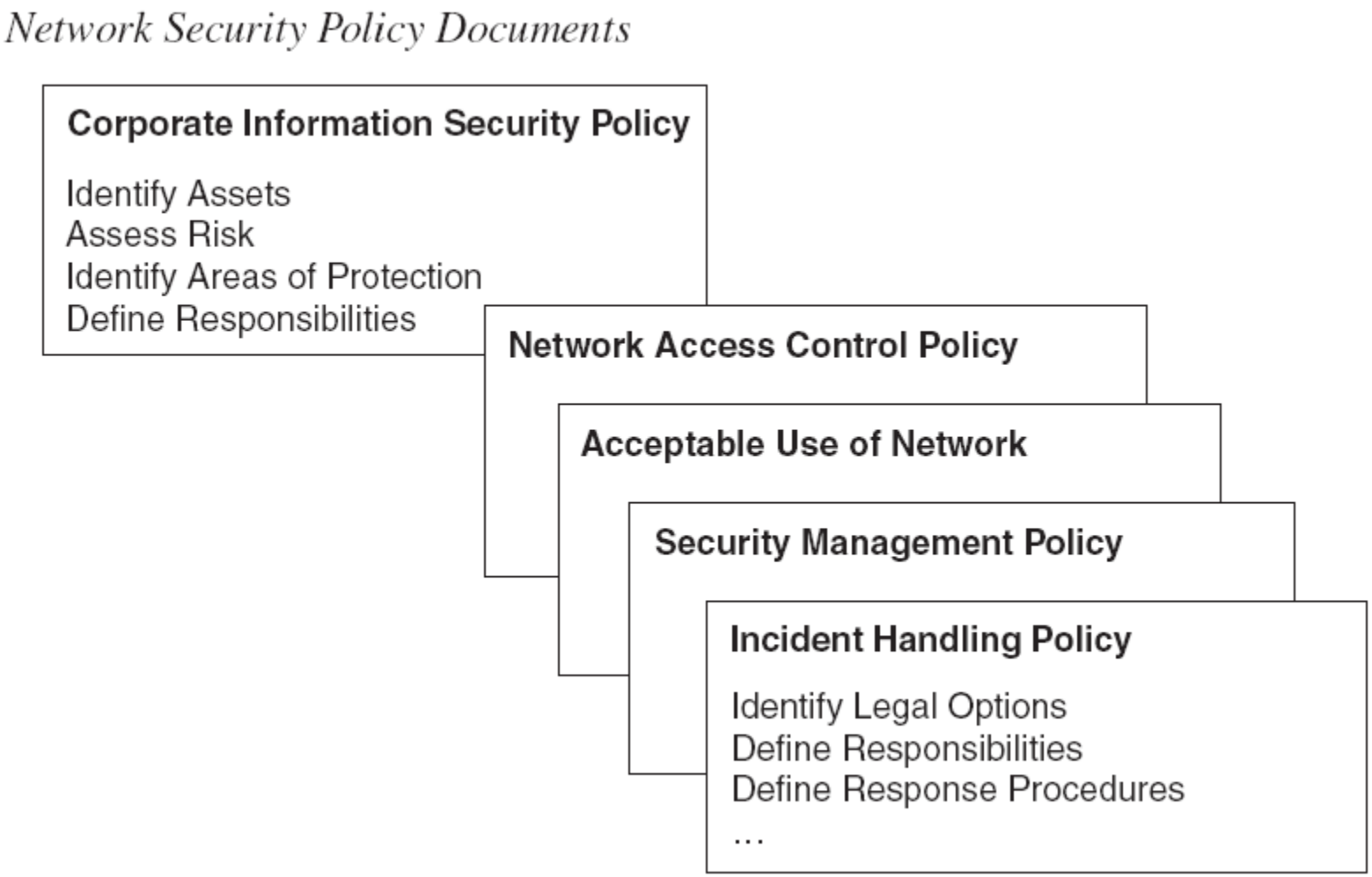
Политики безопасности

- Политика безопасности – документ (заверенный руководством организации) в котором сформулированы **основные принципы** обеспечения ИБ организации
- Типы политик безопасности (по основному средству обеспечения):
  - Административная (например, «соглашение о неразглашении»)
  - Техническая (правила сетевых экранов, шаблоны безопасности)
  - Физическая (камеры видеонаблюдения, замки)

- Процедуры безопасности определяют как именно выполнять те или иные действия, касающиеся политики безопасности.
- В организации должны быть не только разработаны политики безопасности, но и также разработаны и опубликованы простые и ясные процедуры соответствующие политике.

- В узком смысле, термин «политика безопасности» часто используется по отношению к системам управления доступом:
- Политика безопасности включает:
  - множество возможных операций над объектами
  - для каждой пары субъект-объект множество разрешенных операций, являющееся подмножеством всего множества возможных операций
- Типы политик безопасности (в части управления доступом):
    - Дискреционная (дискретная, Discretionary Access Control -DAC)
      - все объекты и субъекты идентифицированы
      - права доступа субъекта к объекту определяются внешним правилом
    - Мандатная (полномочная, Mandatory Access Control MAC)
      - все объекты и субъекты идентифицированы
      - задан упорядоченный набор меток секретности
      - каждому объекту присвоена метка секретности – уровень секретности
      - каждому субъекту присвоена метка секретности – уровень доступа

Сетевая политика, документы



Пример политики безопасности

Политика информационной безопасности

Информация является ценным ресурсом для деятельности Компании и обеспечение информационной безопасности является обязанностью каждого сотрудника.
Настоящая политика определяет основные принципы защиты информационных ресурсов Компании от угроз нарушения конфиденциальности, целостности и доступности.

Доступ к информационным ресурсам предоставляется только в объеме, необходимом для выполнения сотрудниками своих должностных обязанностей.
При построении эффективной системы управления информационной безопасностью Компания руководствуется международными стандартами ISO 17799 и ISO 27001.
Для обеспечения эффективной защиты информации ежегодно проводится комплексный аудит информационной безопасности, включающий в себя аудит системы управления информационной безопасностью и тестирование на возможность несанкционированного проникновения.
Политики информационной безопасности утверждаются президентом Компании.
Все руководители отвечают за выполнение политик информационной безопасности в подчиненных им подразделениях.
Все сотрудники Компании, текущие и бывшие, выполняют требования политик информационной безопасности.
Департамент информационной безопасности осуществляет разработку и внедрение технических и организационных мер для минимизации рисков информационной безопасности.
Департамент внутреннего аудита проводит регулярный аудит эффективности исполнения политик, стандартов и процедур информационной безопасности.
Для обеспечения непрерывности бизнеса Компании должен быть разработан и поддерживаться в актуальном состоянии план непрерывности бизнеса.
Сотрудники Компании проходят ежегодное обучение в области обеспечения информационной безопасности.

Руководящие документы ГТК,1992

- Концепция защиты средств вычислительной техники от НСДкИ.
- Защита от несанкционированного доступа к информации (НСДкИ). Термины и определения.
- Средства вычислительной техники. Защита от НСДкИ. Показатели защищенности от НСДкИ.
- Автоматизированные системы (АС). Защита от НСДкИ. Классификация АС и требования по защите информации.
- Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и средствах вычислительной техники.

Развитие нормативной базы, 1997-1999 гг.

- СВТ. Межсетевые экраны. Защита от НСД. Показатели защищенности от НСД к информации. 1997

Новые нормативные документы по ГОСТ Р ИСО/МЭК 15408-2002 (т.н. «Общие критерии»)

для продуктов и систем информационных технологий, предназначенных для обработки информации, отнесенной к информации ограниченного доступа

- Безопасность информационных технологий. Критерии оценки безопасности информационных технологий
- Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности
- Безопасность информационных технологий. Руководство по регистрации профилей защиты
- Безопасность информационных технологий. Руководство по формированию семейств профилей защиты
- Руководство по разработке профилей защиты и заданий по безопасности

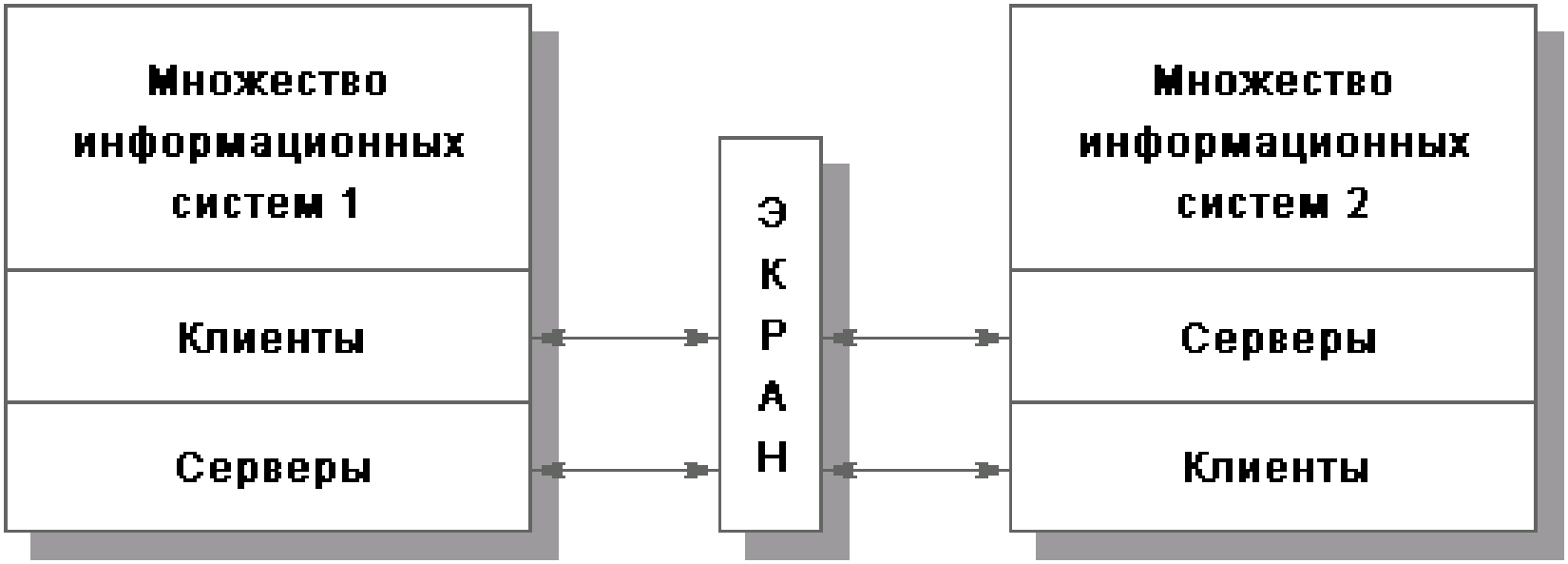
Структура Системы сертификации средств защиты информации по требованиям безопасности информации

- **Гостехкомиссия России** (федеральный орган исполнительной власти, уполномоченный проводить работу по обязательной сертификации). С 08.2004 ФСТЕК http://www.fstec.ru/ ;
- **органы по сертификации средств защиты информации** - органы, проводящие сертификацию определенной продукции;
- **испытательные лаборатории** - лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;
- **заявители** - изготовители, продавцы или потребители продукции

Перечень объектов информатизации, подлежащих аттестации в Системе сертификации средств защиты информации по требованиям безопасности информации

- Автоматизированные системы различного уровня и назначения.
- Системы связи, приема, обработки и передачи данных.
- Системы отображения и размножения.
- Помещения, предназначенные для ведения конфиденциальных переговоров.

МЭ


Множество информационных систем 1
Клиенты
Серверы
Э К Р А Н
Множество информационных систем 2
Серверы
Клиенты

МЭ – набор фильтров

Классы защищенности МЭ (ГТК)

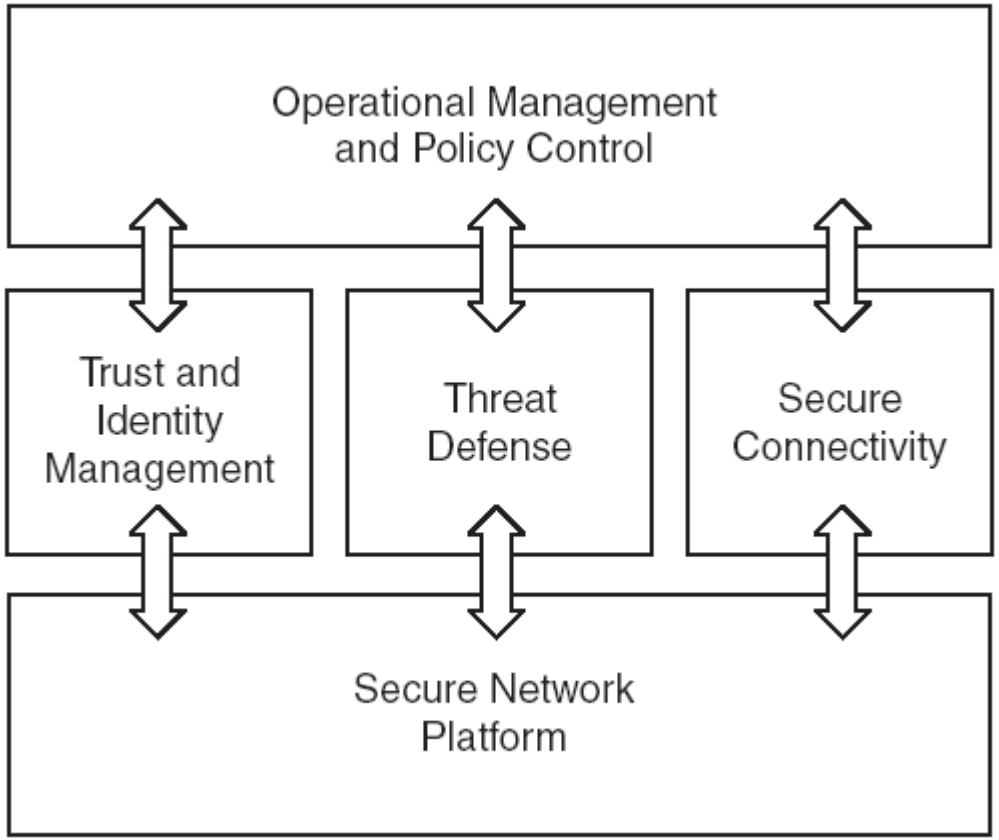
Выделяется пять показателей защищенности:

1. Управление доступом
2. Идентификация и аутентификация
3. Регистрация событий и оповещение
4. Контроль целостности
5. Восстановление работоспособности

Определяется следующие пять классов защищенности МЭ:

- Простейшие фильтрующие маршрутизаторы - 5 класс
- Пакетные фильтры сетевого уровня - 4 класс
- Простейшие МЭ прикладного уровня - 3 класс
- МЭ базового уровня - 2 класс
- Продвинутые МЭ - 1 класс

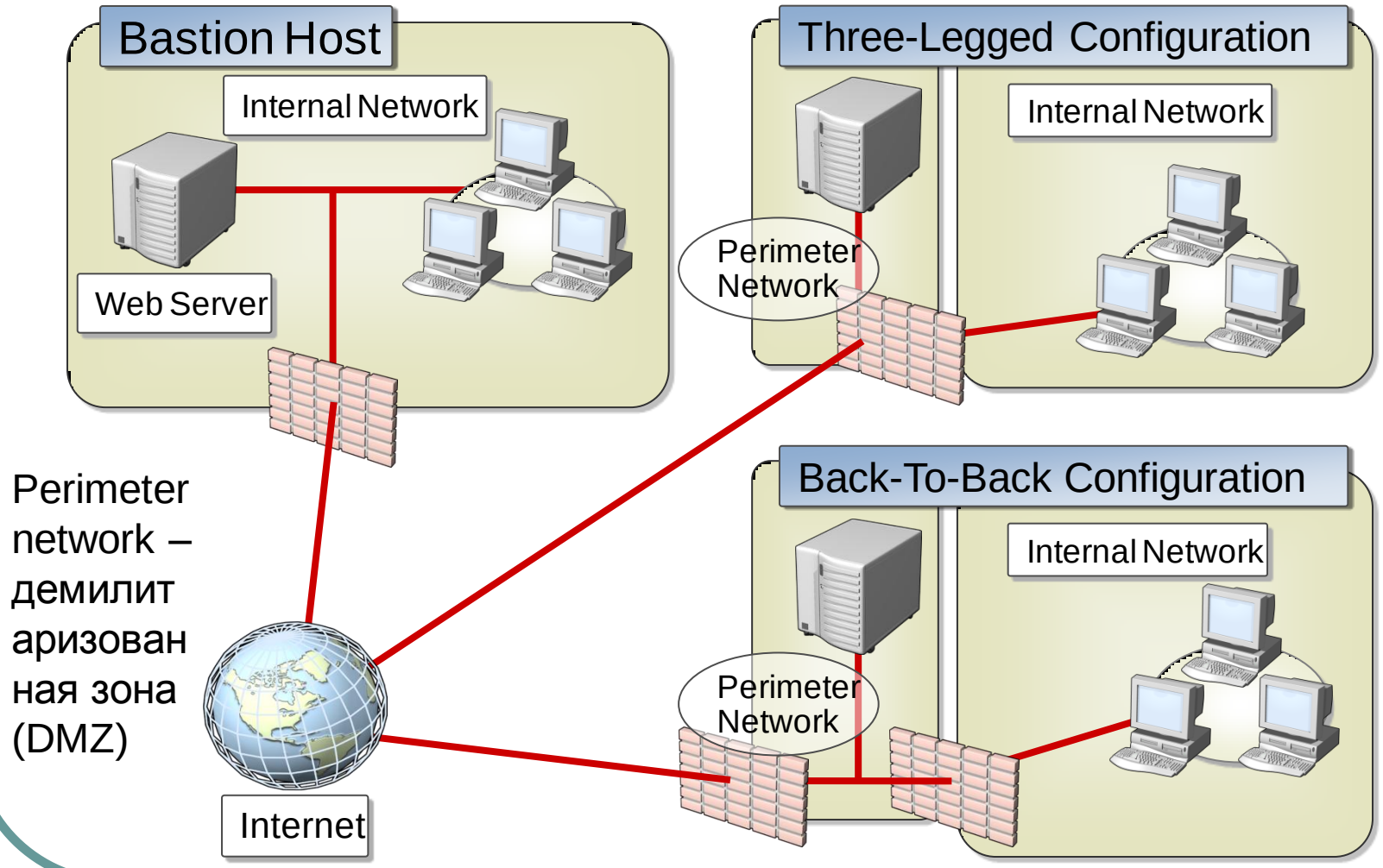
Cisco Self-Defending Network



Firewall, IPS, IDS

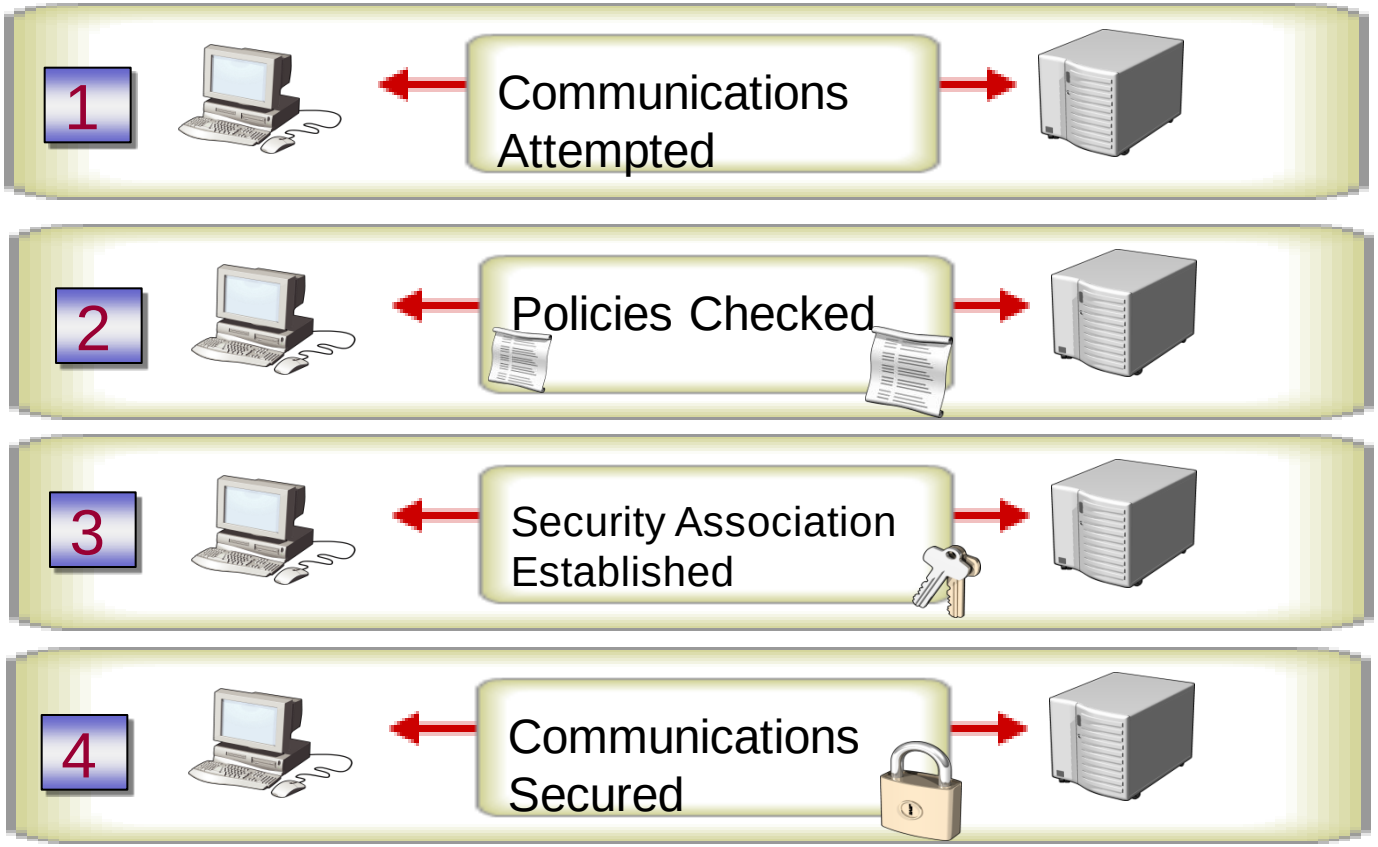
- Firewall/Brandmauer/межсетевой экран – общий термин, определяющий аппаратно-программную систему, обеспечивающую контроль над передачей данных между сетями для решения задач ИБ. В узком смысле (частный случай FW – пакетный фильтр).
  - Statefull – отслеживающий устойчивые связи (TCP-соединения, устойчивые UDP-потоки)
  - Stateless – без отслеживания связей
  - Personal – ориентированный на защиту ПК (host-base – аналогичный, но может защищать сервер)
  - Уровня
    - Сетевого - пакетная фильтрация
    - Транспортного - пакетная фильтрация
    - Приложений - поиск сигнатур, статобработка, поиск аномалий
- IDS (Intrusion Detection System) - СОВ
- IPS (Intrusion Prevention System) - СПВ

Конфигурации firewall



Perimeter network – демилитаризованная зона (DMZ)

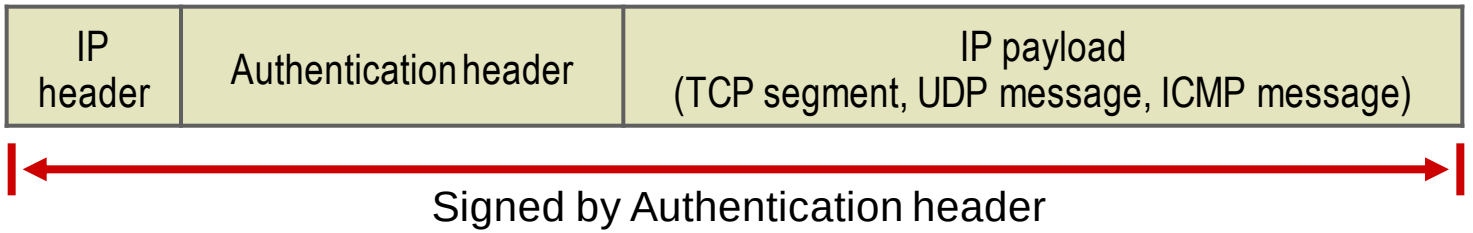
IPsec



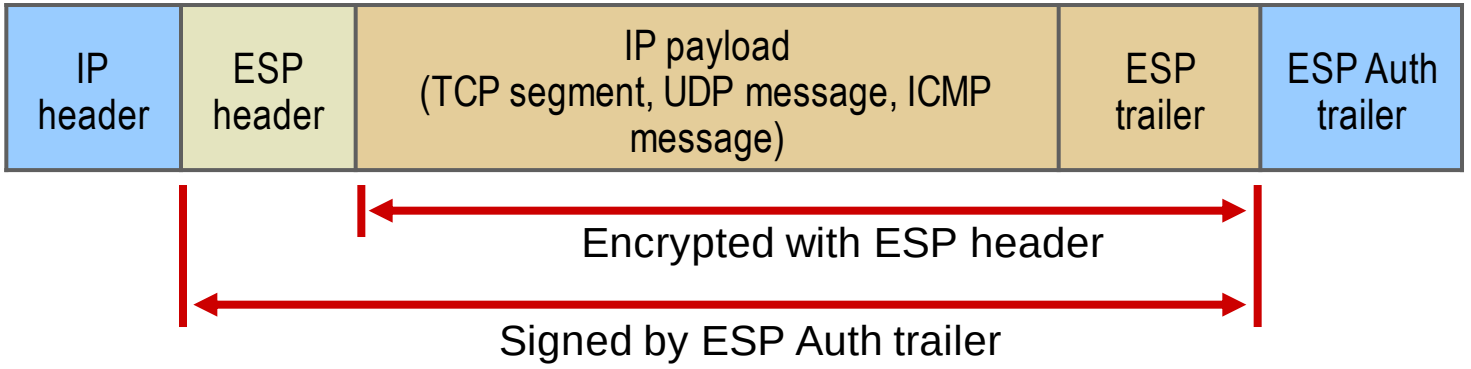
IPsec также используется в составе L2TP-VPN

IKE, AH, ESP

AH provides authentication, integrity, and anti-replay protection

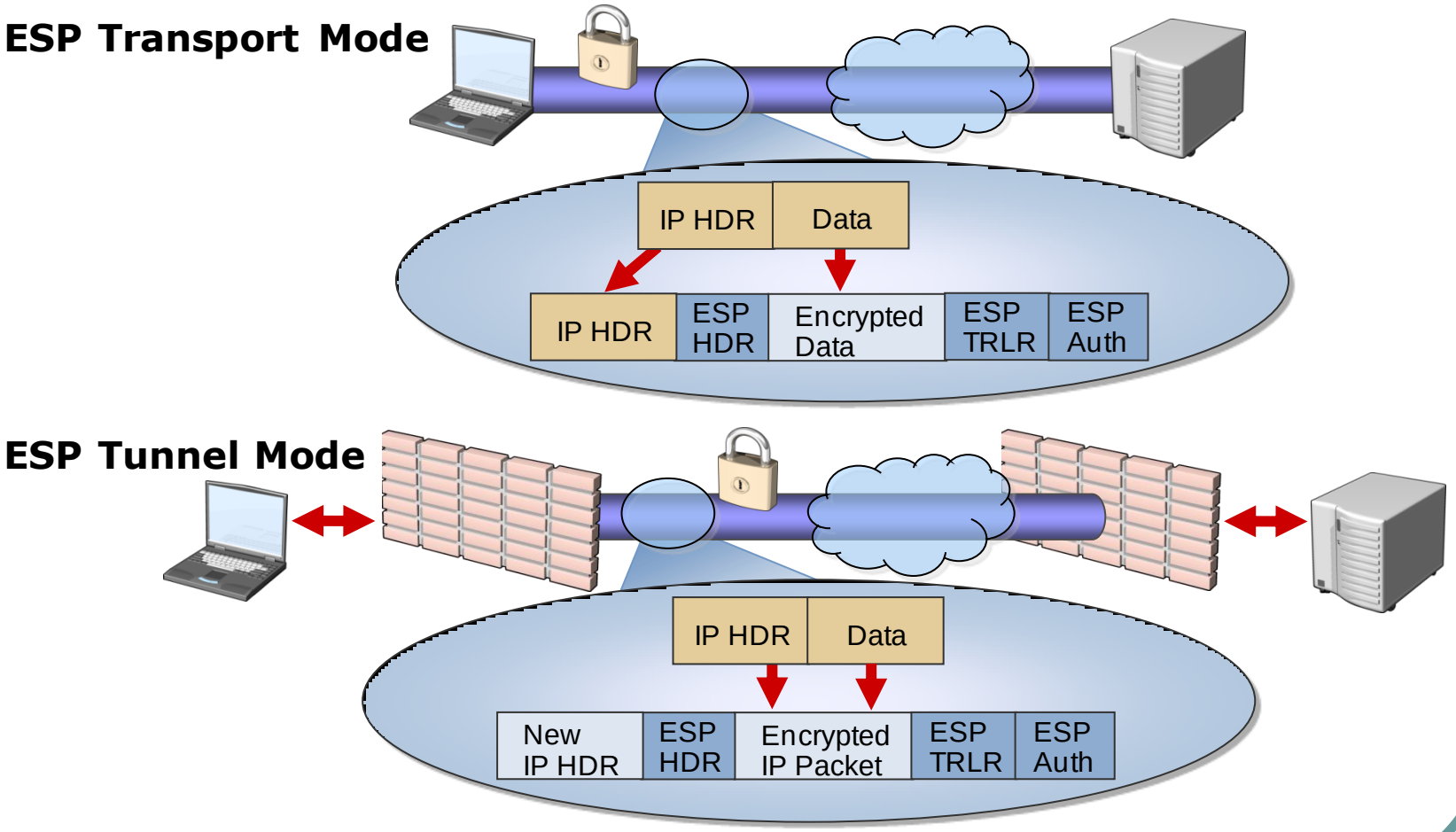


ESP provides confidentiality, authentication, integrity, and anti-replay protection

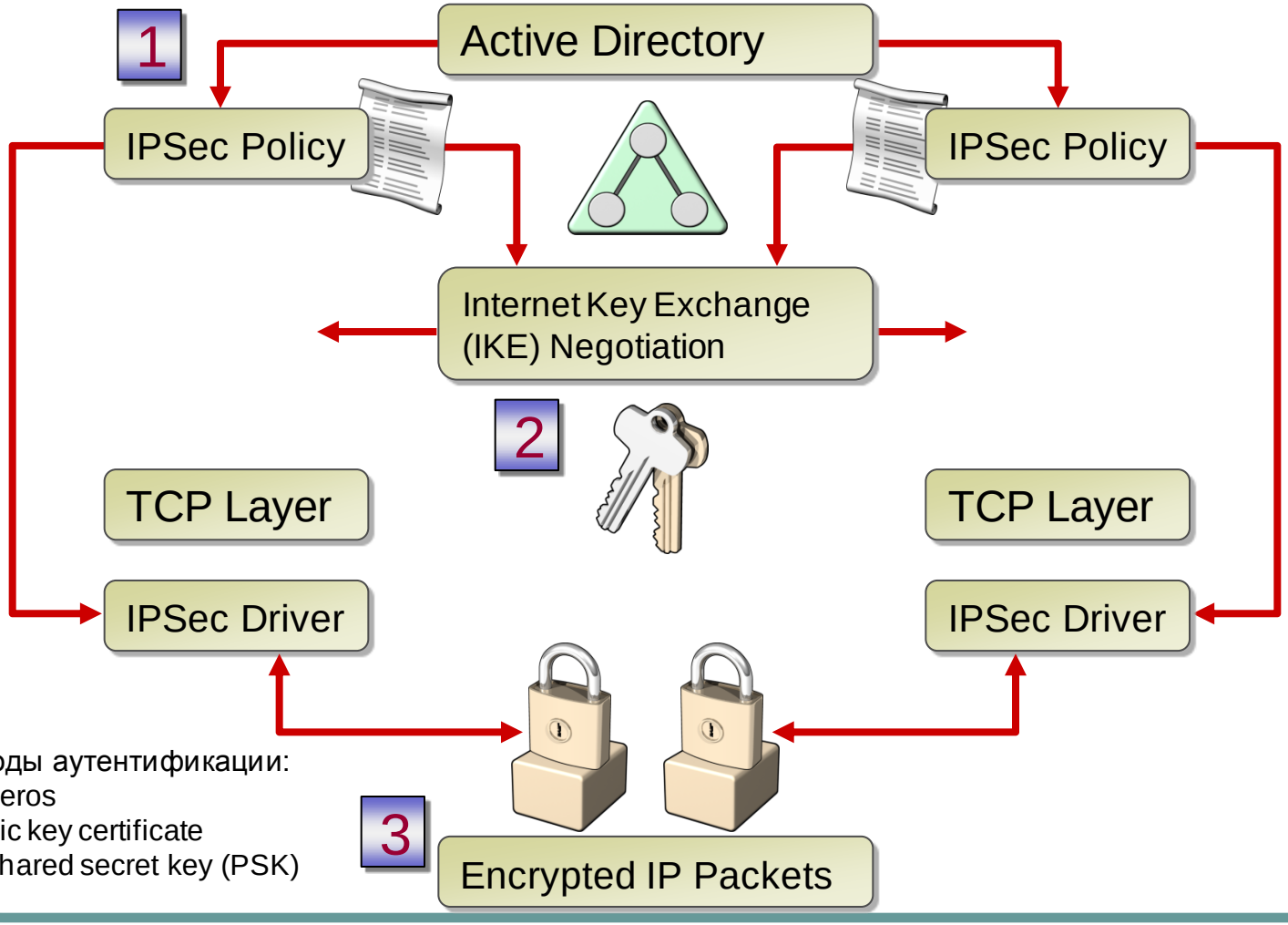


Номера протоколов: 50 - ESP, 51 - AH

IPsec режимы



IPsec реализация



Методы аутентификации:
Kerberos
Public key certificate
Preshared secret key (PSK)