Безопасность информационных систем

Обеспечение безопасности компьютерных сетей

LOGO

Протокол TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) - это промышленный стандарт стека протоколов, разработанный для глобальных сетей.

Лидирующая роль стека TCP/IP объясняется следующими его свойствами:

- Это наиболее завершенный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю.
- Почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP.
- Это метод получения доступа к сети Internet.
- Этот стек служит основой для создания intranet- корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW, разработанную в Internet.
- Все современные операционные системы поддерживают стек TCP/IP.
- Это гибкая технология для соединения разнородных систем как на уровне транспортных подсистем, так и на уровне прикладных сервисов.
- Это устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер.

Протокол TCP/IP

Характеристика стека TCP/IP

Основной протокол сетевого уровня – IP-протокол

Уровень II (Основной уровень)

Протокол управления передачей TCP (Transmission Control Protocol)

обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений

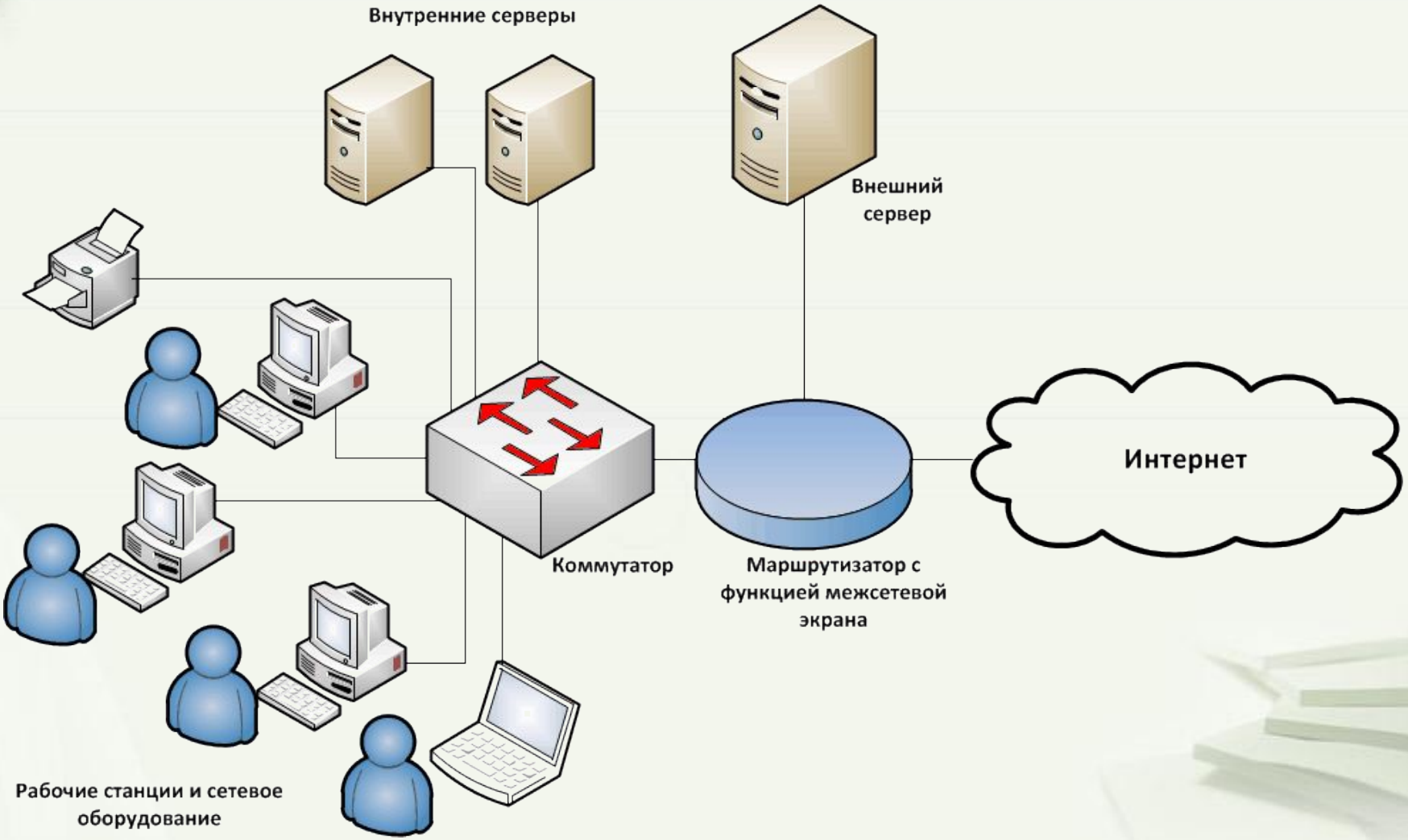
Протокол дейтаграмм пользователя UDP (User Datagram Protocol)

обеспечивает передачу прикладных пакетов дейтаграммным способом, как и IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами

Уровень I (Прикладной уровень)

- **FTP-протокол**
- **протокол эмуляции терминала telnet**
- **почтовый протокол SMTP**
- **гипертекстовые сервисы доступа к удаленной информации, такие как WWW и многие другие**

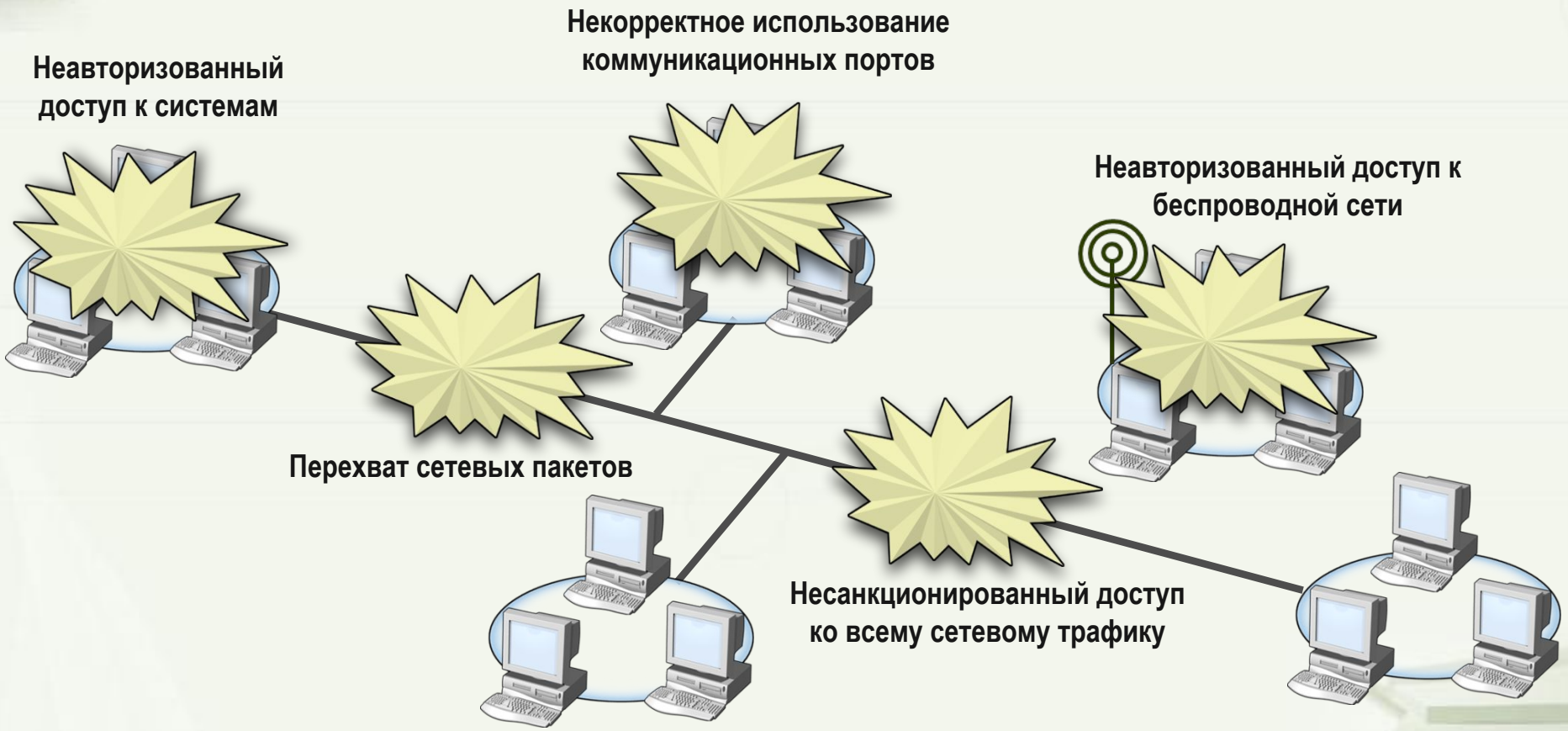
Типовая IP-сеть организации



Актуальность проблемы защиты информации в корпоративных сетях

- **Современные уровни и темпы развития средств информационной безопасности значительно отстают от уровней и темпов развития информационных технологий.**
- **Высокие темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности.**
- **Резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных.**
- **Значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютерных сетей.**
- **Многочисленные уязвимости в программных и сетевых платформах.**
- **Бурное развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.**
- **Современные методы накопления, обработки и передачи информации способствовали появлению угроз, связанных с возможностью *потери*, *искажения* и *раскрытия* данных, адресованных или принадлежащих конечным пользователям.**
- **Низкая квалификация конечных пользователей в вопросах потенциальных угроз при работе в локальных сетях и глобальной сети Интернет.**

Угрозы локальной сети



Основные категории сетевых атак

Существует четыре основных категории сетевых атак:

- атаки доступа;
- атаки модификации;
- атаки типа «отказ в обслуживании»;
- комбинированные атаки.

Атаки доступа

- Подслушивание (Sniffing)
- Перехват (Hijacking)
- Перехват сеанса (Session Hijacking)

Атаки типа «отказ в обслуживании» (Denial-of-Service, DOS)

- Отказ в доступе к информации
- Отказ в доступе к приложениям
- Отказ в доступе к системе
- Отказ в доступе к средствам связи

Атаки модификации

- Изменение данных
- Добавление данных
- Удаление данных

Комбинированные атаки

- Подмена доверенного субъекта
- Посредничество
- Посредничество в обмене незашифрованными ключами
- Атака эксплойта
- Парольные атаки
- Угадывание ключа
- Атаки на уровне приложений
- Анализ сетевого трафика
- Сетевая разведка

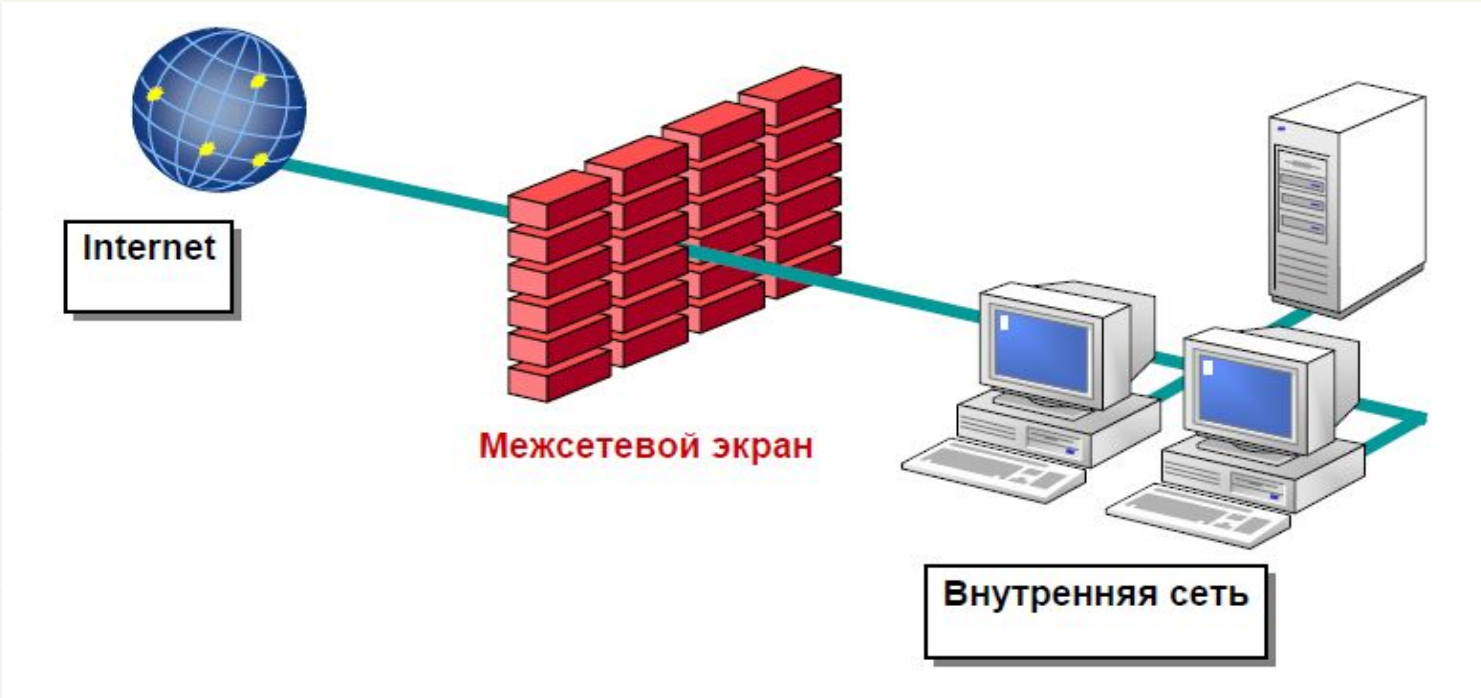
Комбинированные атаки

- Злоупотребление доверием
- Псевдоантивирусы
- Фишинг (Phishing)
- Фарминг (Pharming)
- Применение ботнетов
- Рассылка спама
- Анонимный доступ в сеть
- Продажа и аренда билетов
- Кража конфиденциальных данных

Угрозы и уязвимости беспроводных сетей

- Вещание радиомаяка
- Обнаружение WLAN
- Подслушивание
- Ложные точки доступа в сеть
- Отказ в обслуживании
- Атаки типа «человек-в-середине»
- Анонимный доступ в Интернет

Определение МЭ



Определение МЭ

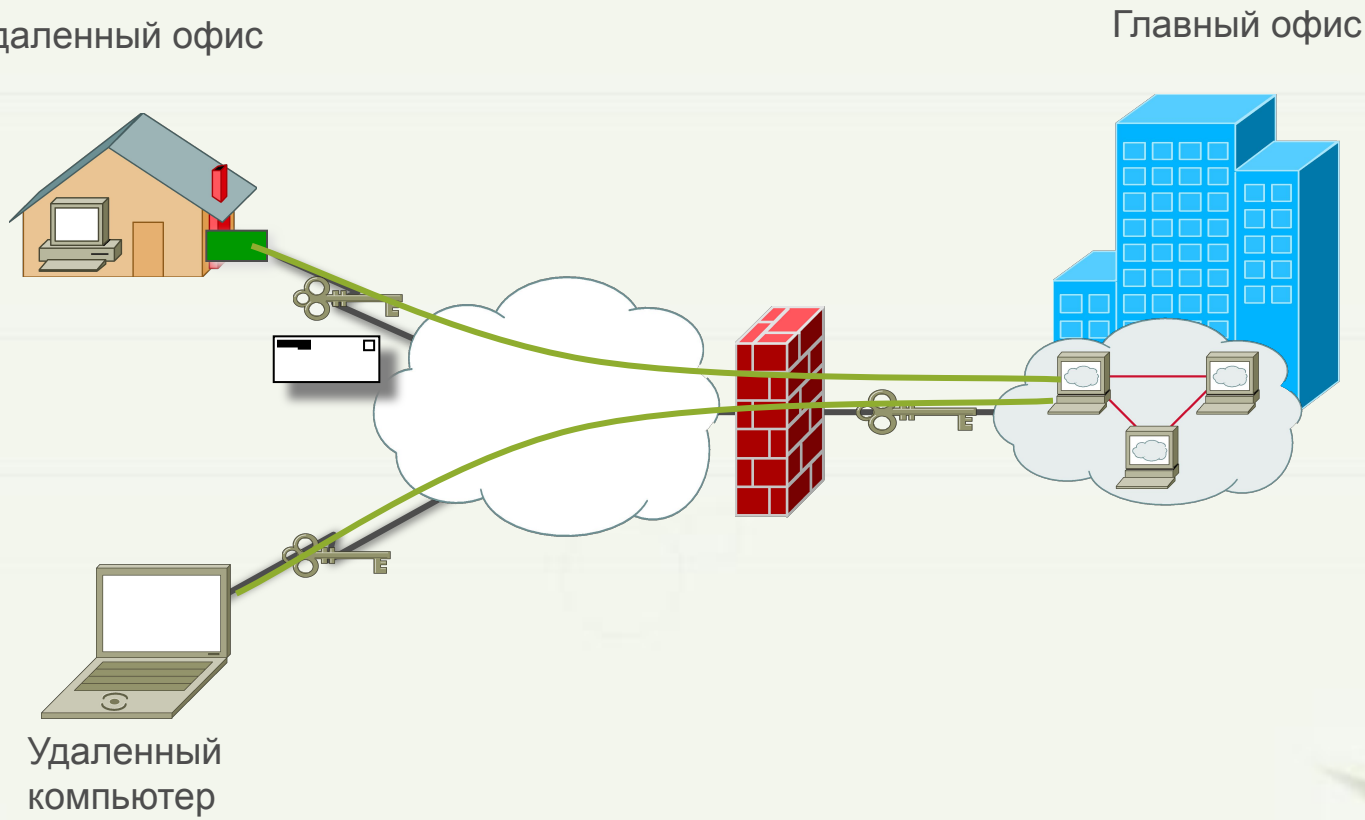
Межсетевой экран (brandmauer, firewall) – узел сети, служащий средством реализации политики информационной безопасности при межсетевом взаимодействии

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль информации, поступающей в ИС и/или выходящей из ИС, и обеспечивает защиту ИС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее передаче в (из) ИС

Основные функции МЭ

- **Управление трафиком (разрешение-запрет, фильтрация)**
- **Преобразование адресов**
- **Посредничество при реализации межсетевого взаимодействия (прокси)**
- **Аудит событий безопасности**
- **Оповещение администратора о событиях безопасности**

Защита межсетевого взаимодействия

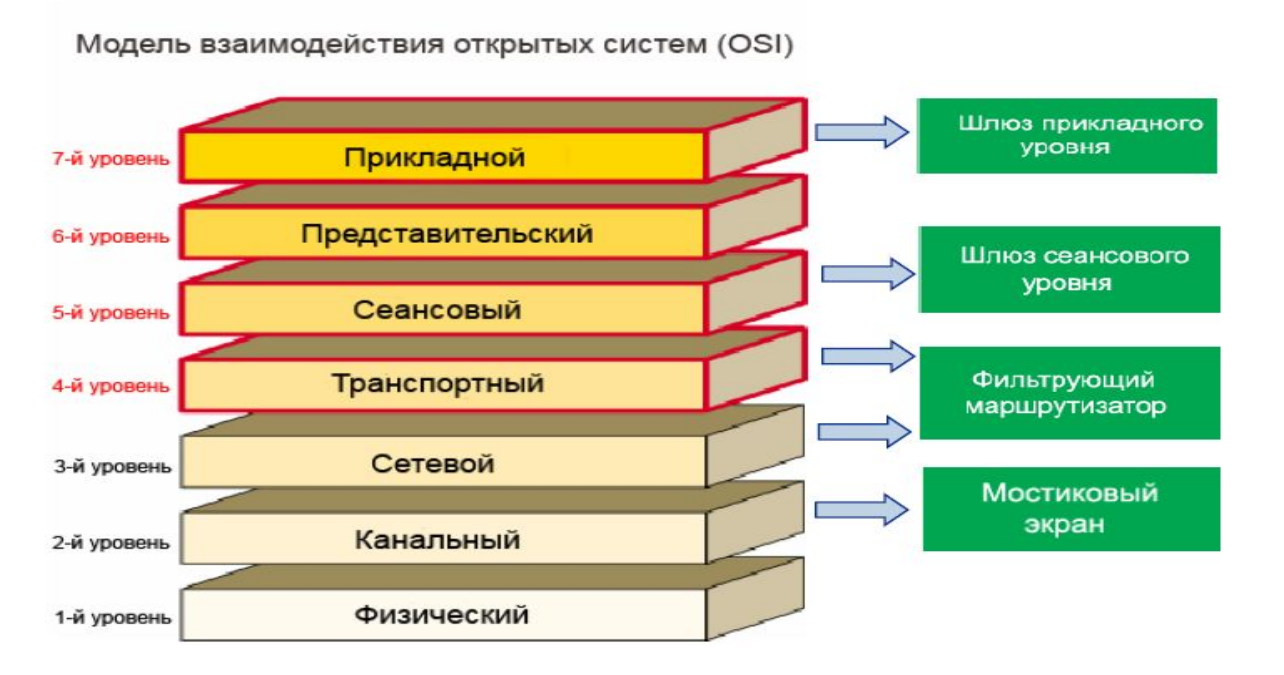


Классификация межсетевых экранов

1. По технологии:
   - фильтр VLAN (коммутатор)
   - пакетные фильтры (маршрутизатор)
   - шлюзы сеансового уровня
   - МЭ инспекции состояния
   - МЭ экспертного уровня
   - шлюз прикладного уровня (прокси-сервер)

2. По типам защищаемых объектов:
   - персональный МЭ
   - коллективный (пограничный, сетевой)

Классификация межсетевых экранов



3. В соответствии с функционированием на разных уровнях МВОС (OSI):

- Мостиковые экраны (2 уровень OSI)
- Фильтрующие маршрутизаторы (3 и 4 уровни OSI)
- Шлюзы сеансового уровня (5 уровень OSI)
- Шлюзы прикладного уровня (7 уровень OSI)
- Комплексные экраны (3-7 уровни OSI)

Пакетный фильтр («классический» межсетевой экран) (3-й и, отчасти, 4-й уровень OSI)

Особенности:

- Базовое средство защиты сети
- Пакеты проверяются на сетевом и транспортном уровне
- Списки доступа
- Фильтрация исходящего и входящего трафика

Функции пакетного фильтра успешно выполняет МАРШРУТИЗАТОР

Пакетные фильтры

Проводят анализ информации:

- физический сетевой интерфейс, с которого получен пакет (MAC-адрес);
- IP - адрес источника;
- IP - адрес назначения;
- тип протокола (TCP,UDP,ICMP);
- номер порта источника;
- номера порта назначения.

Выполняют действия:

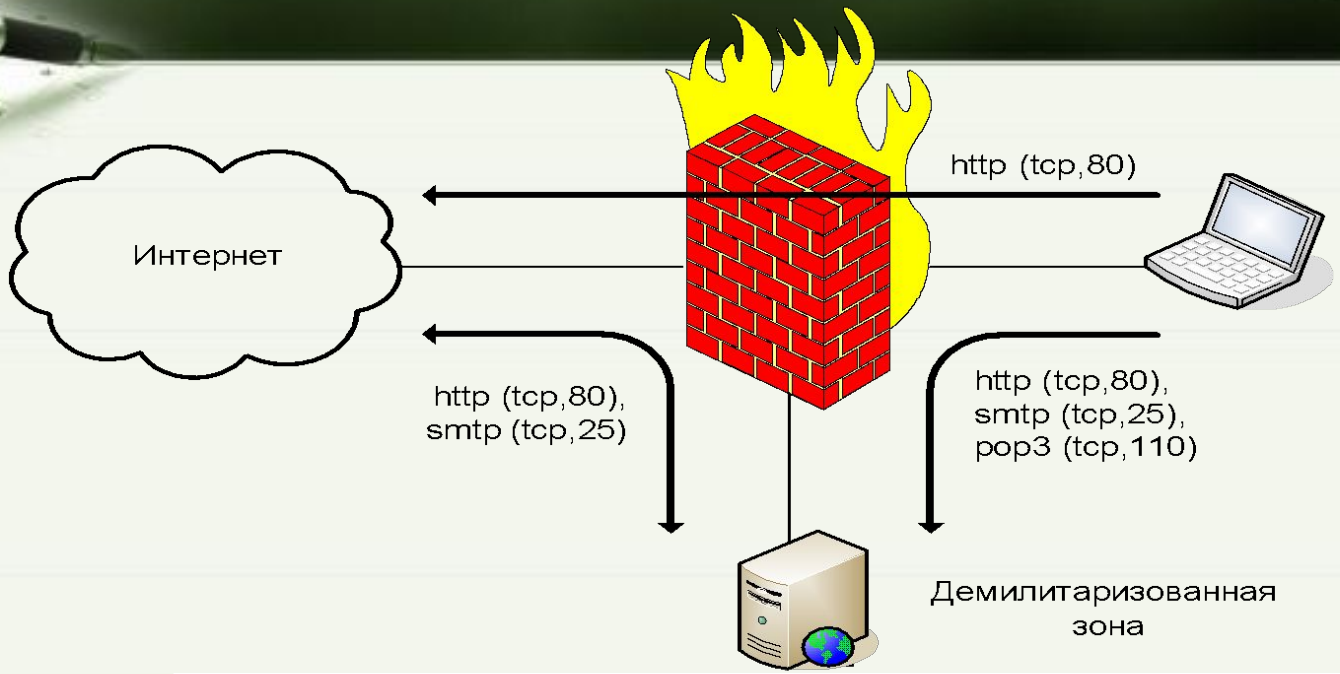
- Запретить (deny)
  - drop (“сброс соединения” TCP)
  - reject (хост недостижим или порт недоступен)
- Разрешить (allow)

Логика работы пакетного фильтра

1. **ЗАПРЕЩЕНО ВСЁ,**
   что явным образом не разрешено

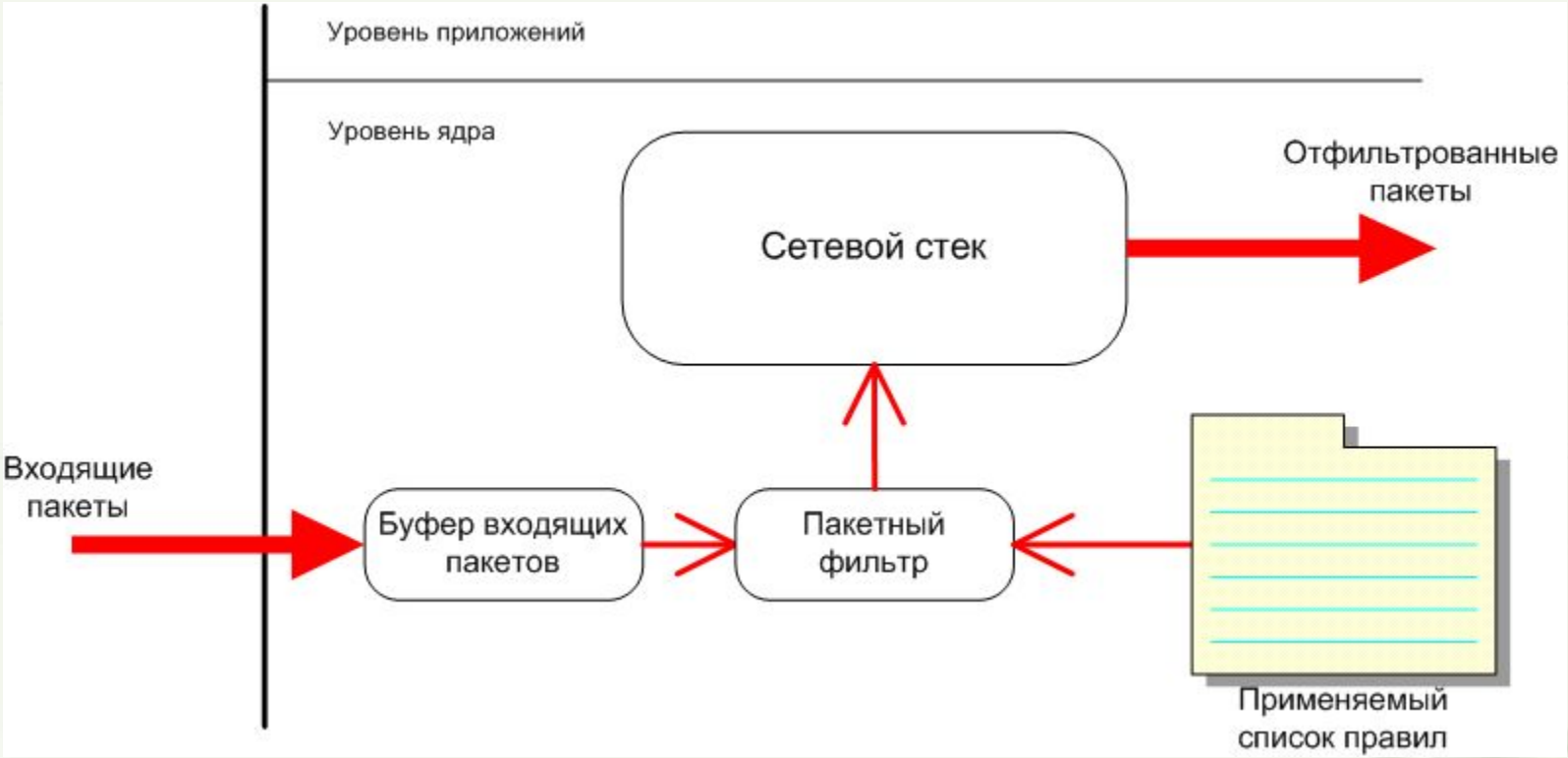
2. **Обработка правил осуществляется в порядке следования «СВЕРХУ ВНИЗ»**

Правила пакетной фильтрации



Источник	Цель	Протокол	Действие
1	3	http	разрешить
1	2	http	разрешить
1	2	smtp	разрешить
1	2	pop3	разрешить
2	3	smtp	разрешить
3	2	http	разрешить
любой	любой	любой	запретить

Принцип работы пакетного фильтра



Достоинства пакетных фильтров

- **Высокая производительность**
- **Относительная дешевизна**
- **Возможность трансляции сетевых адресов**
- **Могут быть реализованы «аппаратно»**
- **Не требуют конфигурирования конечных сетевых узлов, «прозрачны» для приложений**
  - Не хранят информацию о сеансе
  - Нет аутентификации при обращении к службам МЭ

Эффективно противодействовать угрозам на сетевом уровне способны межсетевые экраны, обрабатывающие не только содержание пакетов, но и закономерность передвижения пакетов

Межсетевые экраны уровня соединения (шлюзы сеансового уровня)

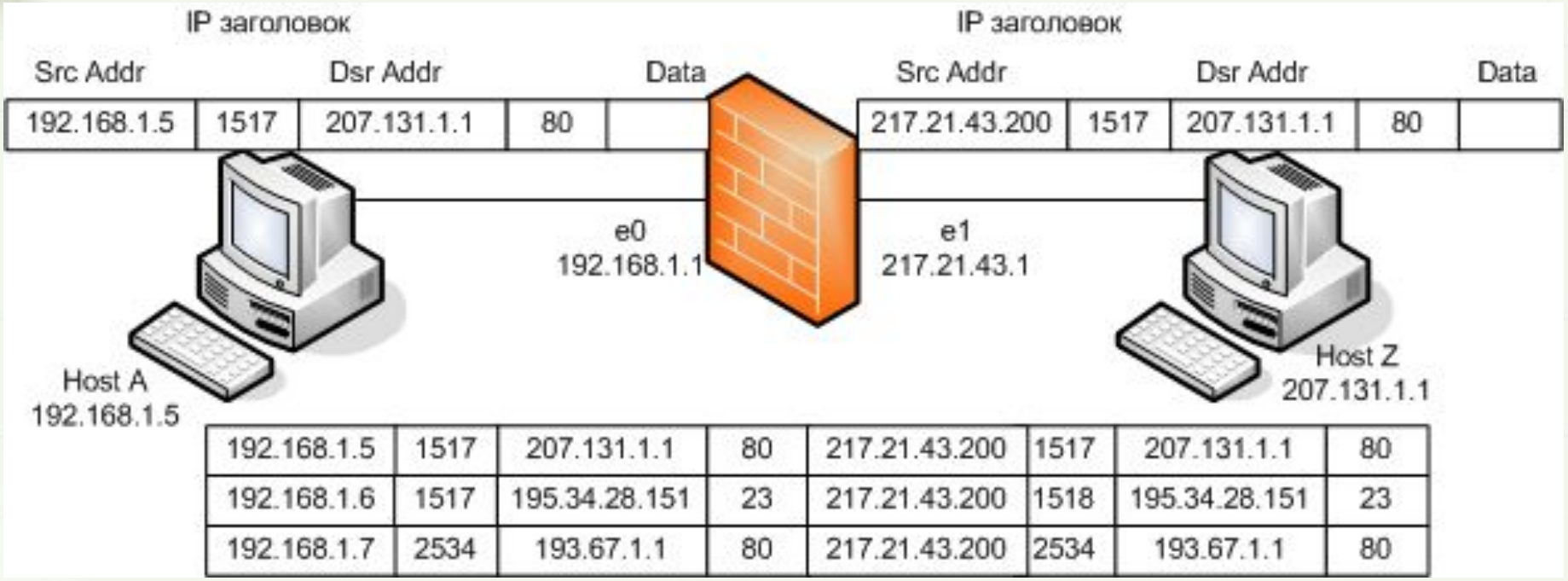
Основная задача – проверка, является ли пакет **запросом** на соединение (TCP) или представляет данные, относящиеся к **установленному соединению** между транспортными уровнями различных узлов.

Трансляция сетевых адресов (network address translation, NAT)

Используется для:

1. Скрытия адресации внутренней сети от внешнего сегмента
2. Обеспечения частичной анонимности отправителя пакета.
3. Преобразования приватных IP адресов внутренней сети (192.168.*.*, 172.16-31.*.*, 10.*.*.*) в реальные - для возможности работы в Интернет.

Трансляция адресов портов (port address translation, PAT)



192.168.1.5	1517	207.131.1.1	80	217.21.43.200	1517	207.131.1.1	80
192.168.1.6	1517	195.34.28.151	23	217.21.43.200	1518	195.34.28.151	23
192.168.1.7	2534	193.67.1.1	80	217.21.43.200	2534	193.67.1.1	80

Адреса внутренних узлов могут быть преобразованы в один глобальный адрес (назначенный внешнему интерфейсу), но отправляться вовне с разных «жестко привязанных» портов

Межсетевые экраны прикладного уровня (proxy)

Основная задача – проверка данных на соответствие *определенному* протоколу прикладного уровня перед установкой соединения.

Устанавливает состояние полного (завершенного) соединения и последовательность информации.

Проверка параметров безопасности, содержащихся внутри данных прикладного уровня.

Межсетевые экраны прикладного уровня

Межсетевые экраны прикладного уровня

Каждая служба-PROXY специфична и предназначена для определенного приложения.

Функционирует на прикладном уровне.

«Прозрачна» для пользователя.

Достоинства МЭ прикладного уровня

- Работают с протоколами верхнего уровня (только :)
- Хранят информацию о состоянии приложения и сеанса
- Имеют возможность ограничивать доступ к определенным сетевым службам
- Оперируют с данными, содержащимися в пакете
- Обеспечивают возможность выполнения дополнительных функций (кэшируют ответы, фильтруют URL, поддерживают аутентификацию)
- Проводят аудит событий

Недостатки МЭ прикладного уровня

- PROXY «слушают» порт, как сетевой сервис, т.е. не работают с портом, как МЭ
- Вносят временнỳю задержку (пакет обрабатывается дважды – приложением и PROXY)
- Каждому протоколу – свой PROXY
- PROXY требуют выполнения настроек на стороне клиента
- PROXY уязвимы к ошибкам прикладного уровня

Межсетевые экраны экспертного уровня

- имеют набор прикладных посредников
- поддерживают технологию инспекции состояния
- имеют встроенные механизмы обнаружения и защиты от типовых атак
- предоставляют возможности централизованного управления и интеграции с системами управления сетями
- поддерживают усиленные схемы аутентификации
- имеют развитую систему аудита и уведомления о событиях безопасности
- поддерживают технологии VPN

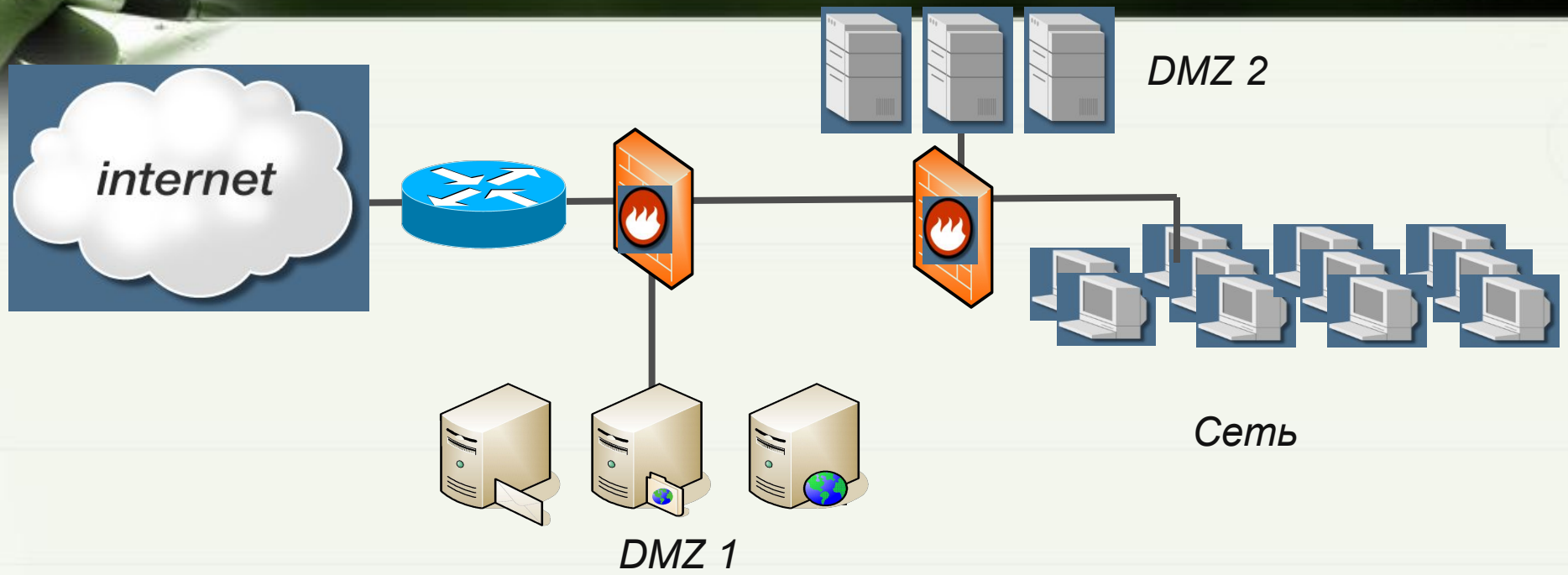
Демилитаризованная зона

DMZ (Demilitarized Zone) демилитаризованная зона – сеть, которая добавляется между защищенной сетью и сетью, которая имеет меньший уровень безопасности, для создания дополнительного уровня безопасности.

Задачи защиты DMZ

- разграничение доступа к ресурсам и серверам в DMZ
- конфиденциальность информации, передаваемой при работе пользователей с ресурсами DMZ
- контроль за действиями пользователей, например, за обращениями к базам данных.

Архитектура DMZ



СТБ 34.101.13-2009 Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в демилитаризованной зоне корпоративной сети

СТБ 34.101.14-2009 Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты программных средств маршрутизатора для использования в демилитаризованной зоне корпоративной сети.

Контроль контента

- Контроль содержания электронной почты
- Контроль содержания Web трафика

СТБ П 34.101.4-2010 Информационные технологии и безопасность. Критери оценки безопасности информационных технологий. Профиль защиты электронной почты предприятия. 01.07.2010

Основные функции систем контроля контента электронной почты

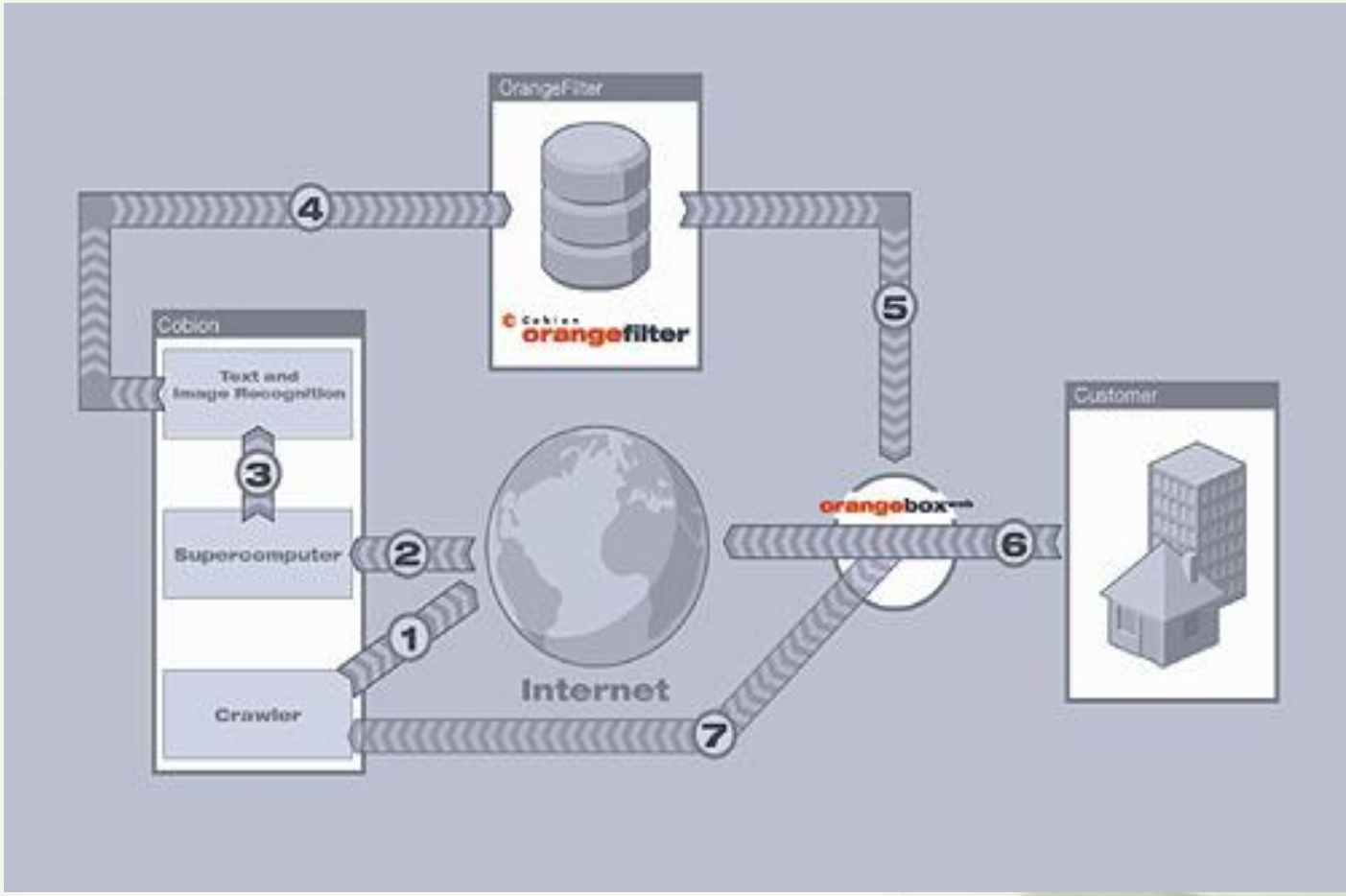
- **Борьба с утечками конфиденциальной информации**
  - полный разбор сообщений с вложениями любого типа;
  - анализ почтового сообщения по всем его составляющим: атрибутам SMTP конверта, заголовкам сообщения, MIME- заголовкам, телу сообщения, присоединенным файлам;
  - службы оповещения о нарушении политики использования почты;
  - карантин для подозрительных сообщений. Проверка IP, протоколов, URL, типов и объема данных
  - анализ содержания текстов
  - распознавание графики
  - антивирусная проверка
- **Защита от спама и потенциально опасных вложений**
  - многоступенчатый механизм распознавания спама;
  - поддержка "черных" и "белых" списков;
  - автоматизированная настройка фильтров;
  - контекстный анализ сообщений;
  - использование антивирусных программ сторонних производителей;
  - совместная работа с межсетевыми экранами.
- **Повышение производительности и экономия средств**
  - получение реальной картины использования сотрудниками электронной почты;
  - гибкий инструмент для контроля переписки (по типу, размеру, содержимому, вложениям, адресам и другим заголовкам письма);
  - блокирование пересылки файлов, не относящихся к работе;
  - блокирование или отложенную доставку писем с вложениями большого объема (аудио, видео, фото).

Основные функции систем контроля Web контента

- **Борьба с утечками конфиденциальной информации**
  - фильтрации содержимого информации, исходящей из корпоративной сети вовне;
  - блокирования доступа к любой группе ресурсов, которые считаются опасными в связи с принятой в компании политикой безопасности. К таким ресурсам относятся, например:
    - бесплатные почтовые сервисы;
    - файлообменные сайты;
    - социальные сети (например: www.odnoklassniki.ru социальные сети (например: www.odnoklassniki.ru , http://moikrug.ru);
    - live journals (ЖЖ);
    - IM (ICQ, jabber, msn и т.д.).
- **Обеспечение безопасности использования Интернет-ресурсов**
  - блокировку Интернет-ресурсов, содержание которых нежелательно или подозрительно;
  - фильтрацию информации, передаваемой по каналу HTTP, по адресам, форматам и содержимому;
  - антивирусную проверку;
  - мониторинг активности пользователей;
  - протоколирование действий пользователей;
  - оповещение о нарушении политики безопасности.
- **Повышение производительности и экономия средств**
  - категоризацию и блокирование доступа к сайтам, не связанным с работой;
  - блокирование загрузки файлов, не относящихся к работе;
  - установку ограничений на типы скачиваемых файлов и на объем
  - пользовательского трафика;
  - получение реальной картины использования сотрудниками Интернет-ресурсов.

Алгоритм работы системы контроля Web контента

1. «Паук» crawler ползает по Сети
2. Загрузка страниц в компьютерный центр
3. Анализ содержания текстов и изображений этого сайта и их классификация
4. Создание БД по категориям сайтов
5. Обновление БД
6. Пользователь просматривает Интернет-ресурсы
7. Инициируется адаптация БД



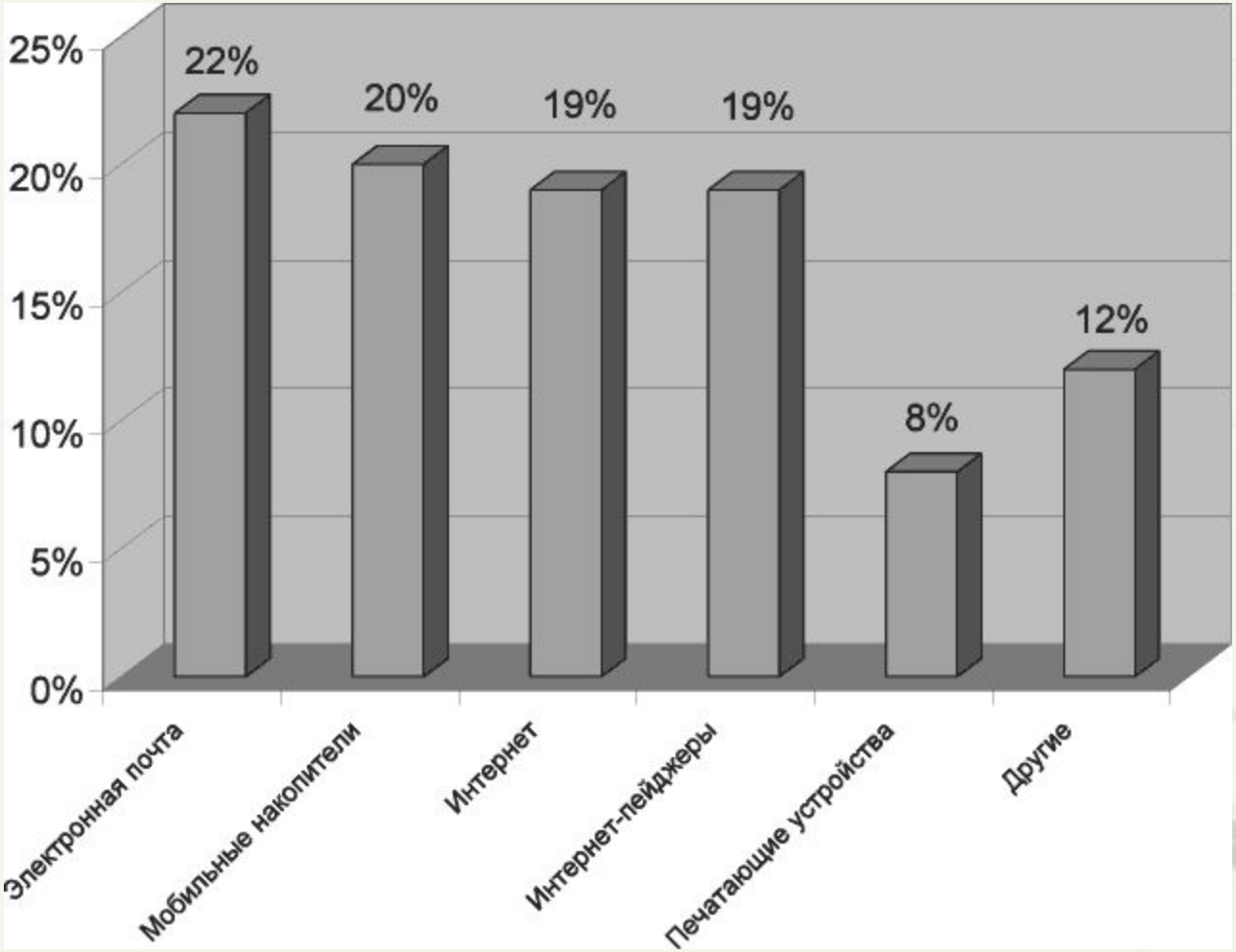
Пример категорий Web контента

- Азартные игры
- Алкоголь
- Армия
- Автомобили/Транспорт
- Бизнес/услуги
- Благотворительные фонды
- Вебпочта
- Видео
- Вирусные и вредоносные сайты
- Для взрослых/эротика
- Дом/Досуг
- Загрузки
- Здоровье
- Знакомства
- Игровые порталы
- Компьютеры и Технологии
- Криминальная деятельность/хакерство
- Личные веб-страницы
- Магазины
- Музыка
- Наркотики
- Насилие
- Нецензурная речь
- Новости
- Образование и обучение
- Оружие
- Переводы
- Поиск работы
- Поисковые движки
- Политика и Закон
- Порнография/секс
- Правительство
- Путешествия
- Религия
- Риэлторские услуги
- Сайты знакомств
- Сообщества
- Социальные сети
- Спамерские сайты
- Спорт и Отдых
- Табак
- Фармация
- Финансы
- Фишинг
- Чат
- Юмор

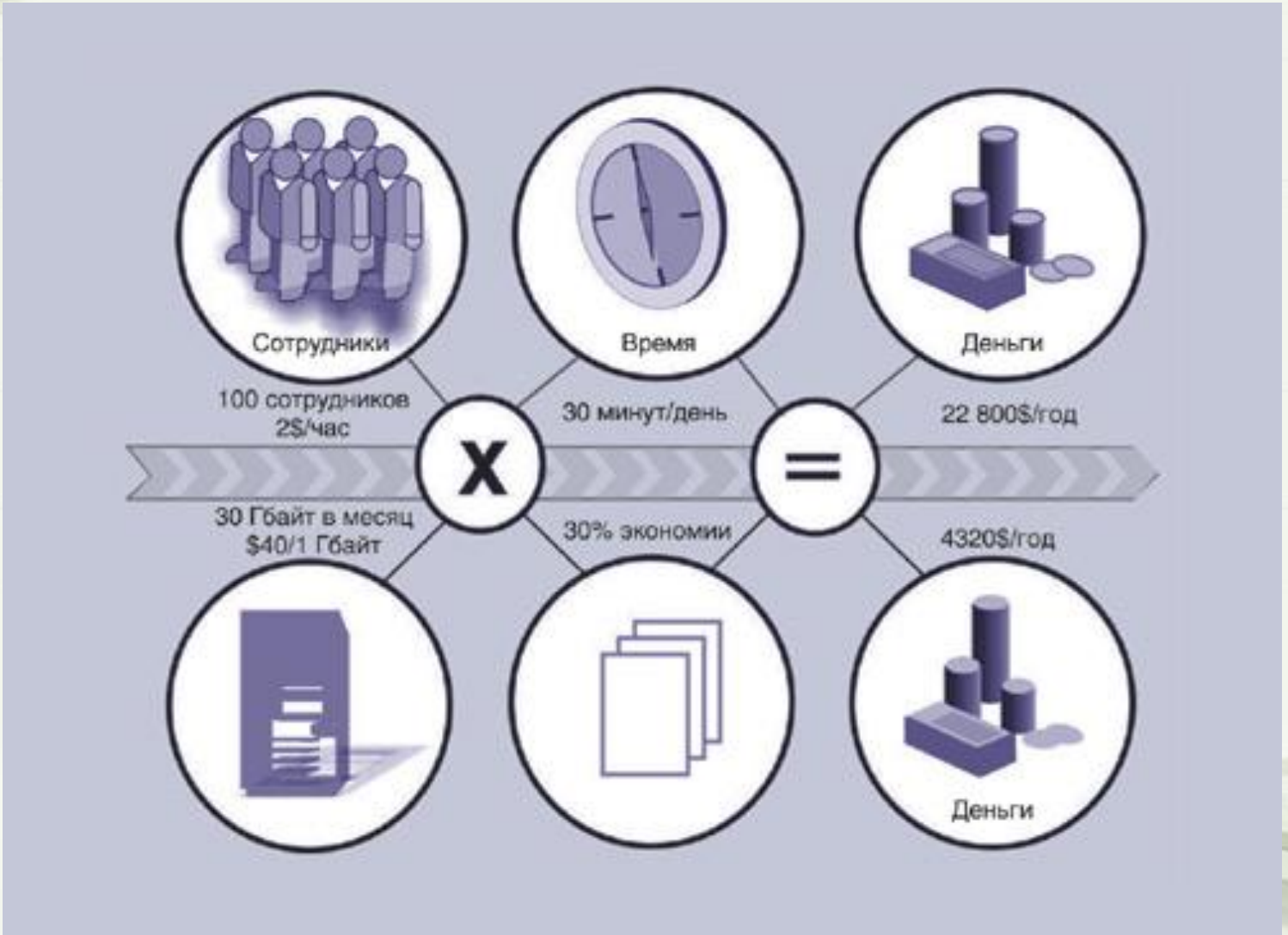
Средство скрытого проникновения в корпоративные сети

- **spam**
- **интернет-пейджеры (IM, Instant messaging)**
  - AOL (AOL IM – AIM, Trillian, SameTime Connect)
  - ICQ (ICQPro, ICQ Lite)
  - Microsoft (MSN Messenger, Windows Messenger, Trillian)
  - Yahoo! (Yahoo! Messenger, Trillian)
- **распределенные сети P2P (Peer-to-peer)**
  - Файловые обменные сети
  - Распределенные вычислительные сети
  - Службы сообщений
  - Сети групповой работы

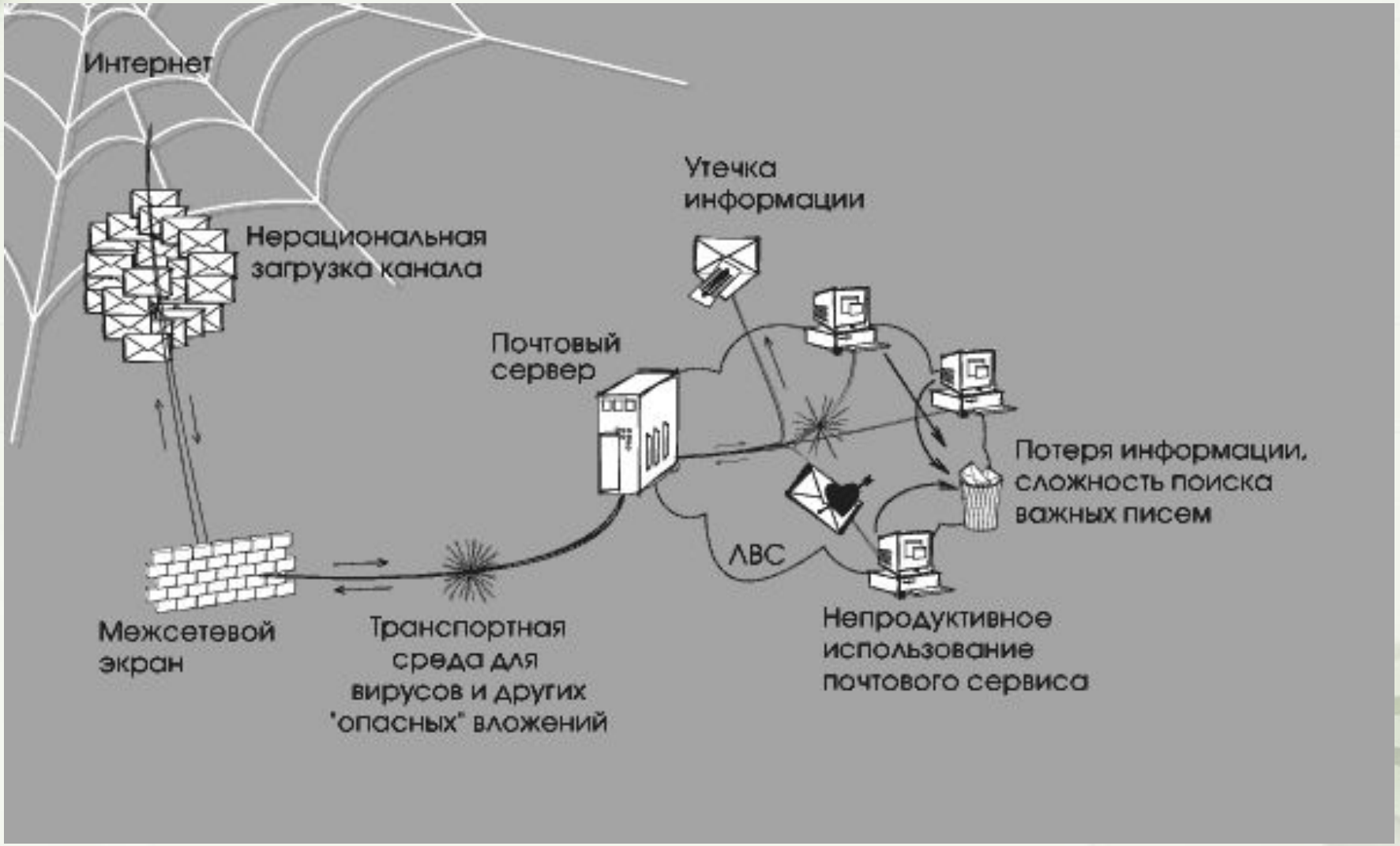
Канал утечки конфиденциальной информации



Интернет и проблемы рабочего времени



Проблемы электронной почты



Структура общего почтового трафика

По оценке Symantec, во второй половине 2006 года количество спам-рассылок неуклонно увеличивалось, доля спама в среднем составляла 59% от общего объема регулируемого трафика, а в странах Европы, Ближнего Востока и Африки - 66%. Зафиксированные Symantec объемы нелегитимных сообщений на 65% состояли из англоязычного спама. Каждое 147-е спам-письмо было снаряжено вредоносным кодом.

Решение проблем защиты электронной почты

- Антивирусная защита
- Защита от спама
- Контроль содержимого (контента)

Антивирусная защита

Антивирусная защита электронной почты – ключевой элемент борьбы с вирусами

- **Антивирусная защита SMTP коннектора**
- **Антивирусная защита почтового сервера**
- **Антивирусная защита почтового клиента**

Защита от спама

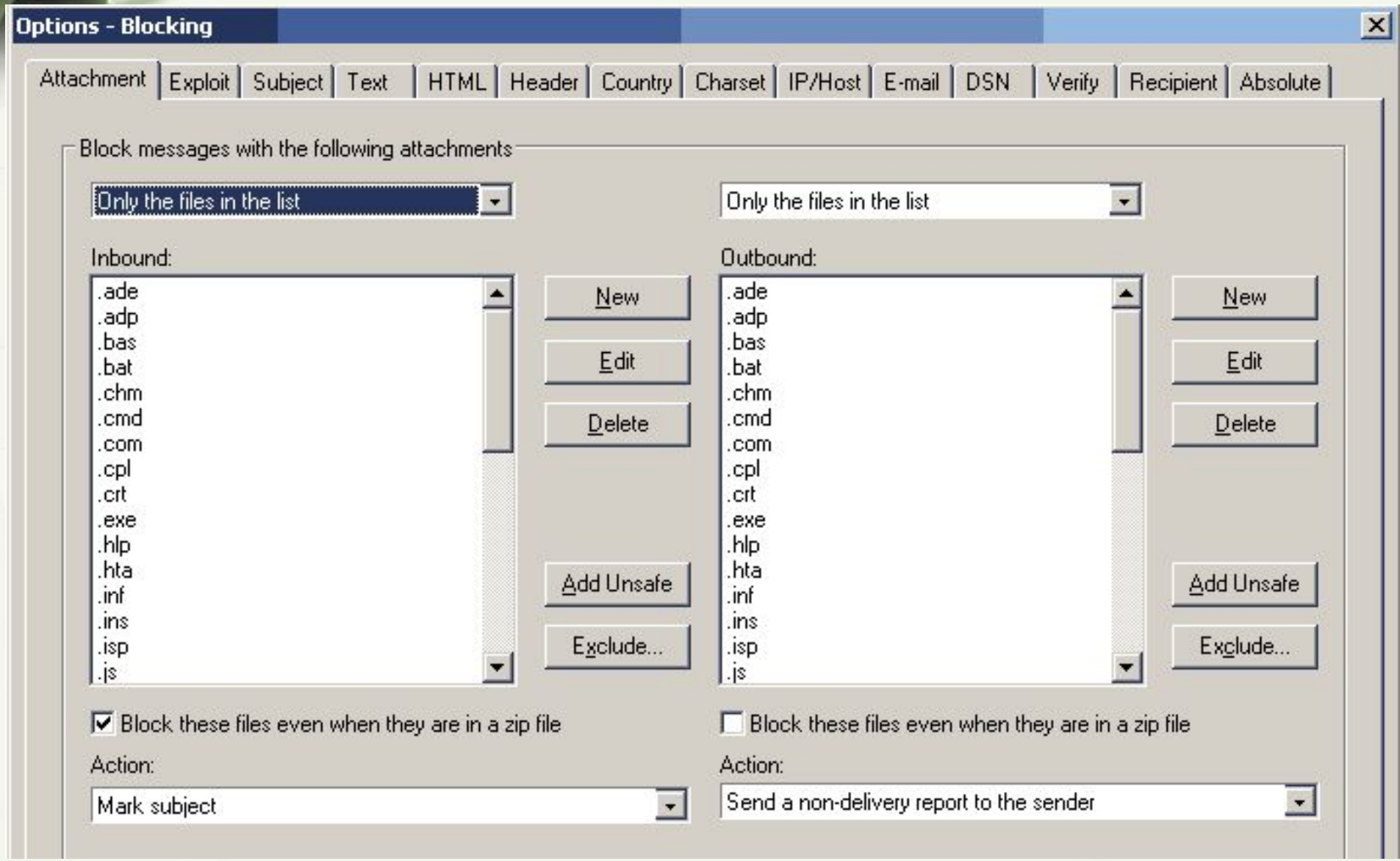
Признаки определения спама:

- сообщение является массовой рассылкой;
- сообщение рассылается без согласия пользователя;
- сообщение содержит рекламу;
- сообщение является анонимным.

Методы защита от спама

- Фильтрация почты по “черным спискам”
- Запрет на получение или отправление файлов определенного типа
- Метод GreyListing
- Фильтрация по теме письма
- Фильтрация контента письма
- Аутентификация почтовых серверов

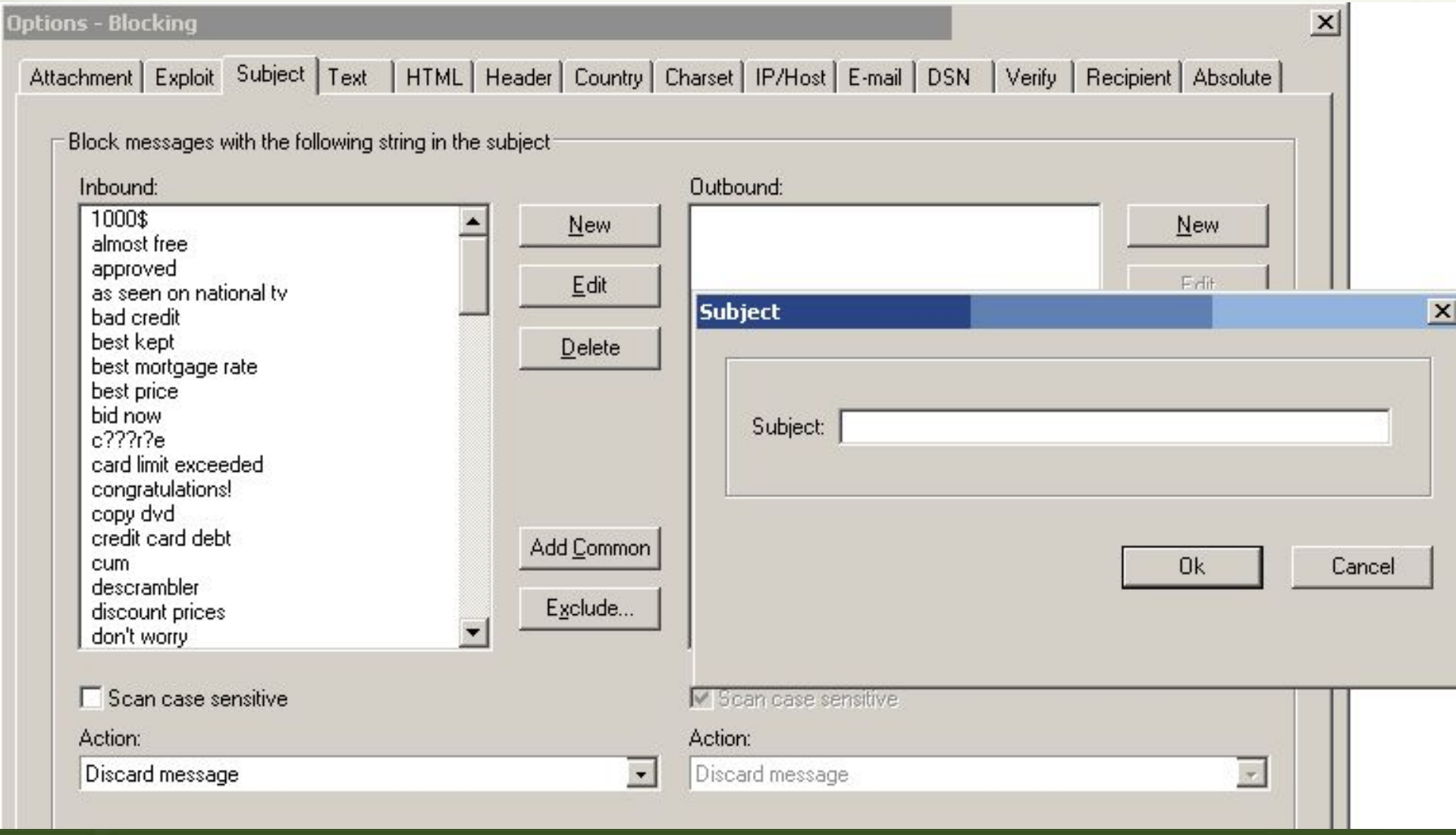
Запрет на файлы определенного типа



Метод GreyListing

- Почтовый сервер отклоняет сообщение в момент прибытия с ошибкой 4xx
- Помещает в базу GreyListing следующие данные:
  - IP-адрес сервера, отправляющего почту
  - почтовый адрес отправителя
  - почтовый адрес получателя
- Легитимный сервер, отправляющий почту повторяет попытку посылки сообщения, т.к. получил ошибку 4xx
- Сервер получатель по базе GreyListing проверяет вновь полученное сообщение, авторизация прошла – почта доставляется получателю

Фильтрация по теме



Фильтрация по тексту

- Метод Distributed Checksum Clearing house (DCC)

http://www.rhyolite.com/anti-spam/dcc

- Статистический метод (Statistical Token Analysis – STA)
- Метод Байеса (Bayes)

Технологии аутентификации

Аутентификация отправителя по IP-адресу:

- SPF (Sender Policy Framework) RFC4408 апрель 2006 - Experimental Protocol (Meng Wong as *Sender Permitted From)*
- SenderID

Криптографическая аутентификация отправителя:

- DKIM

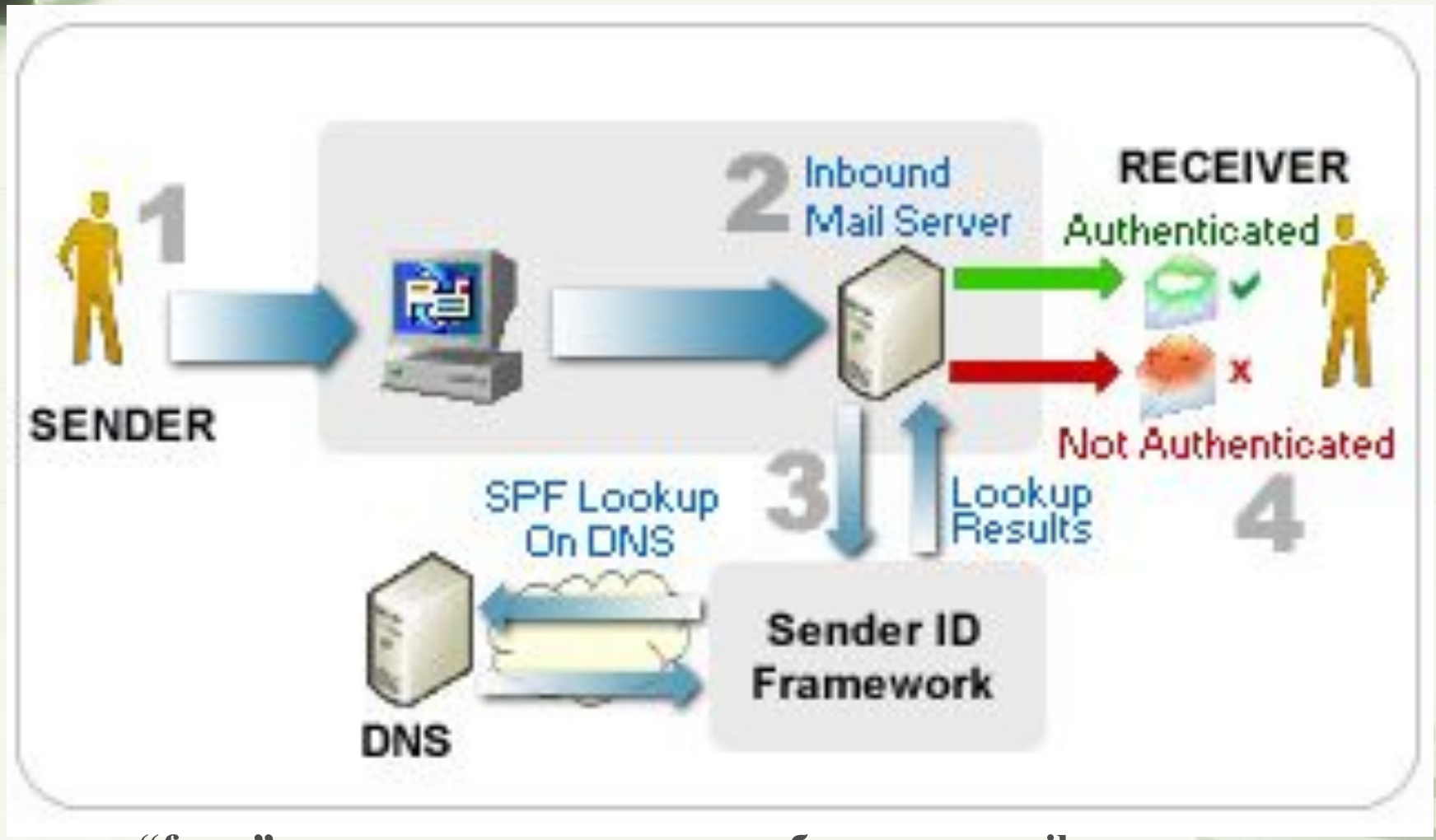
Метод SPF

- Администратор (владелец) домена публикует данные, описывающие возможные источники электронной почты с адресами отправителя из этого домена.
- Почтовый сервер, принимающий E-mail с адресом отправителя из данного домена, может сопоставить реальный источник сообщения (IP-адрес стороны, посылающей почту) с данными, которые опубликовал владелец домена.

Метод SPF

- Результатом анализа SPF-политики на принимающей стороне является SPF-статус сообщения, который может иметь одно из следующих значений:
  - Pass - отправитель сообщения не подделан (согласно анализу SPF-политики).
  - Softfail - сообщение не отвечает "жестким" критериям достоверности отправителя, но нельзя и быть уверенным, что отправитель подделан.
  - Fail - отправитель подделан.

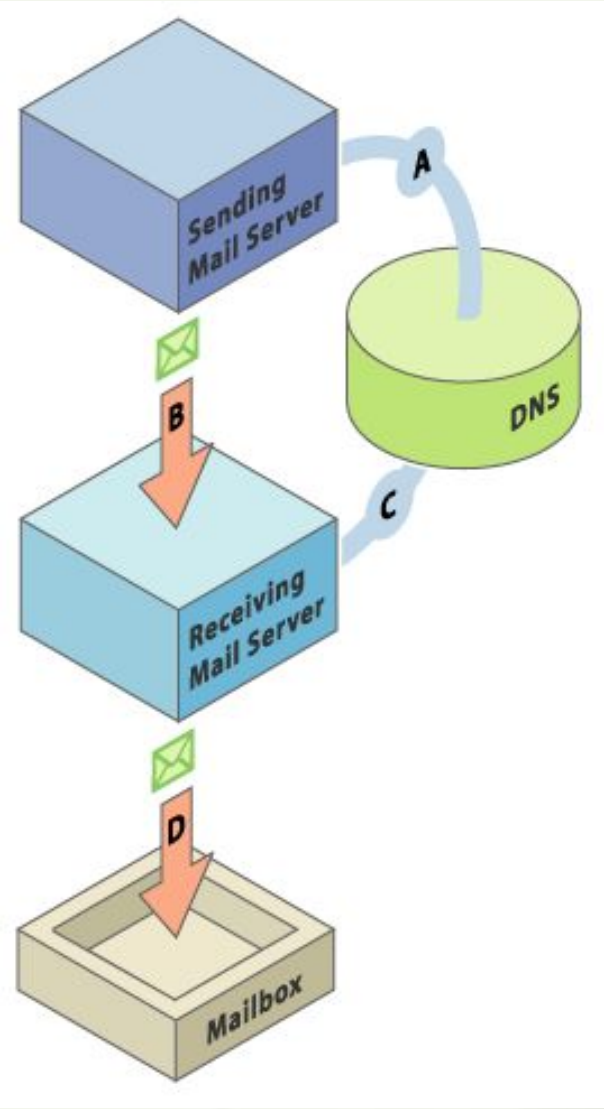
Sender ID Framework *Microsoft*



Проверяет “from”, содержащиеся в теле сообщения e-mail, а не только адреса отправителя уровня SMTP (envelope sender).

DKIM

- Владелец почтового сервиса (отправитель) генерирует пару криптоключей (публичный и приватный).
- Публичный ключ публикуется в DNS, а приватный ключ используется на почтовых серверах для пометки всей исходящей корреспонденции.
- Другая сторона (получатель) извлекает из поля «From» имя домена и отправляет запрос к серверу DNS, чтобы получить публичный ключ для этого домена, после чего проверяет подлинность подписи в заголовке почтового сообщения.



DKIM

- **Достоинства**
  - **«достоверность» является свойством письма, а не почтовой сессии**
- **Недостатки**
  - **при внедрении на публичном сервисе, можно получить любое нужное количество подписанных сообщений.**

Защита электронной почты– организационные меры в сочетании с техническими средствами

Для защиты компании от рисков, связанных с использованием электронной почты, необходимы:

Политика использования электронной почты + Средство реализации политики

Политика использования электронной почты

Что контролируется	Прохождение каких сообщений входящей, исходящей или внутренней электронной почты должно быть разрешено или запрещено.
На кого распространяется	Категории лиц, которым разрешено или запрещено отправлять исходящие или получать входящие сообщения электронной почты.
Как реагирует система	Что необходимо делать с теми или иными сообщениями электронной почты, которые удовлетворяют или не удовлетворяют критериям, определенным правилами использования электронной почты.

Системы контроля контента электронной почты

Функции:

- **декомпозиция электронного письма**
- **анализ содержимого каждого компонента**
- **фильтрация**
- **реагирование**
- **ведение архива переписки по электронной почте.**

Технические решения защиты электронной почты

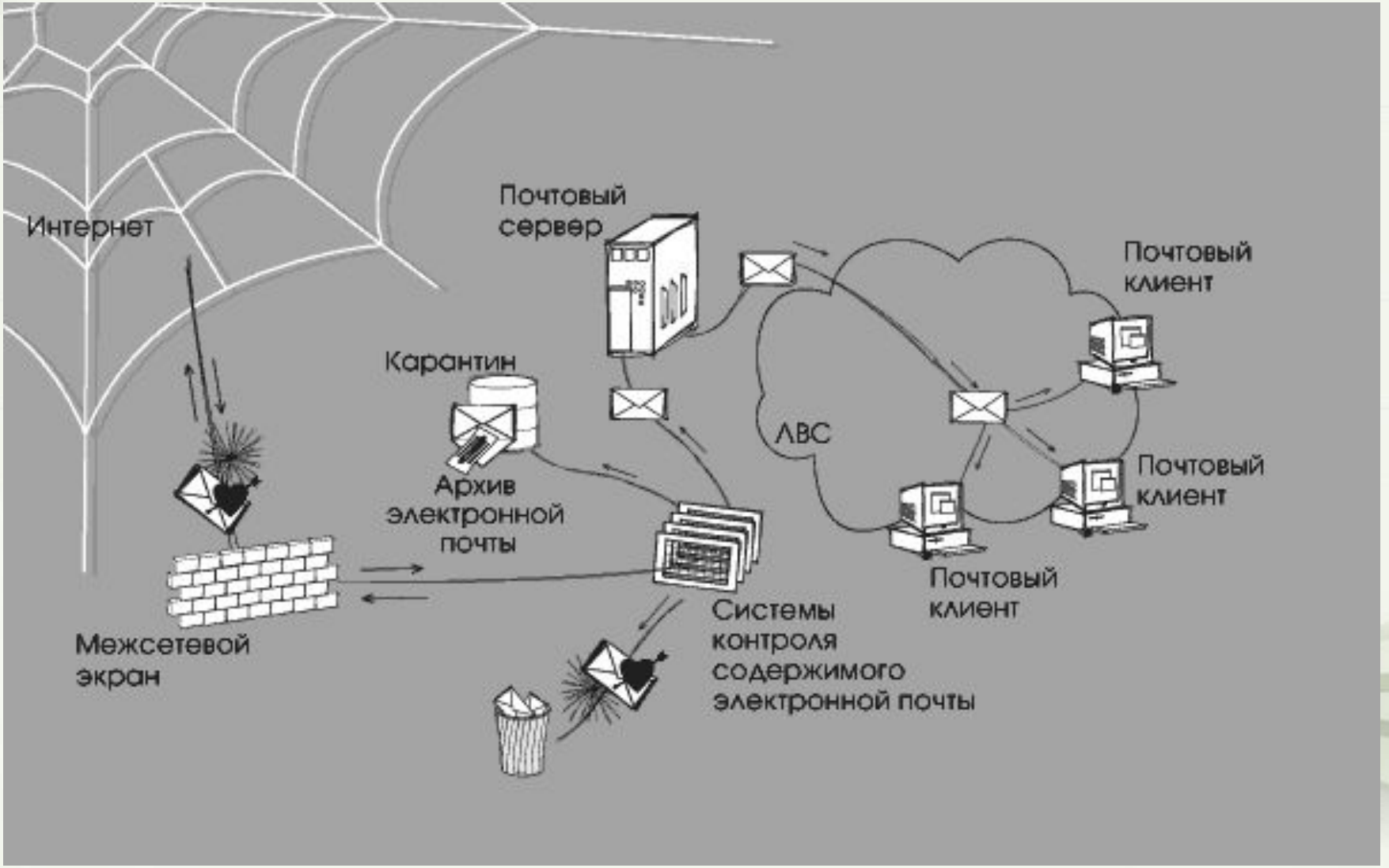
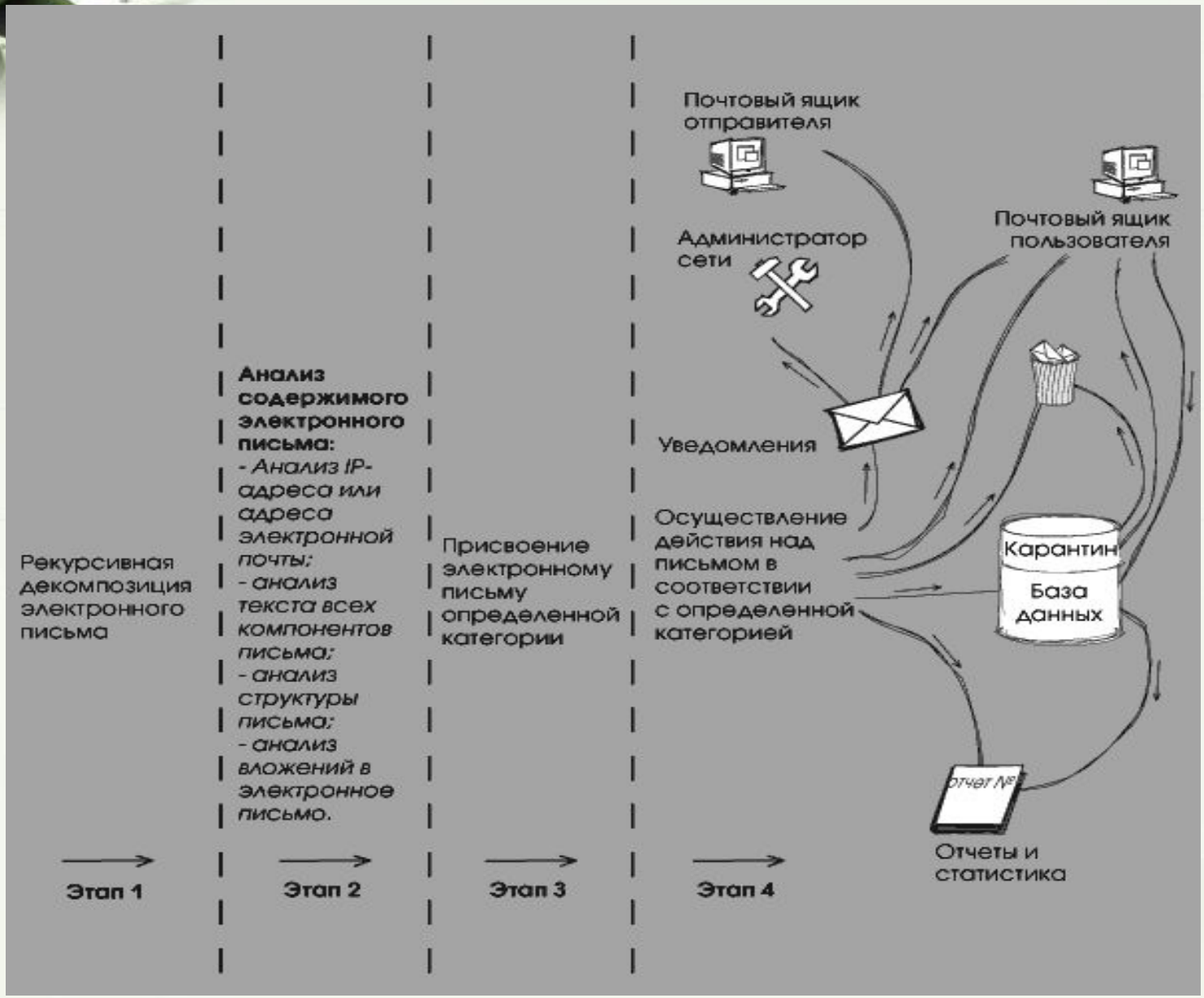


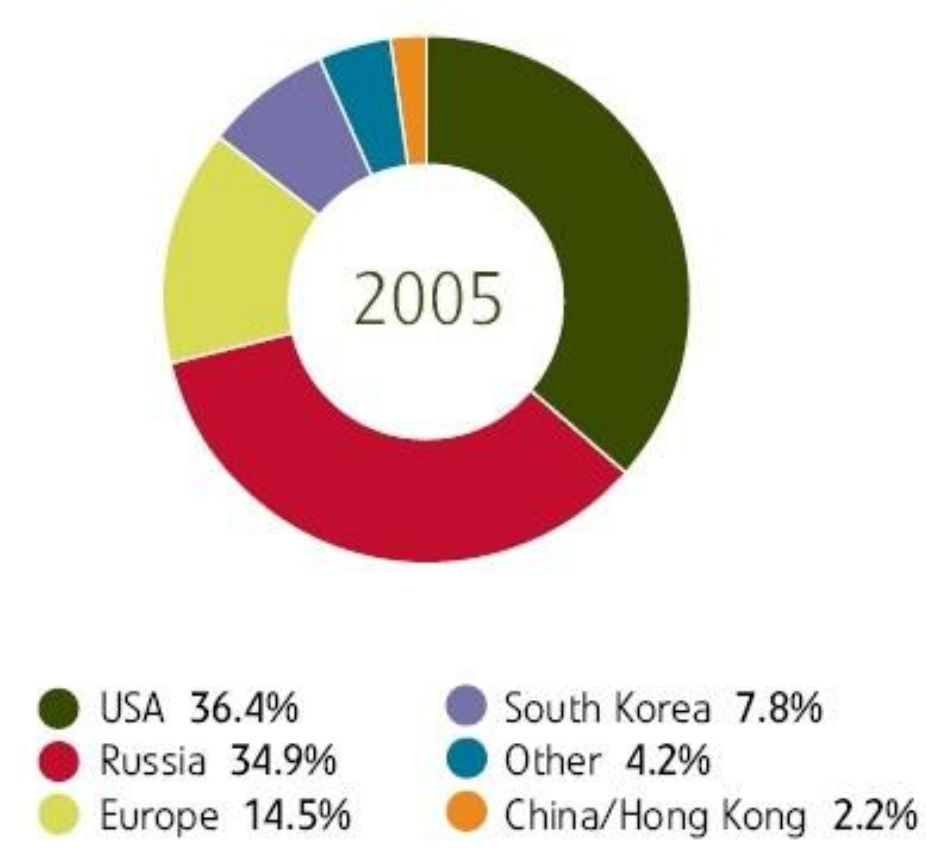
Схема обработки сообщений



Требования к системам контроля содержимого электронной почты

- ***Полнота*** **— это способность систем контроля обеспечить наиболее глубокую проверку сообщений электронной почты**
- ***Адекватность*** **— это способность систем контроля содержимого как можно более полно воплощать словесно сформулированную политику использования электронной почты, иметь все необходимые средства реализации написанных людьми правил в понятные системе условия фильтрации.**

Распределение сайтов с нелегальным контентом



По материалам отчета Internet Watch Foundation за 2005 год (Фонд Интернет наблюдения).

Системы контроля Web-трафика

Основные функции:

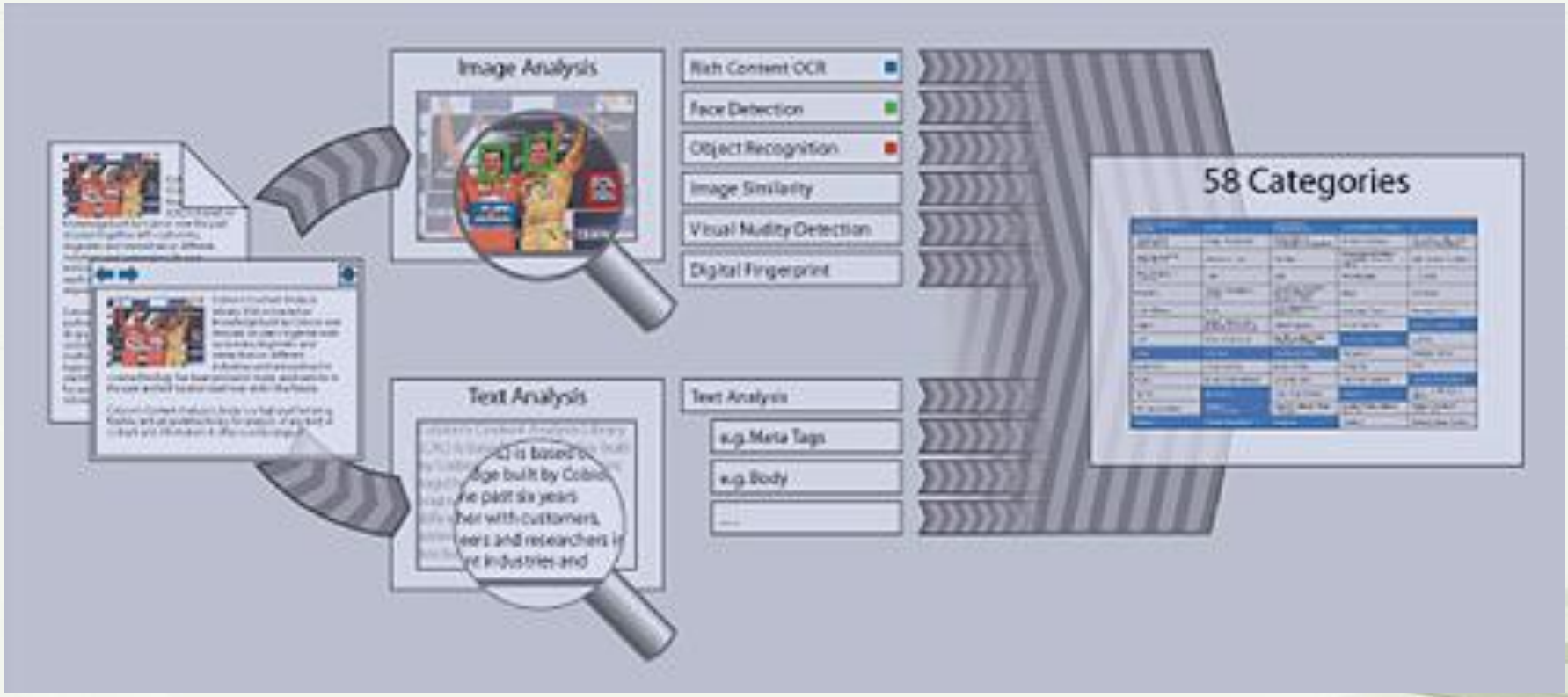
- **Классификация трафика, приходящего из Интернет**
  - **Проверка IP, протоколов, URL, типов и объема данных**
  - **Анализ содержания текстов**
  - **Распознавание графики**
  - **Антивирусная проверка**
- **Разграничение доступа для определенных категорий пользователей**
- **Действие системы**

Системы контроля Web-трафика

Могут обеспечить:

- **предотвращение утечки конфиденциальной информации**
- **мониторинг подозрительной и запрещенной активности пользователя**
- **защиту от атак с использованием социальной инженерии**
- **защиту от вирусов и др. вредоносного кода**
- **контроль доступа пользователей к Интернет ресурсам**
- **организацию упорядоченного использования Интернет ресурсов пользователями**

Схема классификации содержимого Интернета по категориям



Настройка правил

Технологии фильтрации IM и P2P трафика

- Детектирование протокола передачи данных
- Мониторинг соединений на портах, характерных для IM и P2P трафика
- Проверка сигнатур передаваемых файлов
- Антивирусная проверка
- Фильтрация на основе смыслового анализа текстов сообщений
- Блокировка спима (спам для IM)

Обзор систем контентной фильтрации

Производитель	Страна	Программный продукт
Secure computing	США	Webwasher SCM Suite SmartFilter®, Sentian
JSB Software Technologies	Англия	Surfcontrol web-filter SurfControl Enterprise Threat Shield
Websense	США	Web Security Suite
IIS (Cobion)	Германия	Proventia Web Filter Proventia Mail Filter

Проблемы с русскоязычным контентом

- неполнота базы данных русскоязычных ресурсов;

- систематическая погрешность категорирования сайтов, связанная с неучетом российских социально-политических реалий;

- систематическая погрешность категорирования сайтов, связанная, как правило, с полностью автоматическим определением категорий русскоязычных сайтов;

- низкая оперативность обновления.

Обзор систем контентной фильтрации

Производитель	URL	Программный продукт
Инфосистемы Джет	http://jetinfo.isib.ru	Дозор
Инфосистемы Джет	http://jetinfo.isib.ru	Дозор-Джет
Яндекс	http://www.antivir.ru/main.phtml?/spamooborona/indexspam	Самооборона

Определение VPN

Виртуальная частная сеть (Virtual Private Network) – зашифрованный инкапсулированный процесс коммуникации, который безопасным образом передает данные из одной точки в другую, безопасность этих данных обеспечена устойчивой технологией шифрования, и передаваемые данные проходят через открытую, незащищенную маршрутизируемую сеть

Идея технологии VPN

В основе технологии VPN лежит идея обеспечения безопасного взаимодействия объектов/субъектов посредством сетей общего доступа, таким образом, как если бы этот доступ осуществлялся через «собственную» частную сеть организации.

VPN обеспечивает:

- максимально возможную безопасность при взаимодействии по каналам общего доступа
- поддержку внутрикорпоративной адресации
- предсказуемую производительность

Основные функции VPN

- **Защита виртуальных каналов, проходящих через публичные сети**
- **Защита собственно информации, которая передается по виртуальному каналу.**

VPN. Преимущества.

- в большинстве случаях, VPN сети обеспечивают достаточный уровень защищенности передаваемых данных.
- позволяют существенно снизить затраты на организацию канала между филиалами организации по сравнению с другими техническими решениями.
- позволяют удаленным пользователям соединяться с центральным офисом через интернет, тем самым существенно экономить на междугородних (международных) звонках.

Главная черта технологии VPN - использование Internet в качестве магистрали для передачи корпоративного IP-трафика.

Безопасность при реализации VPN

- Предварительная идентификация и авторизация сторон
- Шифрование трафика
- Поддержка различных уровней доступа
- Удобство администрирования

Варианты использования VPN

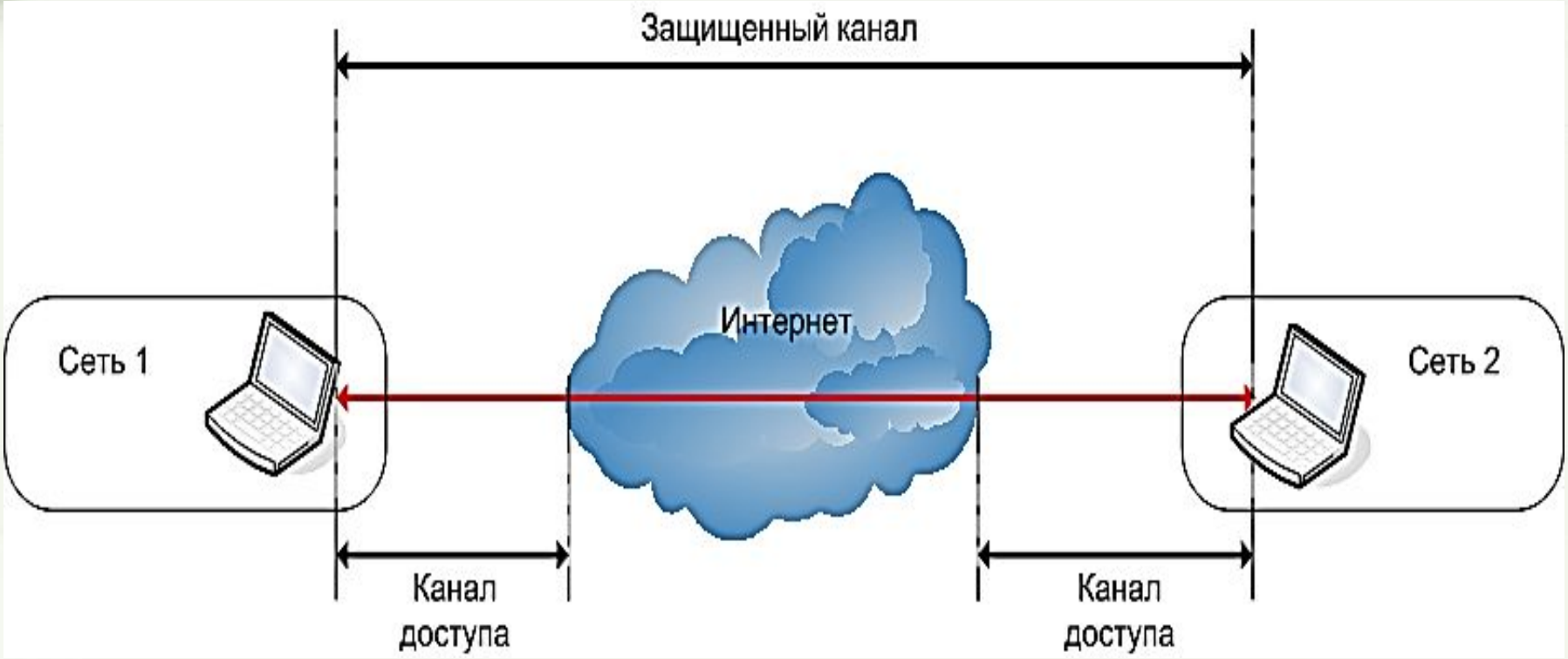
- **Intranet VPN**
  - Удаленные офисы
  - Удаленные пользователи (Remote Access VPN)
  - Узлы локальной сети (Client/Server VPN)
- **Extranet VPN**
  - Связь партнеров
  - Информационные общие ресурсы
  - Доступ пользователей к службам:
    - ✔ FTP, Telnet, E-Mail
    - ✔ Web
    - ✔ E-Commerce
    - ✔ Remote Access

Схемы построения VPN

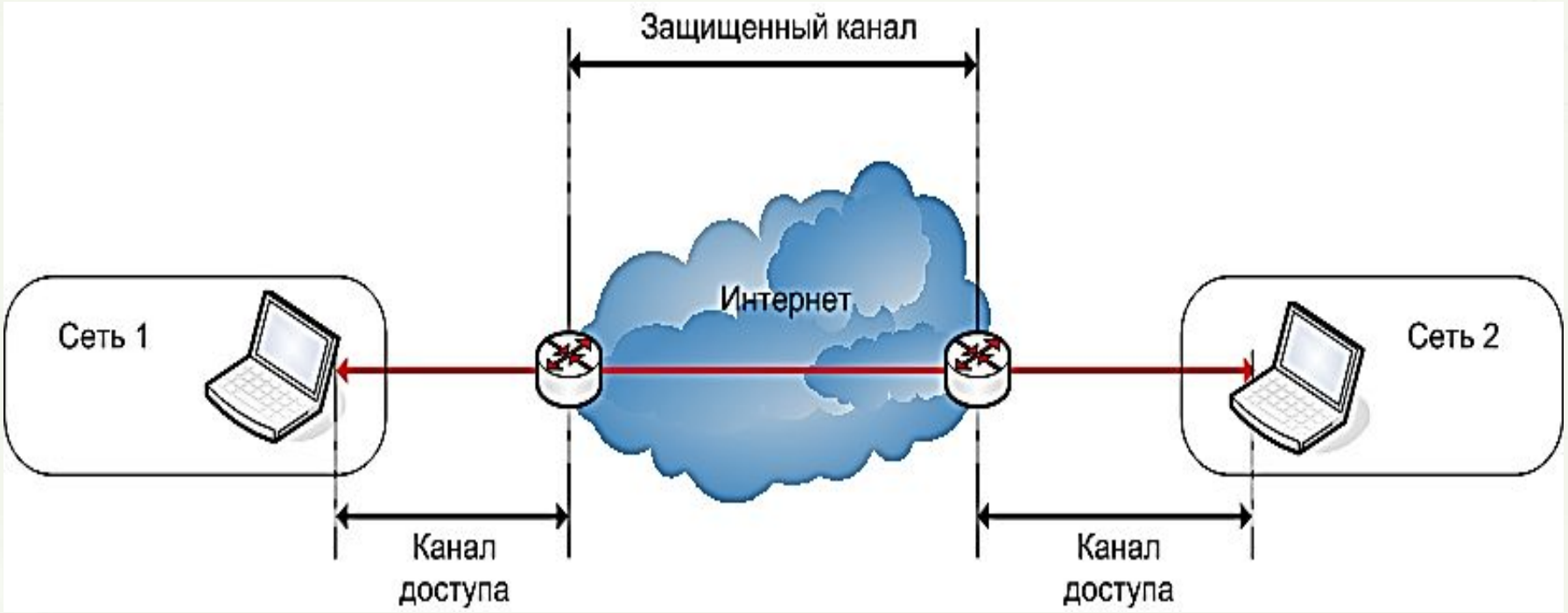
- реализация VPN владельцем (Customer Provided VPN, CPVPN)

- реализация VPN сервис-провайдером (Provider Provisioned VPN, PPVPN)

Реализация VPN владельцем



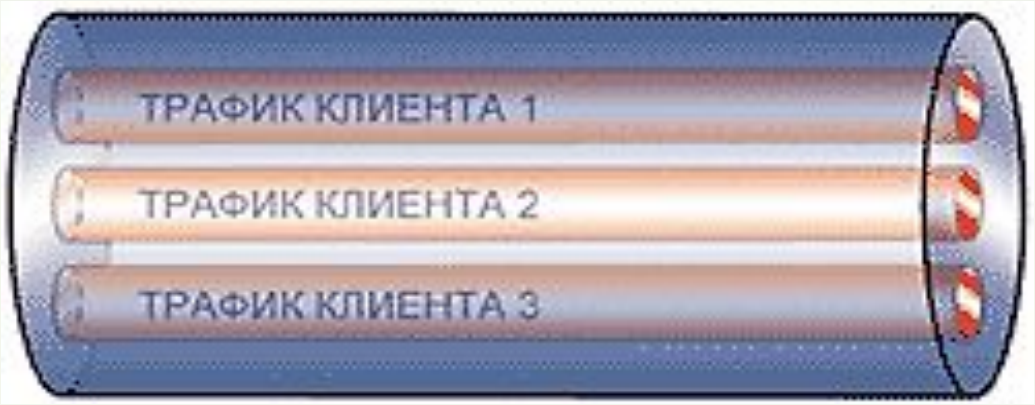
Реализация VPN сервис-провайдером



Протоколы туннелирования VPN

Туннелирование – это процесс инкапсуляции (вложения) пакета данных внутрь IP пакета.

Туннелирование – процесс создания виртуального канала или соединения, проведенное через открытую сеть.

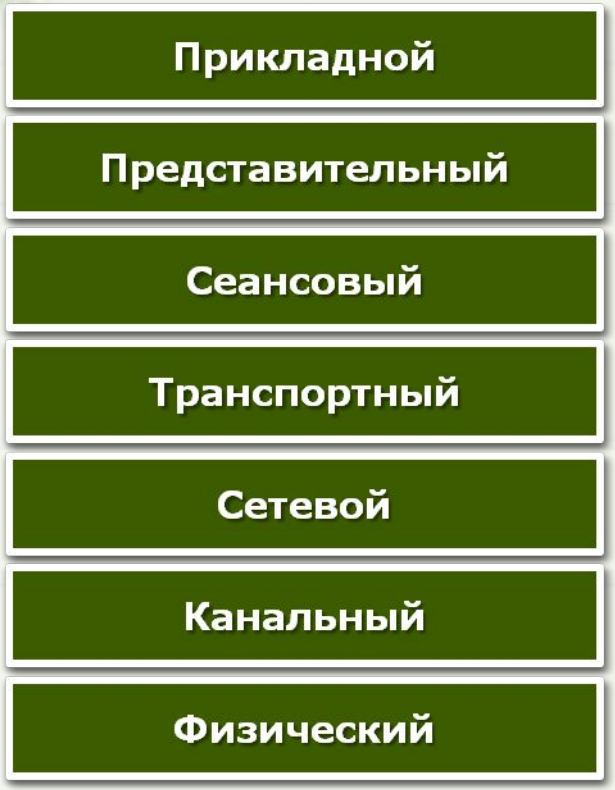


Протоколы туннелирования VPN

Туннель создается между двумя узлами сети. Сторона, которая инициирует создание туннеля называется **инициатором**, вторая сторона – **терминатор туннеля**.

Инициатор туннеля инкапсулирует (вкладывает) пакеты локальной сети (в том числе, пакеты немаршрутизируемых протоколов) в новые IP-пакеты, содержащие в своем заголовке адрес этого инициатора туннеля и адрес терминатора туннеля. На противоположном конце терминатором туннеля производится обратный процесс извлечения исходного пакета.

Протоколы туннелирования VPN



SSL

IPSec (Remote Access AND LAN-to-LAN, Strong Security)

PPTP, L2F, L2TP

Layer 2 VPN - протоколы PPTP (Point to Point Tunneling Protocol), L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunneling Protocol)

Layer 3 VPN - протокол IPSec (Internet Protocol Security)

Аутентификация

Аутентификация (authentication) - процедура проверки подлинности участников процесса обмена информации

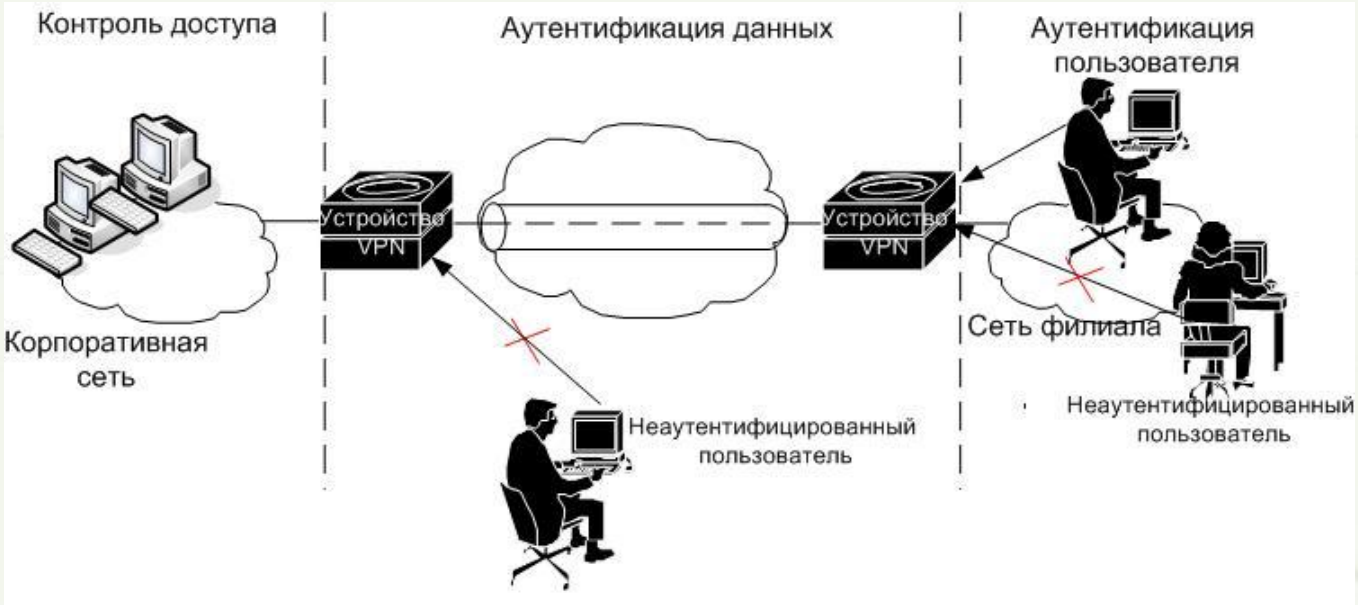
Аутентификация в VPN

- данных
- пользователей

Аутентификация

Аутентификация данных подтверждает, что сообщение было послано в целостности и в него не вносились изменения.

Аутентификация пользователя является процессом, позволяющим пользователю получить доступ к сети



! Важно, чтобы в любых вариантах технологии VPN предлагались оба типа аутентификации.

Аутентификация данных

- Протокол IPSec
- Алгоритмы хэширования (MD5,SHA1)
- Запросы сертификата PKI

Примеры построения VPN

- VPN на базе межсетевых экранов
- VPN на базе маршрутизаторов
- VPN на базе сетевой ОС
- VPN на базе аппаратных средств

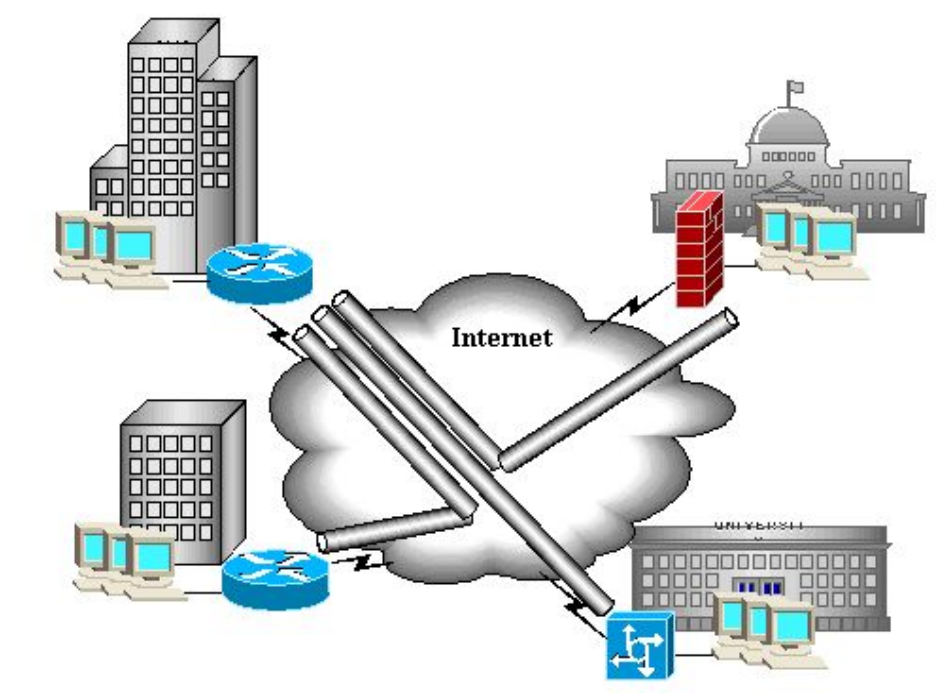
Примеры построения VPN

- **VPN на базе межсетевых экранов**

Большинство брандмауэров поддерживают туннелирование и шифрование данных. В этом случае к программному обеспечению собственно брандмауэра добавляется модуль шифрования. Недостаток метода - зависимость производительности от аппаратного обеспечения, на котором работает брандмауэр. Брандмауэры на базе ПК используются для небольших сетей с небольшим объемом передаваемой информации.

Примеры построения VPN

- **VPN на базе маршрутизаторов**



Поскольку вся информация, исходящая из локальной сети проходит через маршрутизатор, то на него возлагаются и задачи шифрования.

Примеры построения VPN

- **VPN на базе сетевой ОС**

Решения на базе сетевой ОС можно рассмотреть на примере системы Windows NT компании Microsoft. Для создания VPN Microsoft использует протокол PPTP, который интегрирован в ОС Windows NT. В работе VPN на базе Windows NT используется база пользователей, хранящаяся в Primary Domain Controller (PDC). При подключении к PPTP- серверу пользователь авторизуется по протоколам PAP, CHAP или MS-CHAP. Передаваемые пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования используется нестандартный протокол от Microsoft Point-to-Point Encryption с 40- или 128-битным ключом, получаемым в момент установки соединения. Недостатки данной системы - отсутствие проверки целостности данных и невозможность смены ключей во время соединения. Достоинства - легкость интеграции с Windows и низкая стоимость.

Примеры построения VPN

- **VPN на база аппаратных средств**

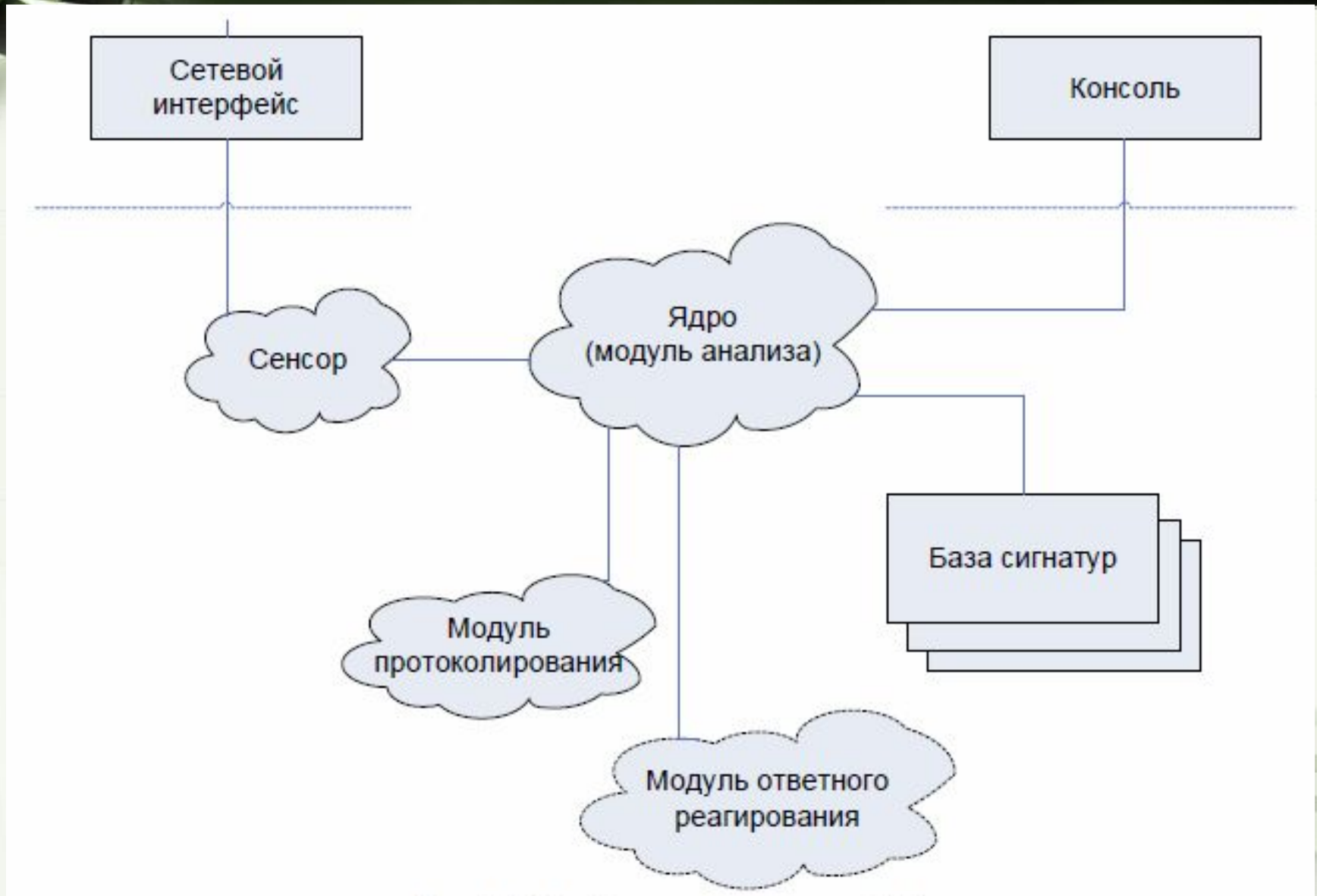
Вариант построения VPN на специальных устройствах может быть использован в сетях, требующих высокой производительности. Таким образом, при интенсивном обмене важной информацией между филиалами для построения VPN лучше использовать специализированное оборудование, однако при ограниченных средствах можно обратить внимание и на чисто программное решение. В случае, кода происходит обмен информацией в небольших объемах, оправданным является использование именно программных средств.

Системы обнаружения и предотвращения вторжений

Системы обнаружения и предотвращения вторжений – это программные или аппаратно-программные комплексы, предназначенные для анализа сетевого трафика, идентификации возможных инцидентов, блокирования вредоносного трафика, записи событий в журналы, предоставление различного рода отчетов.

- IDS – системы обнаружения вторжений
- IPS – системы предотвращения вторжений
- IDPS – системы обнаружения и предотвращения вторжений

Структурная схема IDS



Алгоритм функционирования IDS

Системы обнаружения и предотвращения вторжений

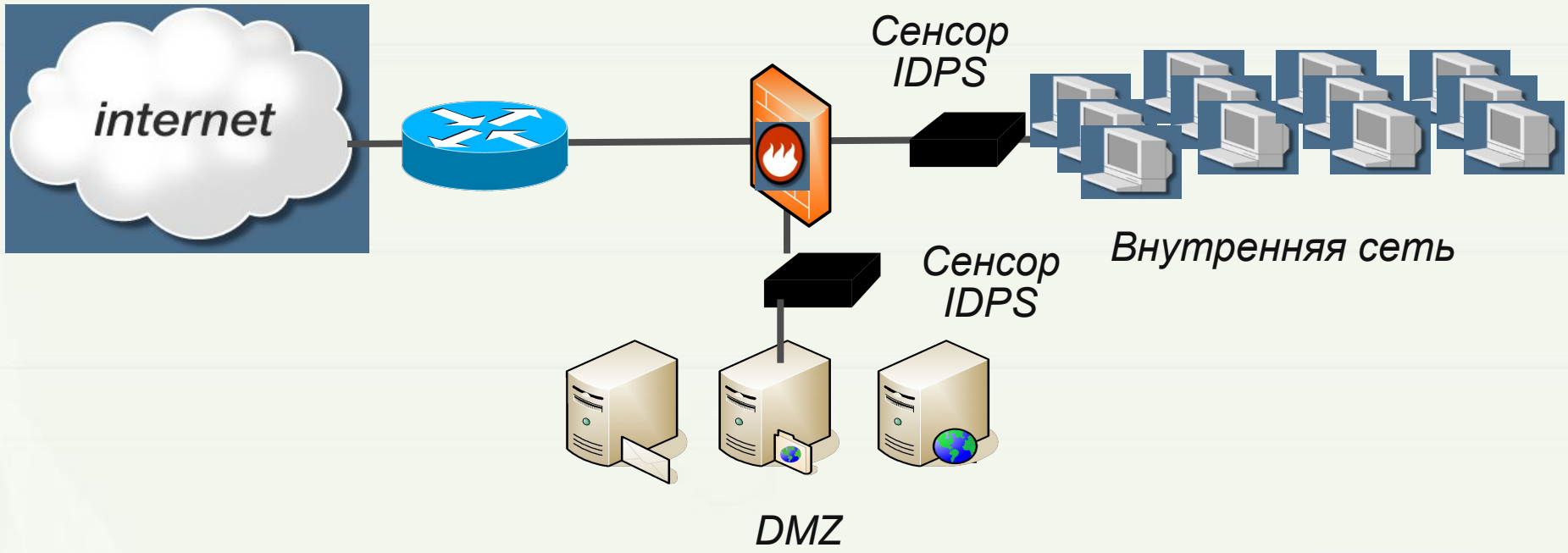
Типы IDPS:

- **Сетевые (network-based IDPS, NIDPS)**
- **Узловые (host-based IDPS, HIDPS)**

Сетевые IDPS

Сетевые IDPS собирают информацию из самой сети, как правило, посредством захвата и анализа пакетов, контролируют сетевой трафик и обнаруживают попытки злоумышленника проникнуть внутрь защищаемой системы или реализовать атаку «отказ в обслуживании». Эти IDPS предназначены для контроля более одного узла сети.

Архитектура NIDPS

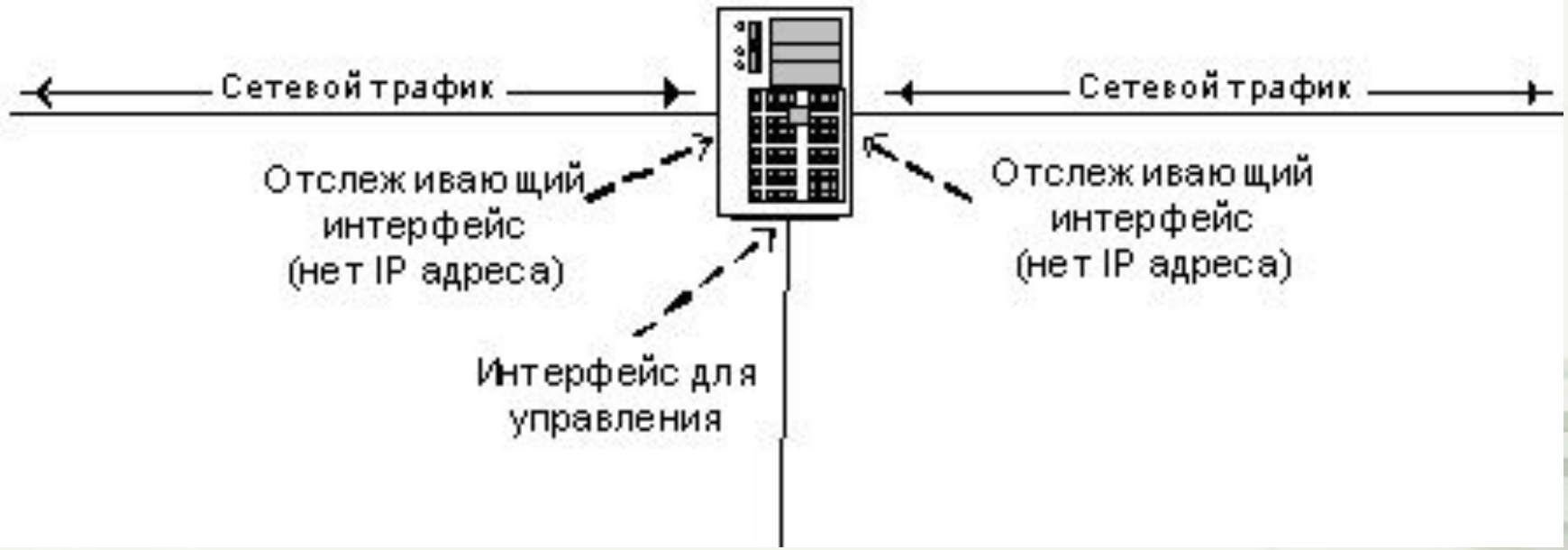


Методы размещение сенсоров

Метод подключения в разрыв сети обеспечивает полный контроль всего трафика, проходящего через контролируемую точку.

Линейный режим (In-line mode)

Недостатки: Единая точка отказа. Задержки при прохождения трафика через устройство.

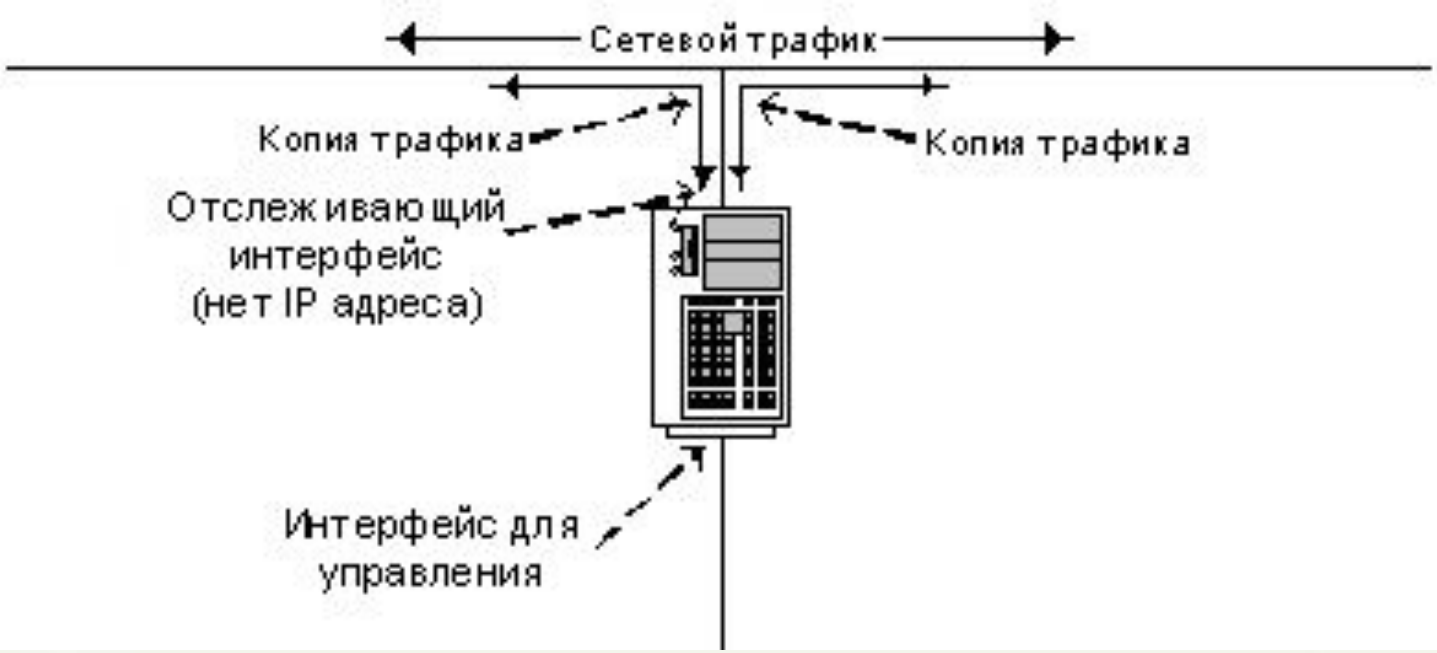


Методы размещение сенсоров

Метод перенаправления предполагает установку сенсора (или нескольких сенсоров) для поиска подозрительного трафика в потоке данных. Проверяемый поток направляется на сенсор с зеркальных портов коммутатора или дублируется другими доступными средствами.

Пассивный режим (passive operation)

Недостатки: Жесткие требования к сопряженному оборудованию. Возможен пропуск атак одиночными пакетами.

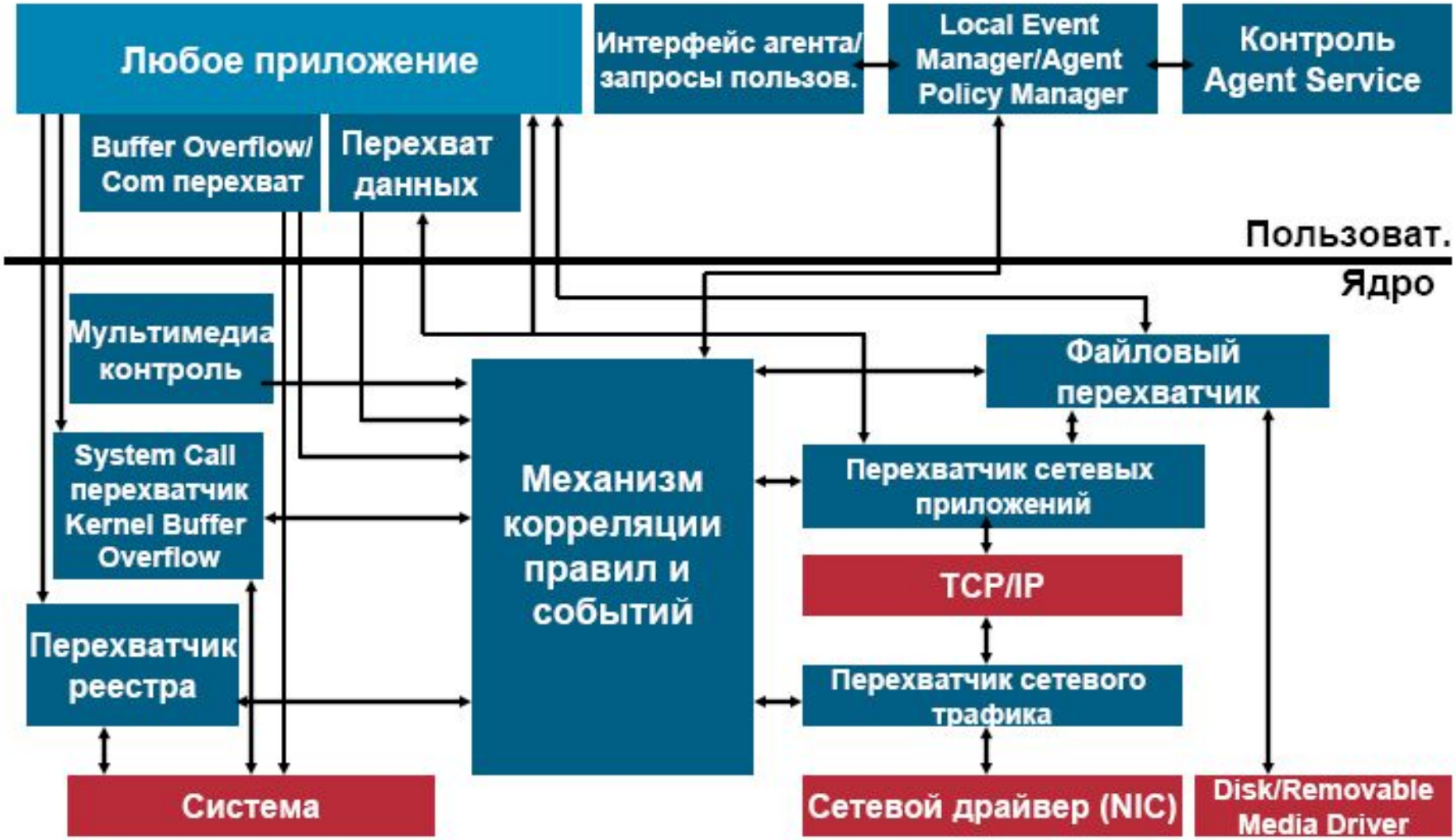


Узловые IDPS

Узловые IDPS устанавливаются на узле, который они будут отслеживать. Узлом может быть сервер, рабочая станция или любое другое сетевое устройство.

HIDPS устанавливает службу или демон, или изменяет ядро операционной системы для получения полномочий первичной проверки. HIDPS прослушивают сетевой трафик отслеживаемого узла, перехватывают потенциально вредоносные действия. HIDPS проверяют целостность файловой системы, анализируют лог-файлы, активность ОС и приложений.

Архитектура HIDPS



Совместное использование сетевых и узловых IDPS

Узловые	Сетевые	Совместное
▪ Защита от локальных атак ▪ Контроль зашифрованных данных ▪ Удаленные устройства ▪ Контроль поведения	▪ Защита ВСЕХ устройств ▪ Ближе к злоумышленнику ▪ Защита от сетевых атак (java) ▪ Защита от DDoS и распространения червей ▪ Поиск аномалий	▪ Обмен информацией (карантин, информация об ОС) ▪ Полная картина в системах корреляции ▪ Эшелонированная защита

IDPS обеспечивают:

Распознавание проникновения в сеть

Генерацию предупреждающих сообщений

Автоматизацию ответных действий

100 % гарантию безопасности не дает!!!

Сканеры безопасности

Сканеры безопасности — это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых узлов, позволяющее сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

Сканеры безопасности

Сканирование ("логический вывод" (inference)) - механизм пассивного анализа, с помощью которого сканер пытается определить наличие уязвимости без фактического подтверждения ее наличия - по косвенным признакам.

Процесс идентифицирует открытые порты, найденные на каждом сетевом устройстве, и собирает связанные с портами заголовки (banner), найденные при сканировании каждого порта. Каждый полученный заголовок сравнивается с таблицей правил определения сетевых устройств, операционных систем и потенциальных уязвимостей. На основе проведенного сравнения делается вывод о наличии или отсутствии уязвимости.

Сканеры безопасности

Зондирование ("подтверждение" (verification)) - механизм активного анализа, который позволяет убедиться, присутствует или нет на анализируемом узле уязвимость. Зондирование выполняется путем имитации атаки, использующей проверяемую уязвимость.

Процесс использует информацию, полученную в процессе сканирования ("логического вывода"), для детального анализа каждого сетевого устройства. Этот процесс также использует известные методы реализации атак для того, чтобы полностью подтвердить предполагаемые уязвимости и обнаружить другие уязвимости, которые не могут быть обнаружены пассивными методами, например подверженность атакам типа "отказ в обслуживании" ("denial of service").

Сканеры безопасности

Сканеры безопасности можно **классифицировать**:

1. Сканеры портов
2. Сканеры, исследующие топологию компьютерной сети
3. Сканеры, исследующие уязвимости сетевых сервисов
4. CGI-сканеры (специализированные - помогают найти уязвимые скрипты)

Сканеры безопасности

К первым трем категориям можно отнести:

Nmap 5
http://www.nmap.org

Nessus 4
http://www.nessus.org/download

Maxpatrol 8
http://www.ptsecurity.ru/maxpatrol.asp

Internet scanner 7
http://www-935.ibm.com/services/us/index.wss/offering/iss/a1027208

Retinanetwork security scanner 5
http://www.eeye.com/html/products/retina/index.html

Shadow security scanner (sss) 7
http://www.safety-lab.com/en/products/securityscanner.htm

Netclarity auditor 6
http://netclarity.com/branch-nacwall.html

Xspider 7
http://www.ptsecurity.ru/xs7.asp

Сканеры безопасности

Специализированный CGI-сканер

- программа для сканирования адреса (или диапазона адресов)
на наличие уязвимых скриптов и соответственно вывода отчёта о наличии (или отсутствии) таких скриптов на сервере.

Принцип работы всех cgi-сканеров одинаков и весьма прост.
Сканер берёт относительный путь к уязвимому скрипту из своей базы и ищет его на сервере.
В общем случае сканер просто посылает следующий запрос на сервер:

GET адрес_хоста/путь_к_скрипту_из_базы HTTP/1.0\n\n

Если документ найден т.е. ответ сервера '200' то предполагается,
что скрипт есть на сервере и выводится сообщение о найденом скрипте.

Так сканер проходится по всей базе и всему диапазону адресов.
Как видите всё просто. Написать такой сканер дело 10 минут.

Cgi-сканеры

Nikto2
http://www.cirt.net/nikto2
DCS 2.1
http://www.gin-group.org/win-files/dcs21.exe
VoidEye
http://void.ru/toolz/voideye/voideye.zip
TwwwScan
http://hacksoft.ru/cgi-bin/ssi_counter.cgi?Message=AAAAD&file=scancgi
UKR Cgi Scanner
http://www.ukrteam.lgg.ru/files/cgi.tar

Спасибо за внимание!