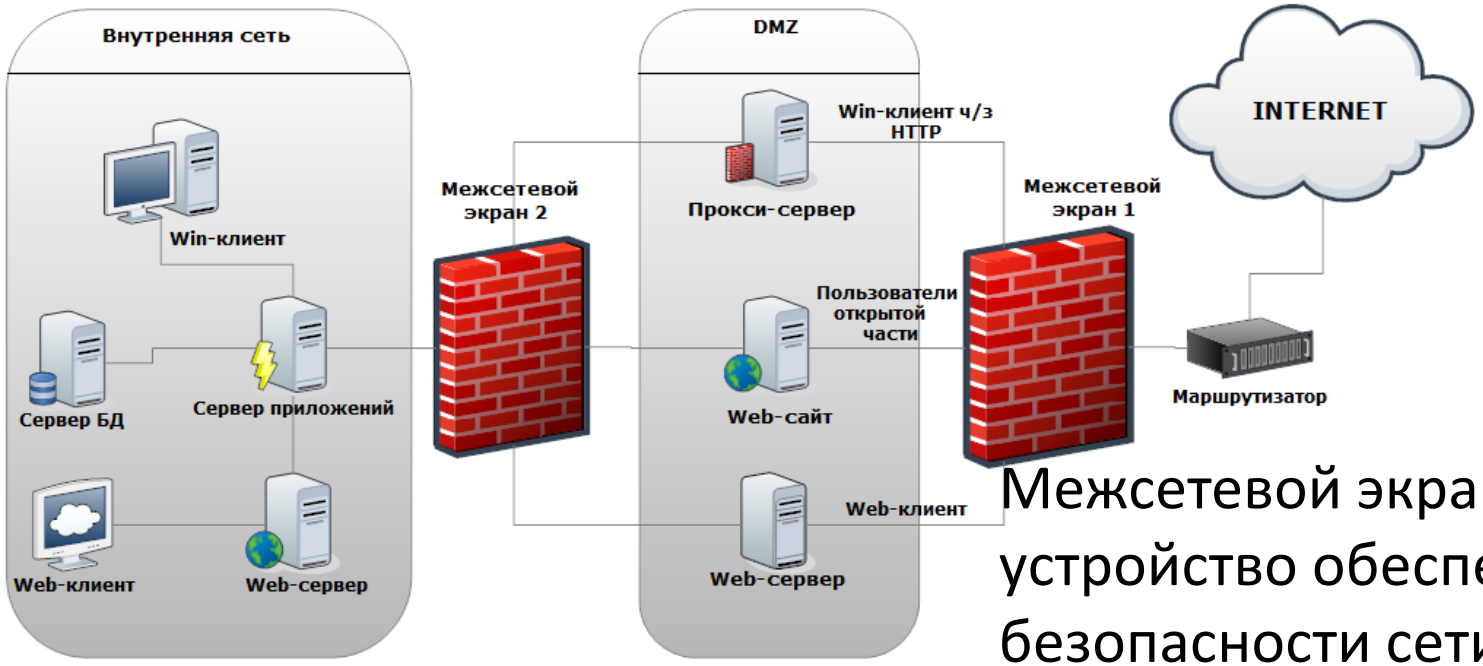
Направление подготовки бакалавров
090301 «Информатика и вычислительная техника»

Информационная безопасность. Межсетевой экран

Караваева Ольга Владимировна

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Межсетевой экран

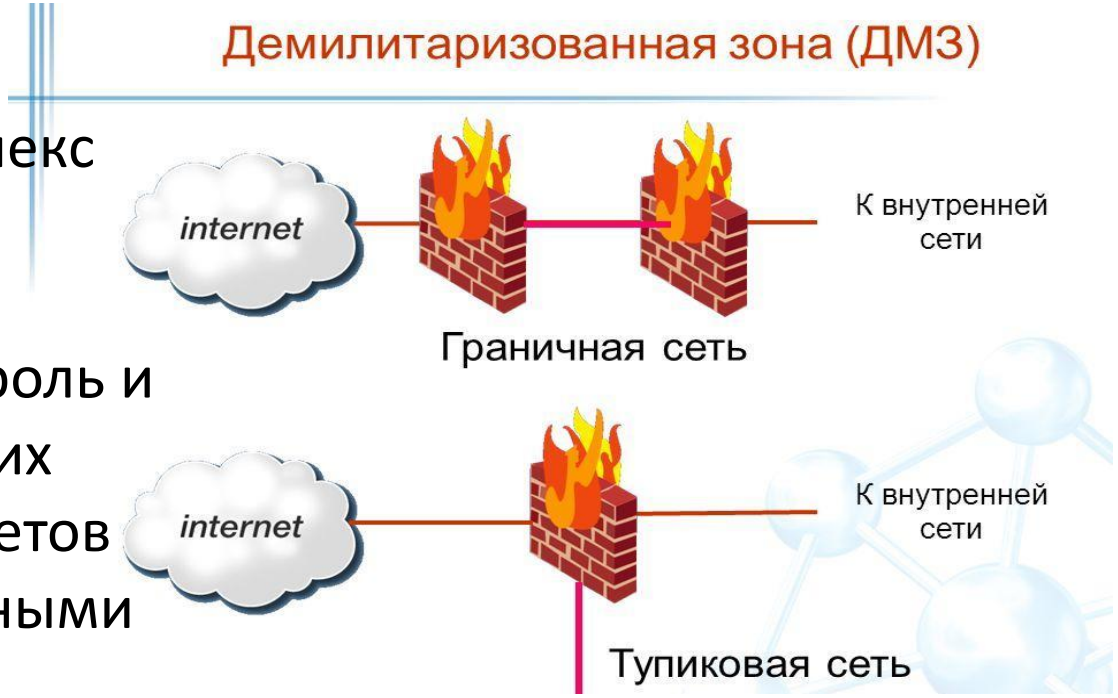


Межсетевой экран (МСЭ) — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Межсетевой экран

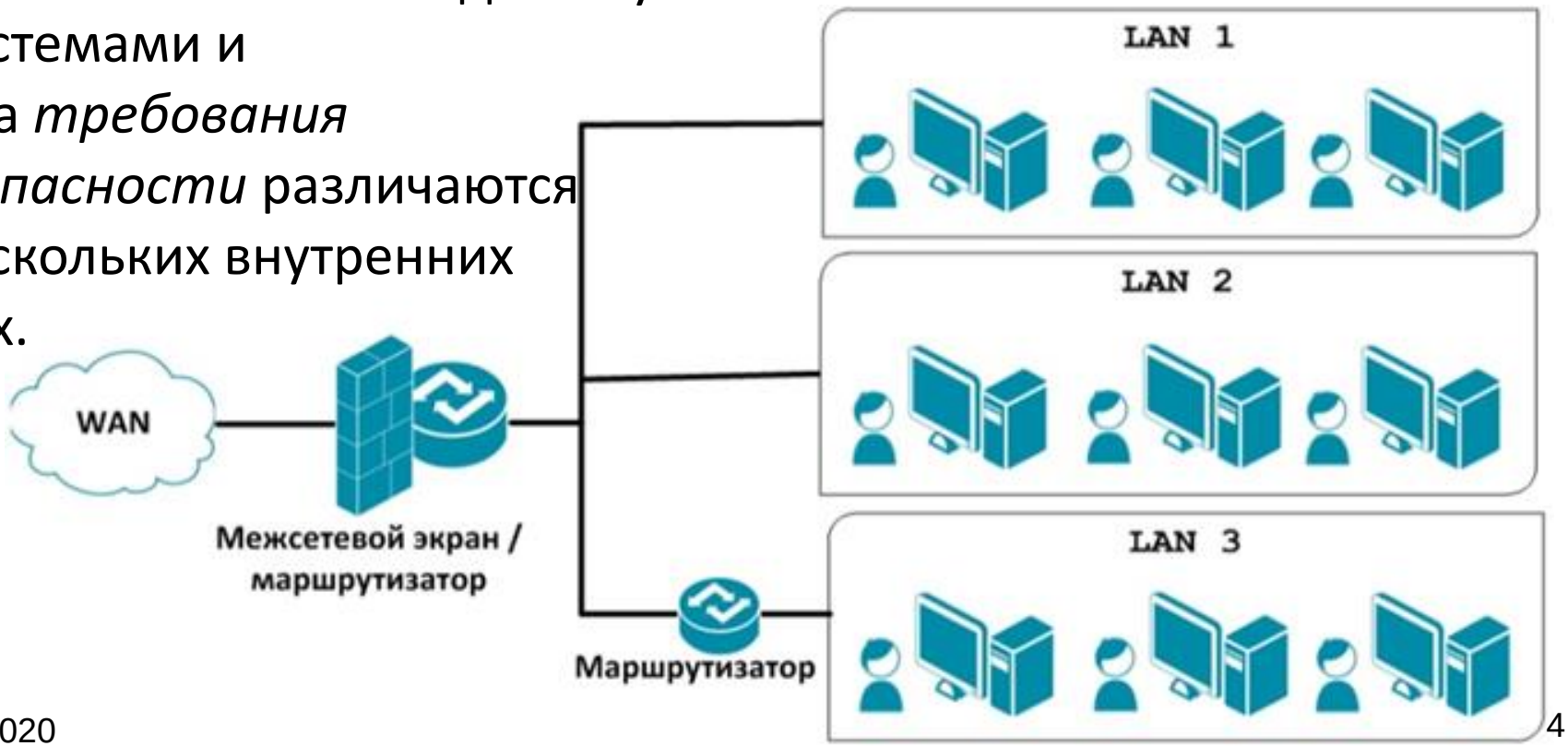
Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

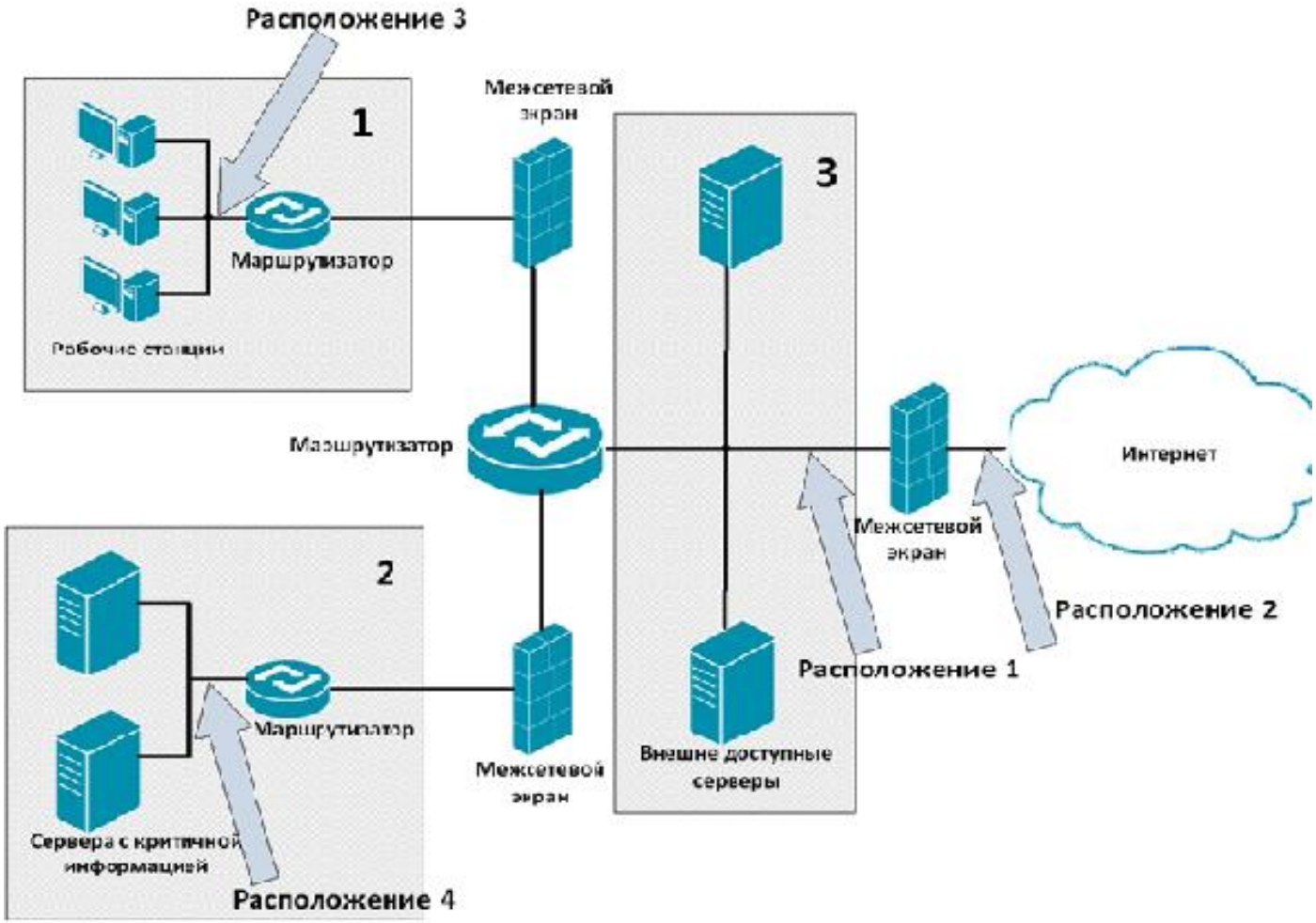
Межсетевой экран

Межсетевые экраны используются для разграничения сетей, имеющих различные требования к безопасности. Межсетевые экраны следует использовать каждый раз, когда внутренние сети и системы взаимодействуют с внешними сетями и системами и когда *требования безопасности* различаются в нескольких внутренних сетях.



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

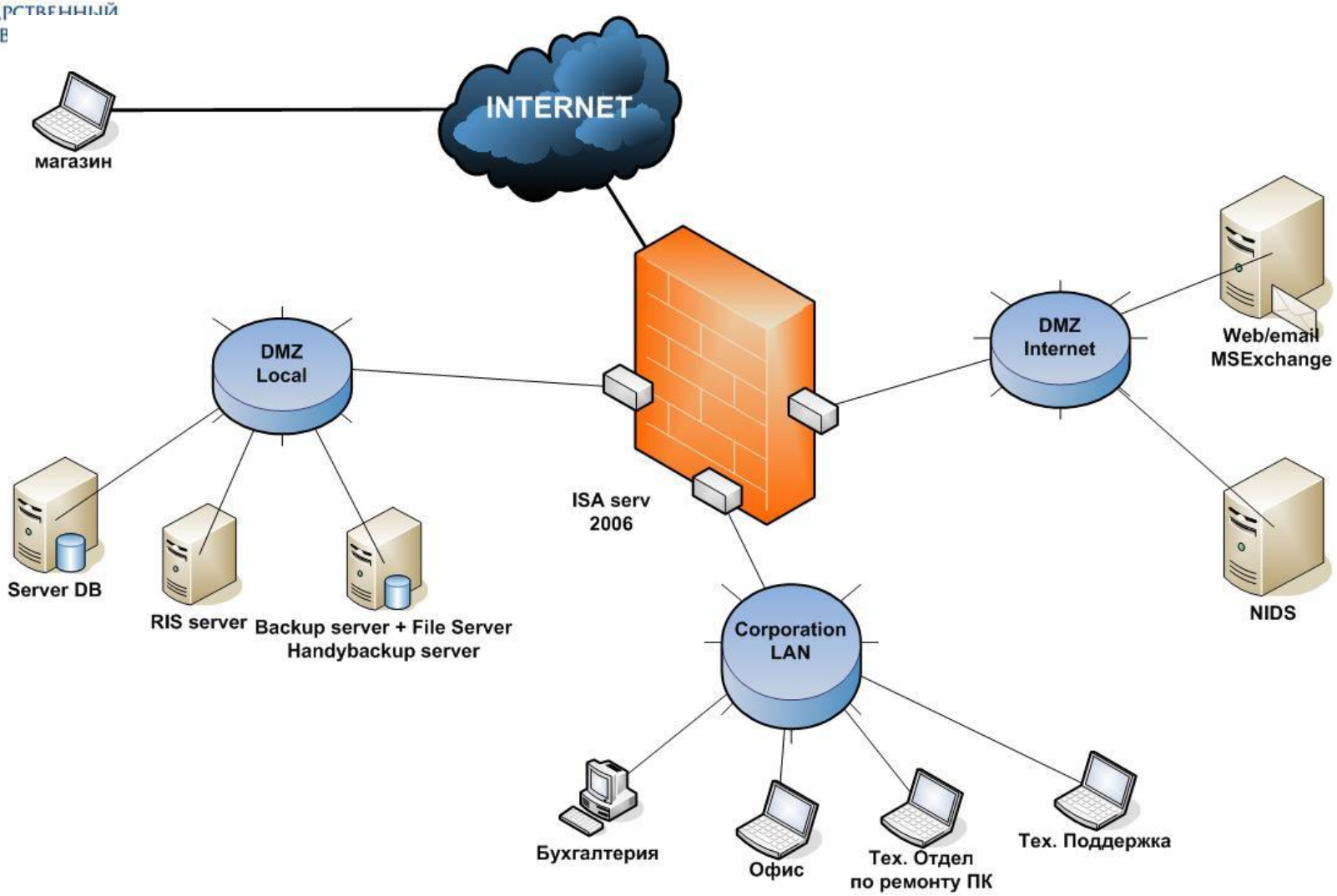
Межсетевой экран



1. Основная подсеть.
2. Подсеть с критичными ресурсами и дополнительными точками доступа
3. DMZ-сеть.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВ

Межсетевой экран

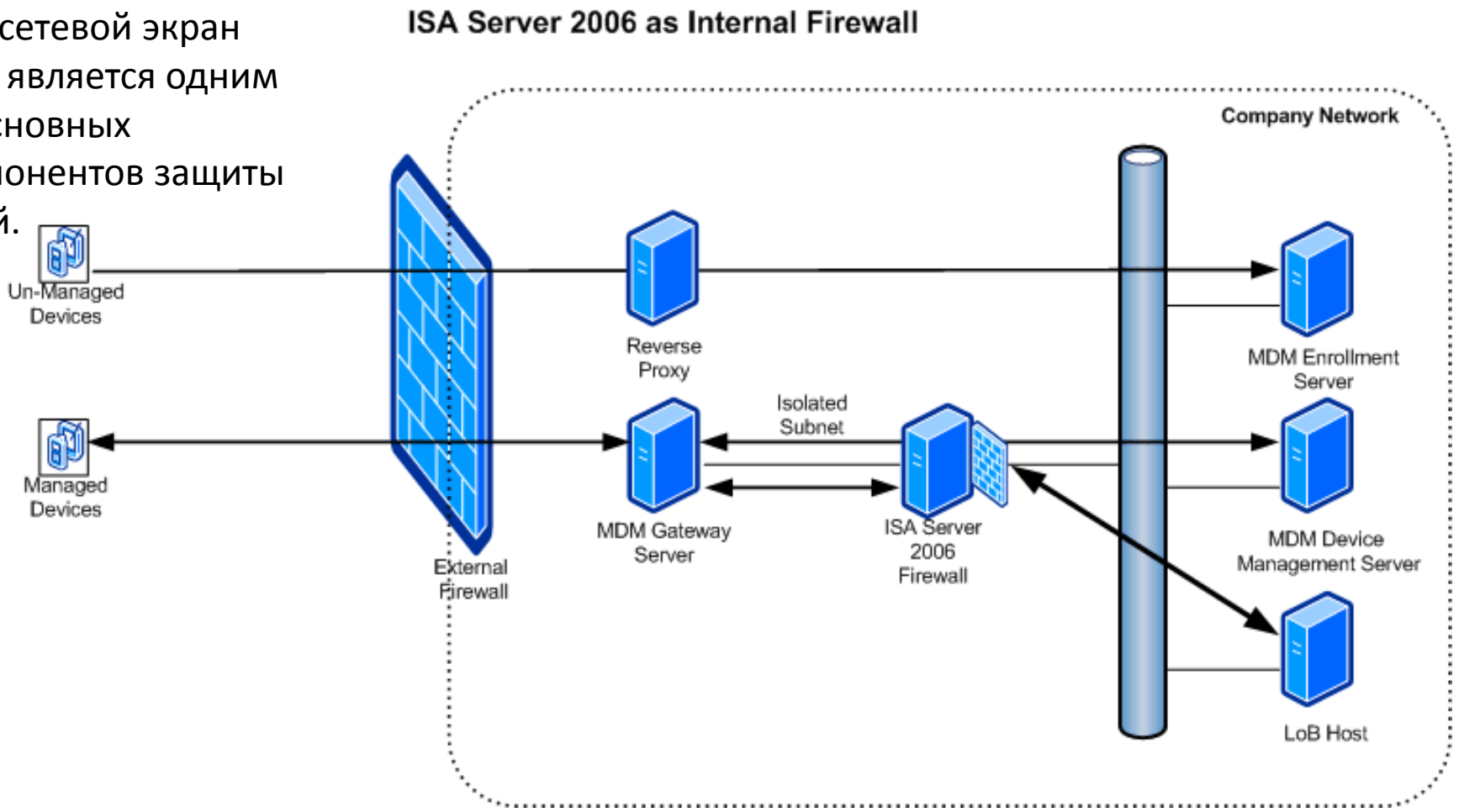


Microsoft **Internet Security** and **Acceleration** Server (**ISA** Server) — прокси-**сервер** для защиты сети от атак извне, а также контроля интернет-трафика.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Межсетевой экран

Межсетевой экран (МЭ) является одним из основных компонентов защиты сетей.



Mobile Device Manager **MDM Gateway Server** – шлюз, позволяющий обеспечить безопасное подключение к корпоративной сети

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

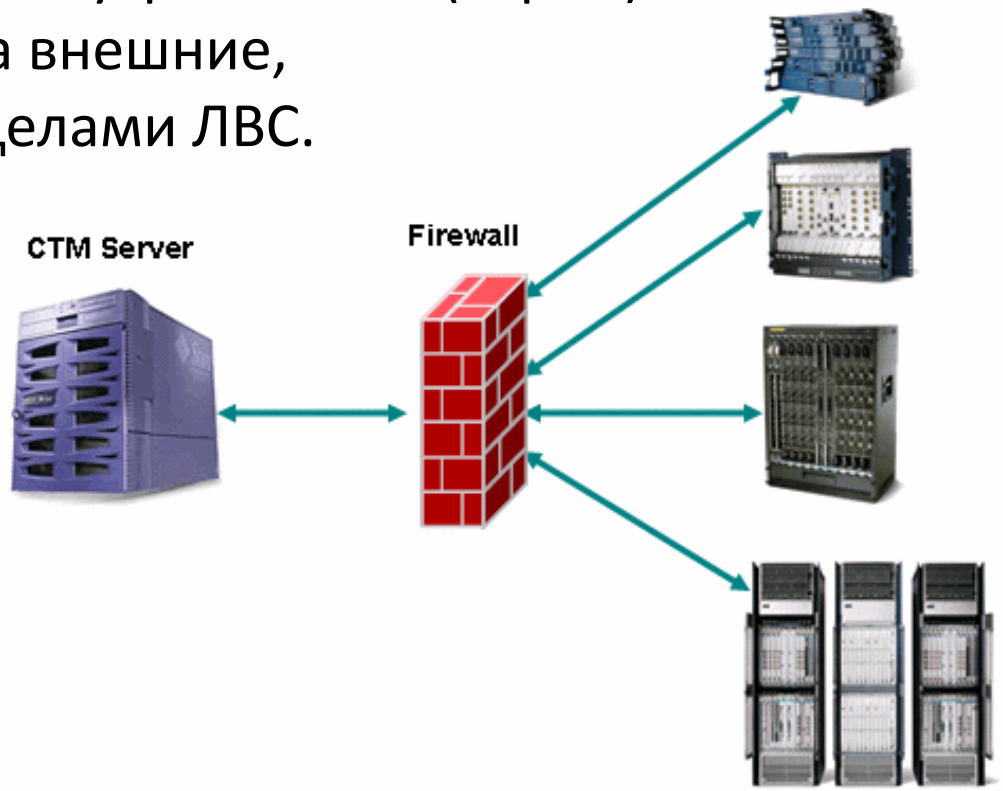
Межсетевой экран

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Межсетевой экран

Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов — динамическую замену внутрисетевых (серых) адресов или портов на внешние, используемые за пределами ЛВС.



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Классификация межсетевых экранов

1) В зависимости от охвата контролируемых потоков данных
   - Традиционный
   - персональный
2) В зависимости от отслеживания активных соединений
   - Stateless (простая фильтрация)
   - Stateful (фильтрация с учетом контекста)

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Классификация межсетевых экранов

3) В зависимости от уровня модели OSI, на котором происходит контроль доступа
   - Работающие на сетевом уровне
   - Работающие на сеансовом уровне
   - Работающие на уровне приложений

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Как работает межсетевой экран

- Фильтрация трафика происходит на основе заранее установленных правил безопасности. Для этого создается специальная таблица, куда заносится описание допустимых и недопустимым к передаче данных. Межсетевой экран не пропускает трафик, если одно из запрещающих правил из таблицы срабатывает.
- Файрволы могут запрещать или разрешать доступ, основываясь на разных параметрах: IP-адресах, доменных именах, протоколах и номерах портов, а также комбинировать их.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Как работает межсетевой экран

- IP-адреса. Каждое устройство, использующее протокол IP, обладает уникальным адресом. Вы можете задать определенный адрес или диапазон, чтобы пресечь попытки получения пакетов. Или наоборот — дать доступ только определенному кругу IP-адресов.
- Порты. Это точки, которые дают приложениям доступ к инфраструктуре сети. К примеру, протокол ftp пользуется портом 21, а порт 80 предназначен для приложений, используемых для просмотра сайтов. Таким образом, мы получаем возможность воспрепятствовать доступу к определенным приложениям и сервисам.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Как работает межсетевой экран

- Доменное имя. Адрес ресурса в интернете также является параметром для фильтрации. Можно запретить пропускать трафик с одного или нескольких сайтов. Пользователь будет огражден от неприемлемого контента, а сеть от пагубного воздействия.
- Протокол. Файрвол настраивается так, чтобы пропускать трафик одного протокола или блокировать доступ к одному из них. Тип протокола указывает на набор параметров защиты и задачу, которую выполняет используемое им приложение.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Недостатки межсетевых экранов

- Межсетевые экраны обороняют сеть от злоумышленников. Однако необходимо серьезно отнестись к их настройке. Будьте внимательны: ошибившись при настройке параметров доступа, вы нанесете вред и файрвол будет останавливать нужный и ненужный трафик, а сеть станет неработоспособной.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Недостатки межсетевых экранов

- Применение межсетевого экрана может стать причиной падения производительности сети. Помните, что они перехватывают весь входящий трафик для проверки. При крупных размерах сети чрезмерное стремление обеспечить безопасность и введение большего числа правил приведет к тому, что сеть станет работать медленно.
- Зачастую одного файрвола недостаточно, чтобы полностью обезопасить сеть от внешних угроз. Поэтому его применяют вместе с другими программами, такими как антивирус.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Классификация угроз

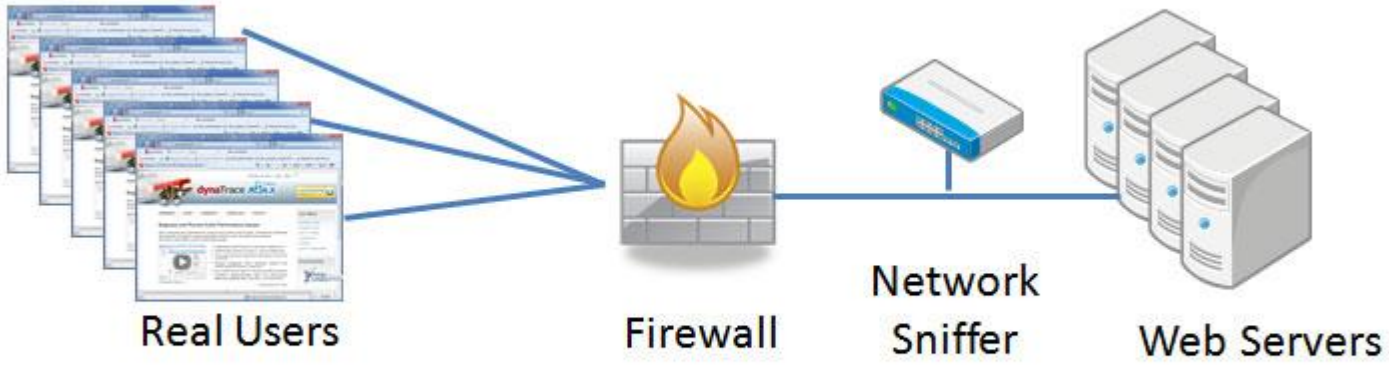
Угрозы, реализуемые по сети, классифицируются по следующим основным признакам:

- характер угрозы.
- цель реализации угрозы (соответственно, конфиденциальность, доступность, целостность информации).
- условие начала атаки.
- наличие обратной связи с атакуемым объектом.
- расположение нарушителя относительно атакуемой информационной системы.
- уровень эталонной модели ISO/OSI, на котором реализуется угроза.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Атаки в сетях на основе стека протоколов TCP/IP.

- **Анализ сетевого трафика.** Данная атака реализуется с помощью специальной программы, называемой sniffer.



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Защита от sniffer’ов

- Сильная аутентификация, например, использование одноразовых паролей
- Анти-снифферы – аппаратные или программные средства, способные выявить работу сниффера в сегменте сети.
- Коммутируемая инфраструктура.
- Криптографические методы.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Сканирование сети

Целью сканирования сети является выявление работающих в сети служб, открытых портов, активных сетевых сервисов, используемых протоколов и т.п., то есть сбор информации о сети.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Сканирование сети

Для сканирования сети чаще всего используются:

- запросы DNS – помогают выяснить злоумышленнику владельца домена, адресную область,
- эхо-тестирование – выявляет работающие хосты на основе DNS-адресов, полученных ранее;
- сканирование портов – составляется полный перечень услуг, поддерживаемых этими хостами, открытые порты, приложения и т.п.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Выявление пароля

Основной целью данной атаки является получение несанкционированного доступа к защищаемым ресурсам путем преодоления парольной защиты. Чтобы получить пароль, злоумышленник может использовать множество способов – простой перебор, перебор по словарю, сниффинг и др.

Подобного рода атак можно избежать, если использовать одноразовые пароли, о которых мы говорили ранее, или криптографическую аутентификацию.

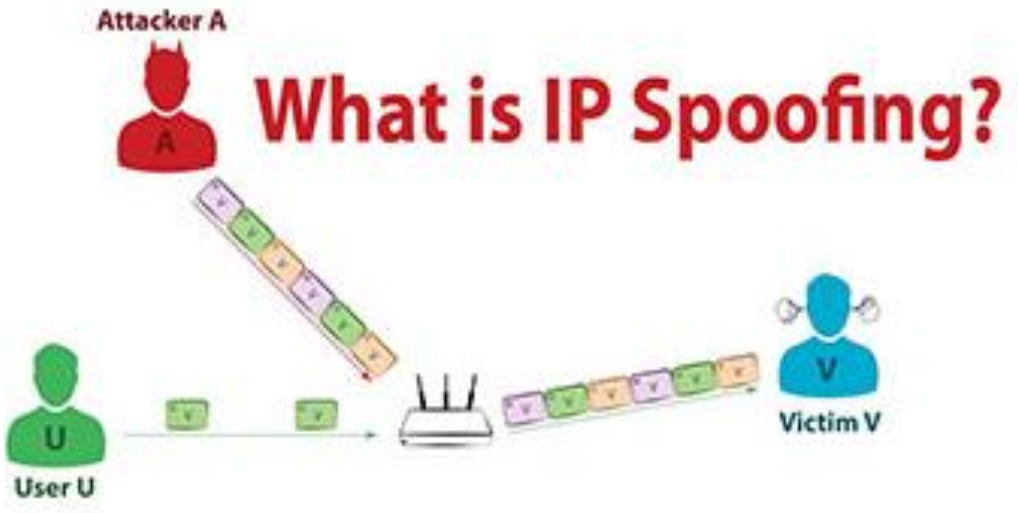
ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

IP-spoofing или подмена доверенного объекта сети.

IP-spoofing или подмена доверенного объекта сети.

Под доверенным в данном случае понимается объект сети (компьютер, маршрутизатор, межсетевой экран и т.п.), легально подключенный к серверу.

Угрозы заключается в том, что злоумышленник выдает себя за доверенный объект сети.



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

IP-spoofing или подмена доверенного объекта сети.

Спуфинг - это подделка исходящего IP-адреса. Спуффинг может быть использован злоумышленником для обхода настроек межсетевых экранов, а также для организации DoS-атак по отношению к третьим лицам.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

IP-spoofing или подмена доверенного объекта сети.

Фишинг - один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт. В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

IP-spoofing или подмена доверенного объекта сети.

Это можно сделать двумя способами:

- воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов,
- или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам.

Атаки данного типа часто являются отправной точкой для прочих атак

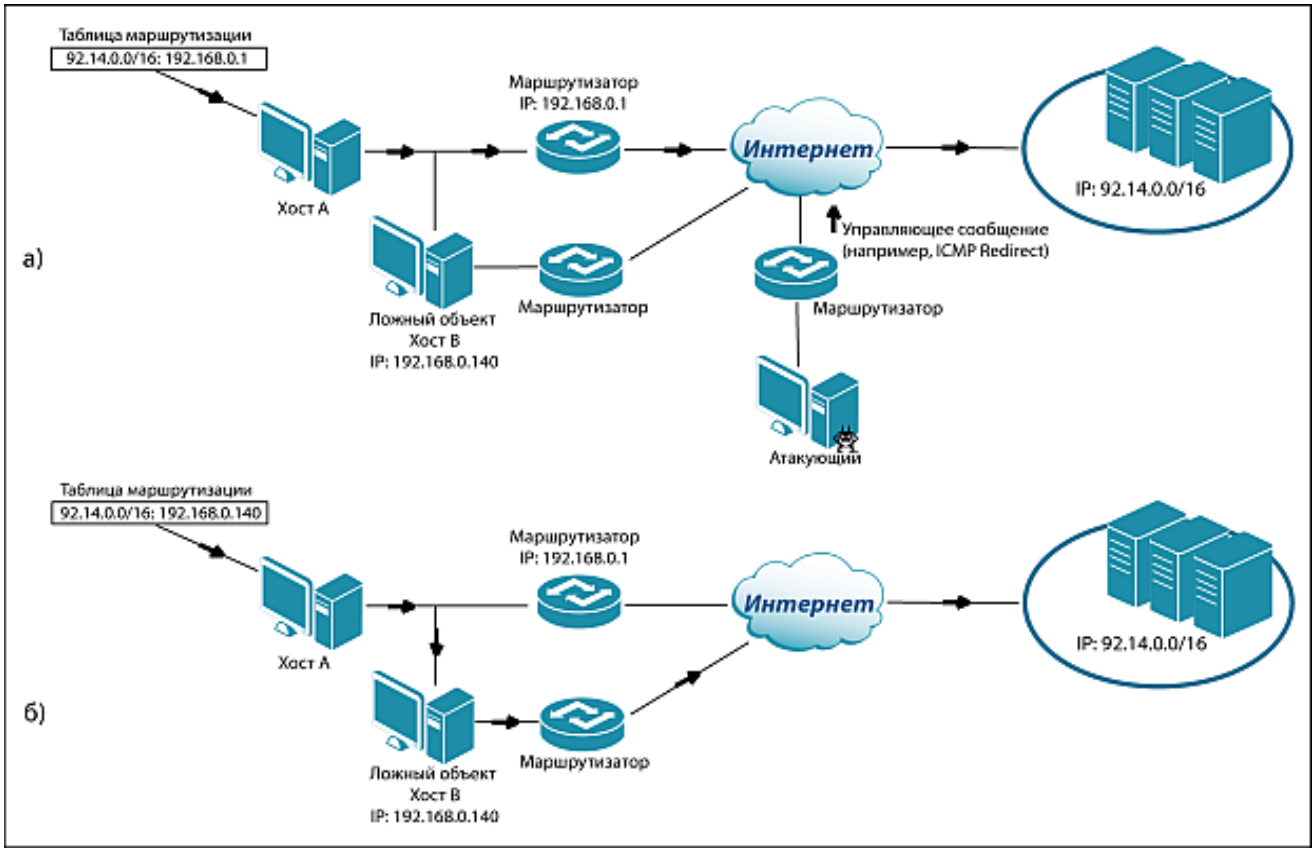
ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

IP-spoofing или подмена доверенного объекта сети.

IP-spoofing или подмена доверенного объекта сети.

Под доверенным в данном случае понимается объект сети (компьютер, маршрутизатор, межсетевой экран и т.п.), легально подключенный к серверу.

Угрозы заключается в том, что злоумышленник выдает себя за доверенный объект сети.



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

IP-spoofing или подмена доверенного объекта сети.

Антиспуфинг – это фильтр для защиты от спама, который блокирует сообщения, отправленные с одного из локальных доменов, но с неавторизованного IP-адреса

Для ослабления угрозы (но не ее ликвидации) можно использовать следующее:

- контроль доступа.
- Фильтрация RFC 2827
- Внедрение дополнительных методов аутентификации.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Для ослабления угрозы можно воспользоваться следующим:

Функции анти-спуфинга - правильная конфигурация функций анти-спуфинга на маршрутизаторах и межсетевых экранах поможет снизить риск DoS.

Функции анти-DoS

Ограничение объема трафика (traffic rate limiting)

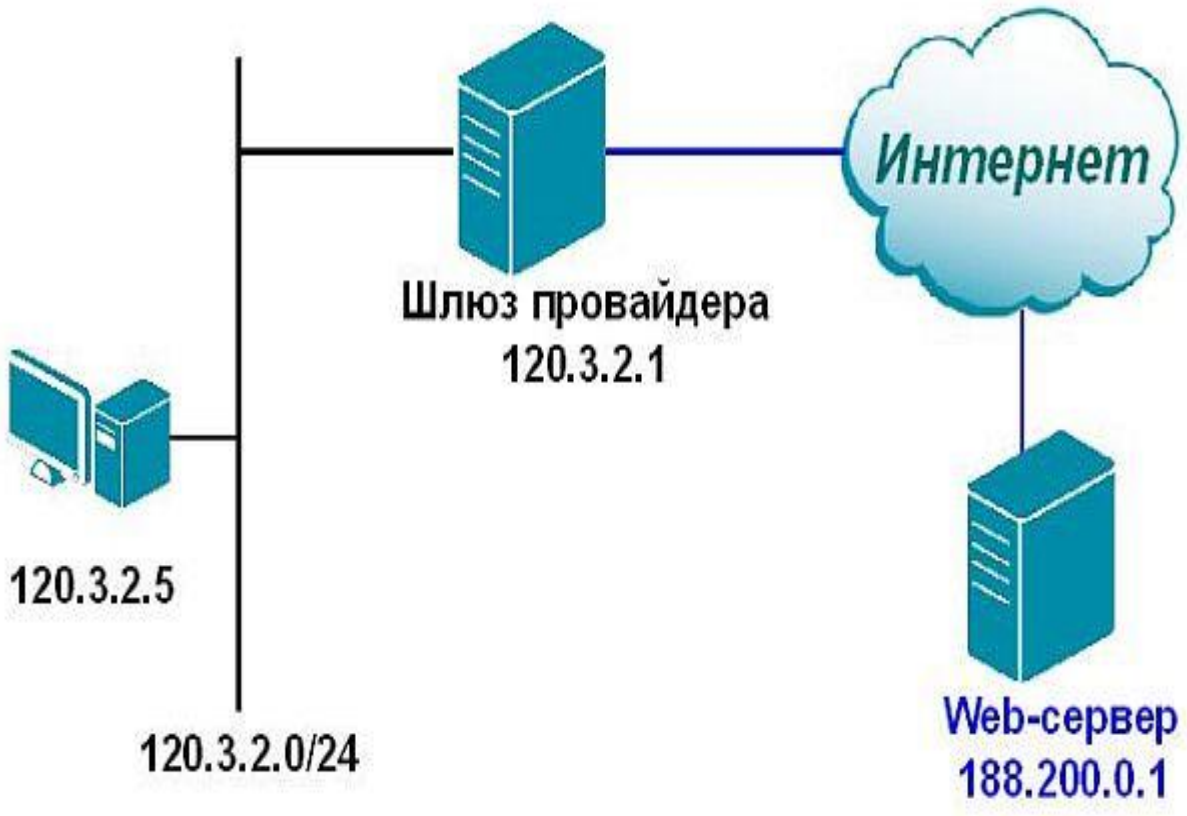
ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Технологии маскировки реальных адресов ЛС

- *NAT* (*Network Address Translation* – преобразование сетевых адресов) – это механизм в сетях *TCP/IP*, позволяющий преобразовывать IP-адреса транзитных пакетов. Механизм *NAT* описан в *RFC* 1631, *RFC* 3022.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Подключение одного компьютера с доступом в Интернет

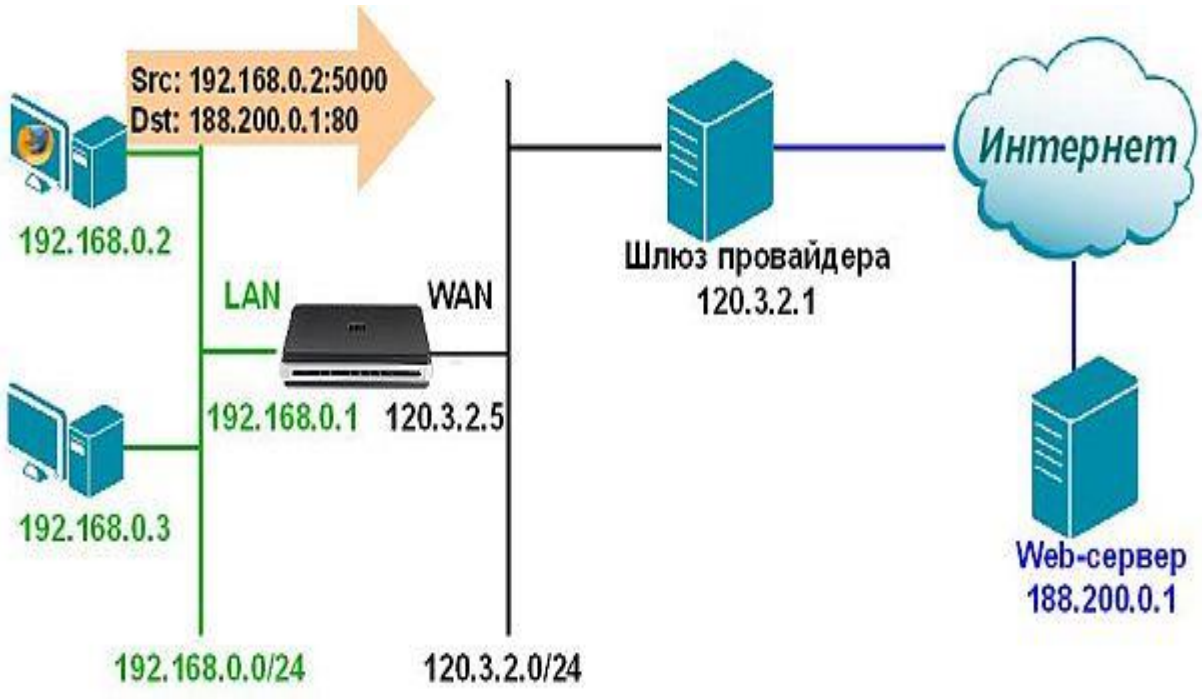


ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Объединение компьютеров в ЛС с доступом в Интернет

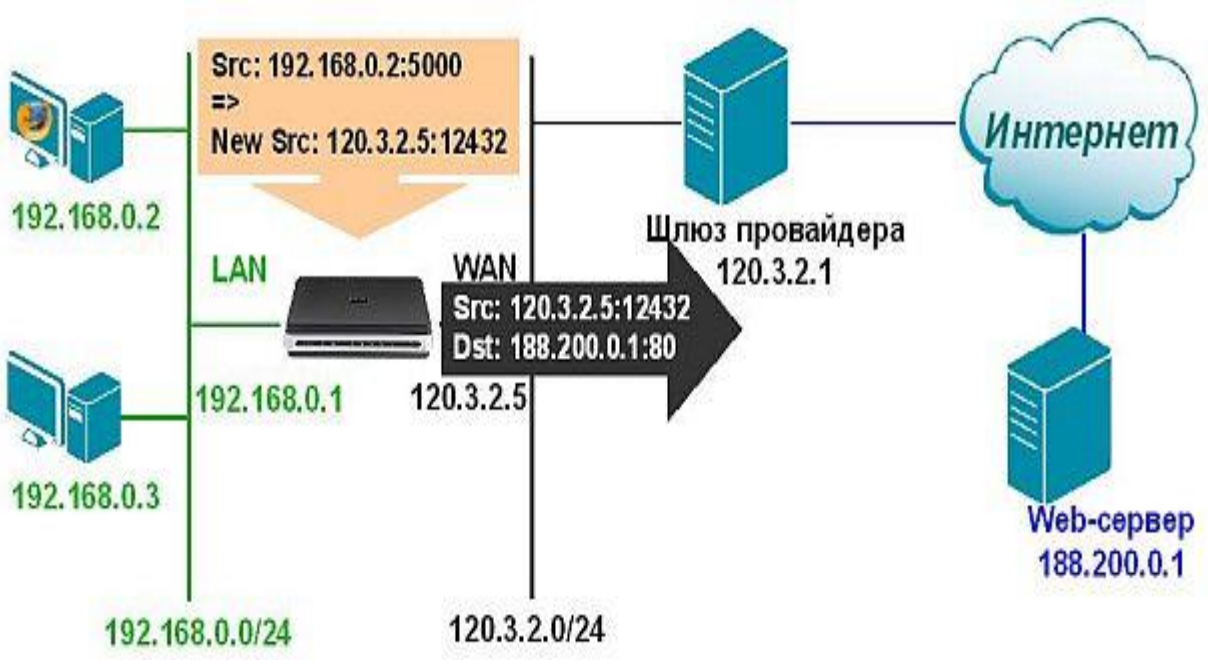
ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Запись в таблице соединений



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Преобразование адресов при использовании функции NAT

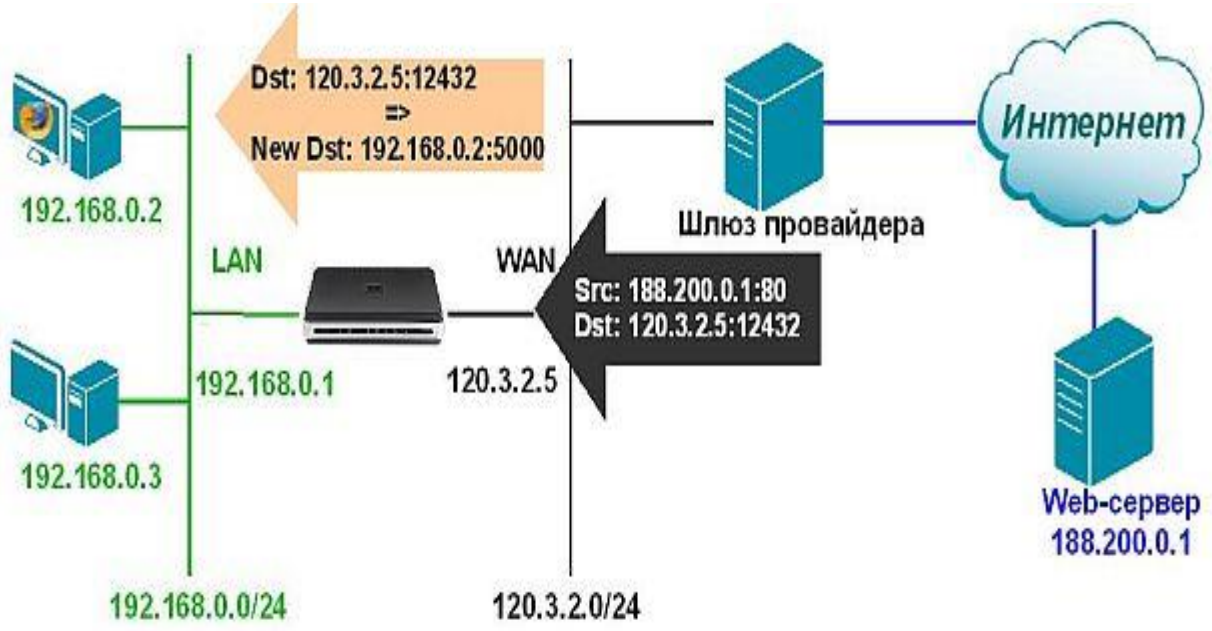


ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Принятие запроса сервером и отправка ответа

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Преобразование адресов при использовании функции NAT



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Три базовые концепции трансляции адресов

- статическая (SAT, Static Network Address Translation),
- динамическая (DAT, Dynamic Address Translation),
- маскарадная (NAPT, NAT Overload, PAT).

ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Четыре типа трансляции сетевых адресов

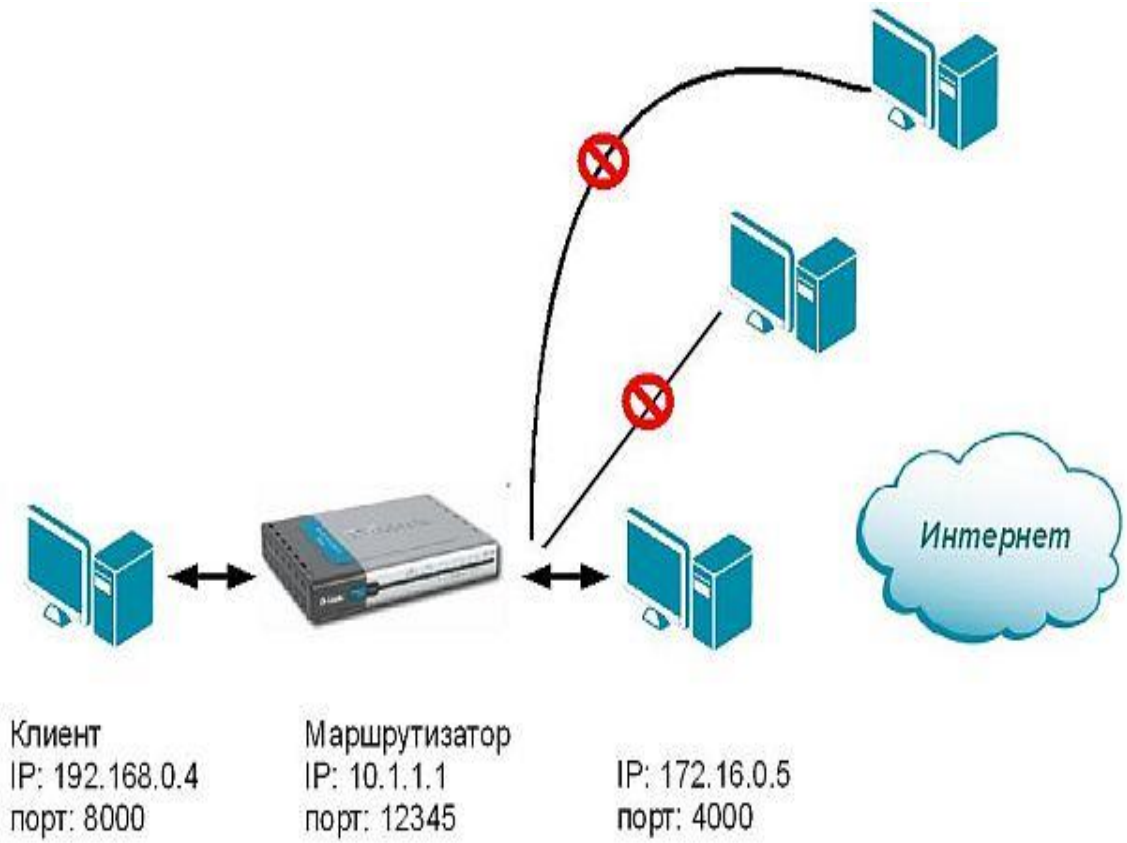
- Full Cone (Полный конус)
- Restricted Cone (Ограниченный конус)
- Port Restricted Cone (Порт ограниченного конуса)
- Symmetric (Симметричный)

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Использование NAT Full Cone

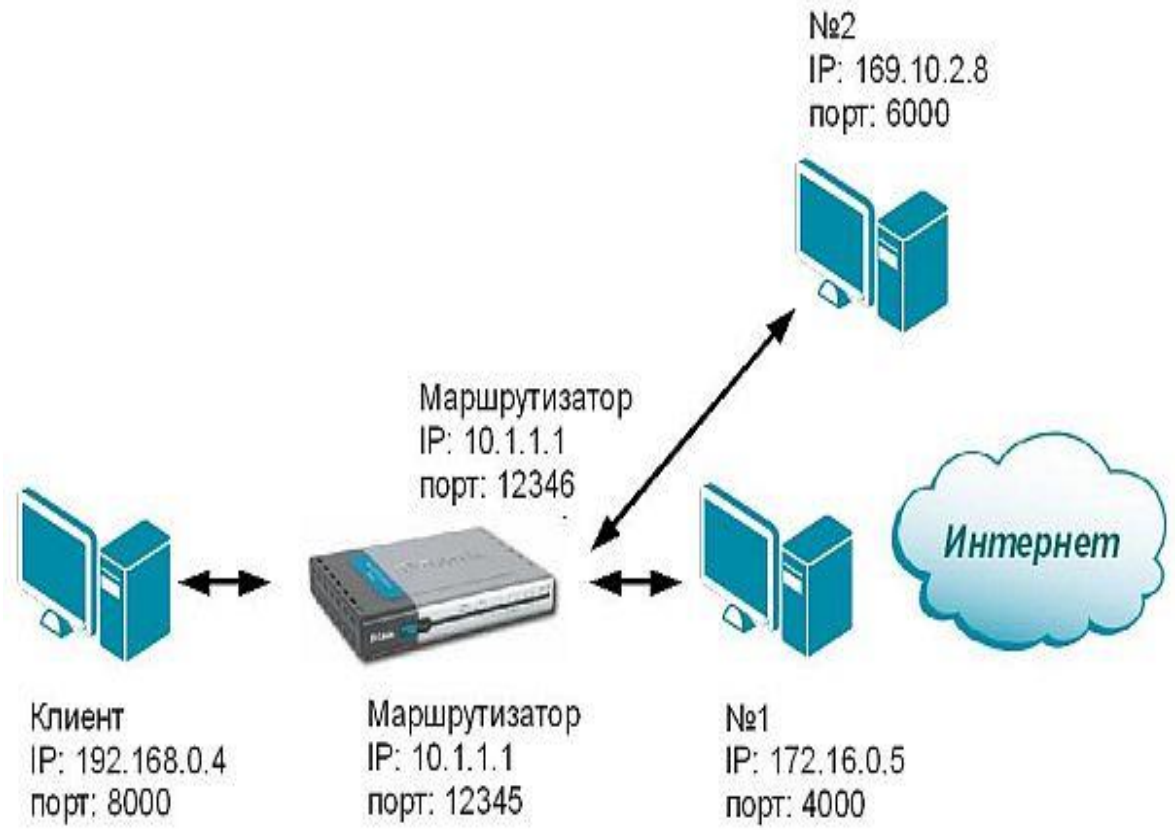
ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Использование NAT Restricted Cone



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Использование Symmetric NAT



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

NAT выполняет три важные функции

- Позволяет сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес
- Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения из внутренней сети во внешнюю
- Позволяет скрыть определенные внутренние сервисы внутренних хостов/серверов.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Недостатки NAT-технологии

- Не все протоколы могут «преодолеть» NAT
- Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций
- Атака DoS со стороны узла, осуществляющего NAT – если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS-атаки на сервис.