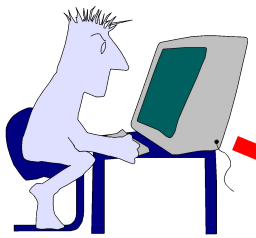
Методы борьбы с проблемами электронной почты

В предыдущей презентации были рассмотрены основные проблемы электронной почты.

Сейчас мы рассмотрим методы решения этих проблем. Для удобства здесь будут повторяться слайды предыдущей презентации с описанием проблемы.

Ошибки в программах и библиотеках



ВЗЛОМЩИК

- Программы с дырами
- Программы, настроенные неправильно
- Программы, сообщающие номер версии

LAN

Может получить полный или частичный контроль над сервером

Mail

SMTP
POP3
IMAP

Защита от взлома

Аналогична защите любой другой программы.

При первоначальной установке:

- Апгрейд ОС
- Безопасная настройка ОС
- Отключение ненужных сервисов
- Апгрейд программ и библиотек; возможно – замена на более безопасные аналоги
- Безопасная настройка программ
- По возможности – запуск программ под непривилегированным юзером
- Скрытие номера версии сетевых сервисов
- Закрытие сервера файерволом от Интернета и включение iptables на сервере

Защита от взлома (прод.)

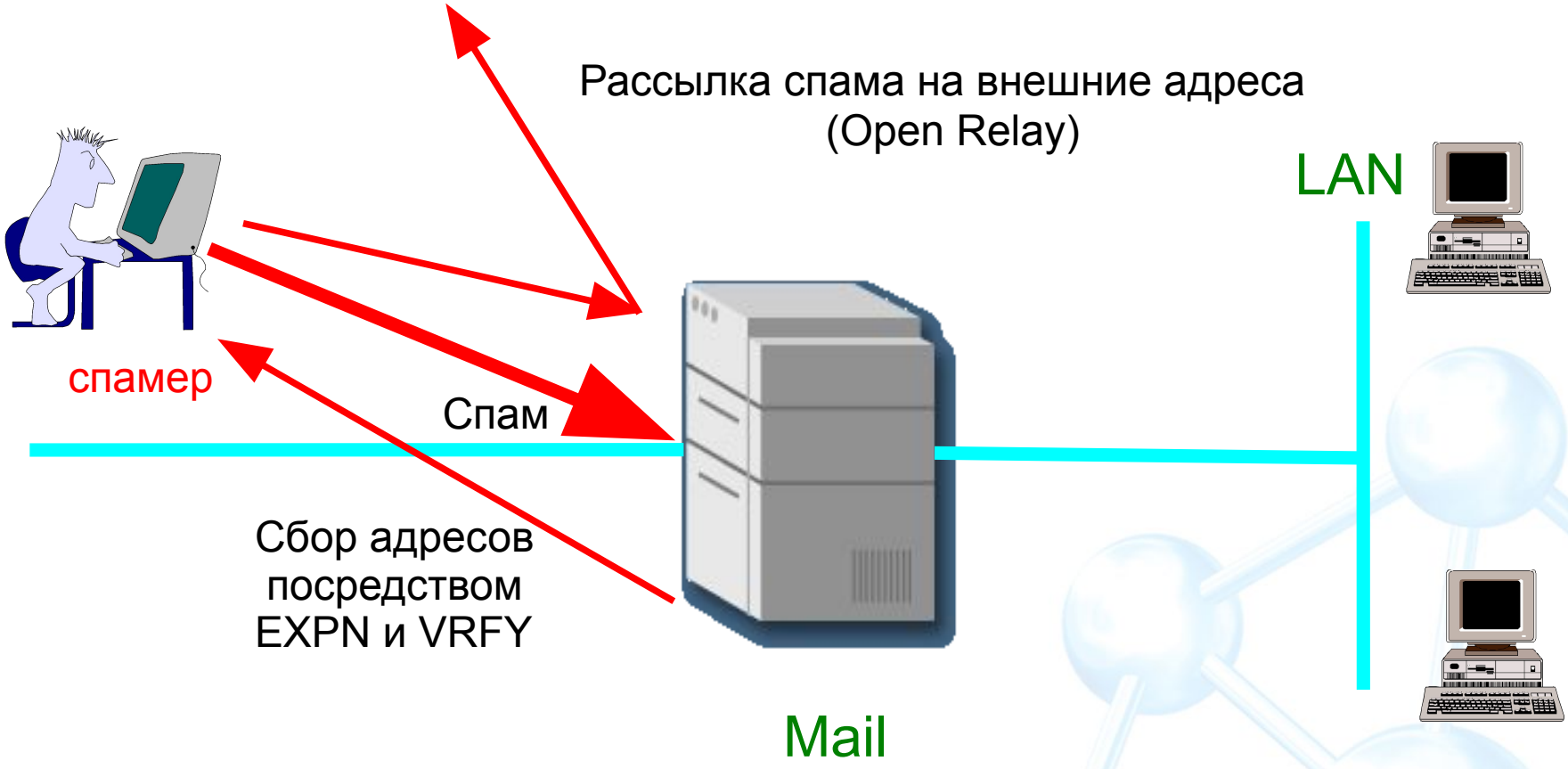
Постоянно:

- Отслеживание сообщений об уязвимостях
- Периодическое сканирование сервера на уязвимости
- Изучение нововведений в программах и ОС
- Общее повышение квалификации

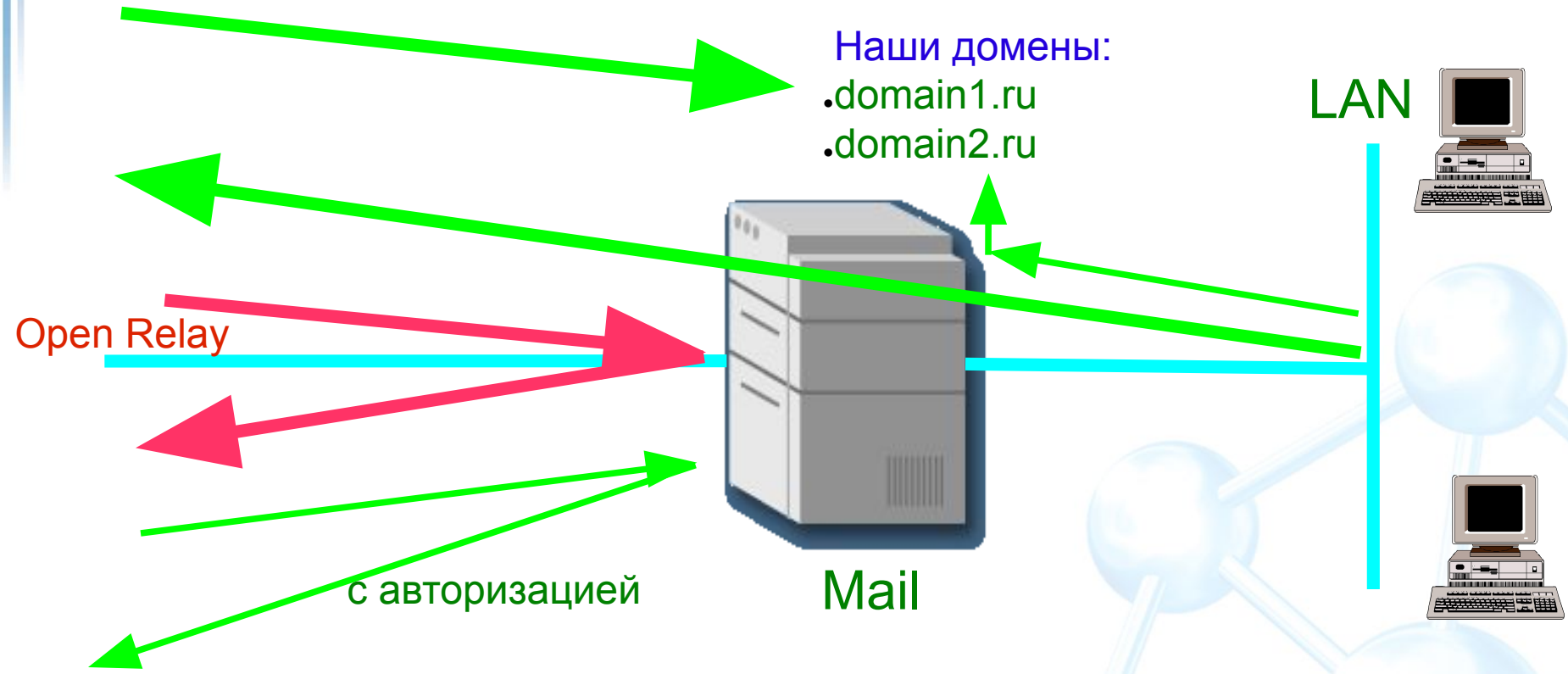
При установке нестандартных программ:

- Установка программ с хорошей репутацией
- Просмотр кода программы на наличие очевидных уязвимостей (например, нефильтрованный пользовательский ввод, используемый для команд оболочки или имен файлов)

Спам


Рассылка спама на внешние адреса
(Open Relay)
LAN
спамер
Спам
Сбор адресов
посредством
EXPN и VRFY
Mail

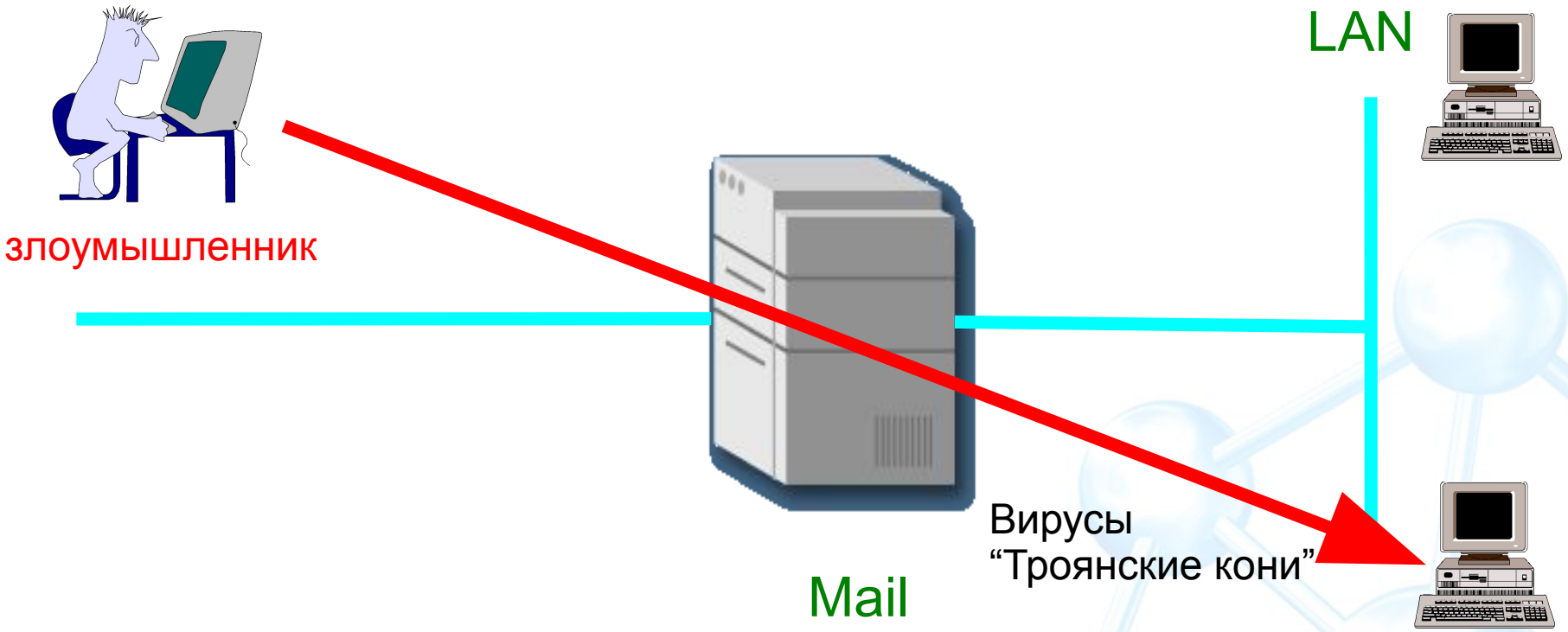
Легитимное использование почты



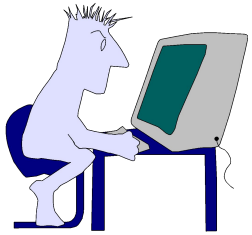
Настраиваем в почтовой программе:

- наши домены
- наши IP-адреса
- авторизацию

Угрозы клиентским машинам



Защита от спама и вирусов



злоумышленник

сбор адресов

~~EXPN~~

~~VRFY~~

LAN

Mail

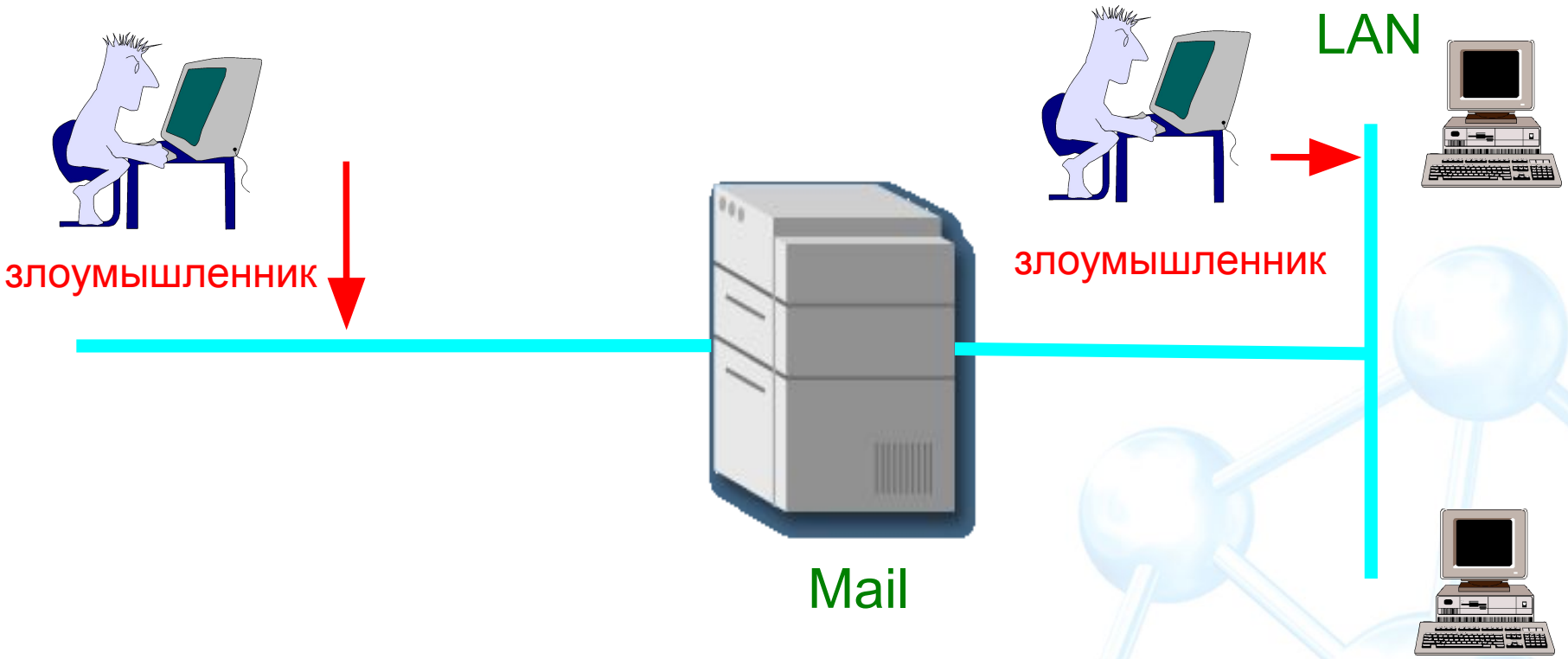
посылка спама

- Проверка в dns black lists
- Фильтровщики спама (SpamAssassin, Antispam Касперского)

посылка вирусов

Установка антивирусов на сервере: KAV (AVP), DrWeb и др.

Сниферы

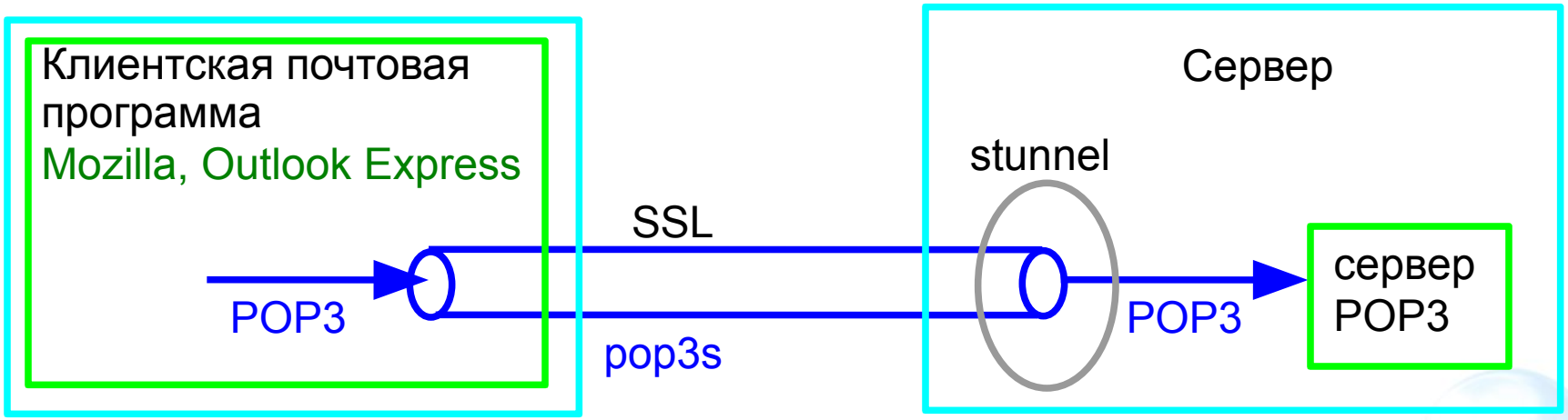


- Подслушивание паролей POP3, IMAP, SMTP
- Подслушивание почтового трафика

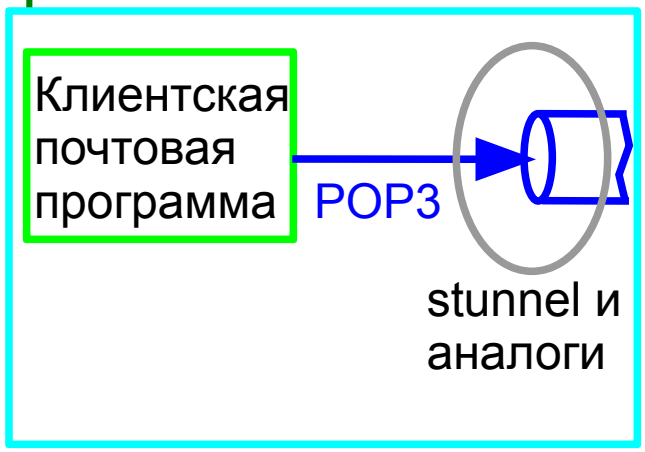
Защита от подслушивания

- Туннелирование POP3 и IMAP через SSL
- SMTP с SSL (STARTTLS)
- Шифрованные каналы между филиалами
- Шифрование важных сообщений средствами почтовой программы (SSL) или с помощью других программ

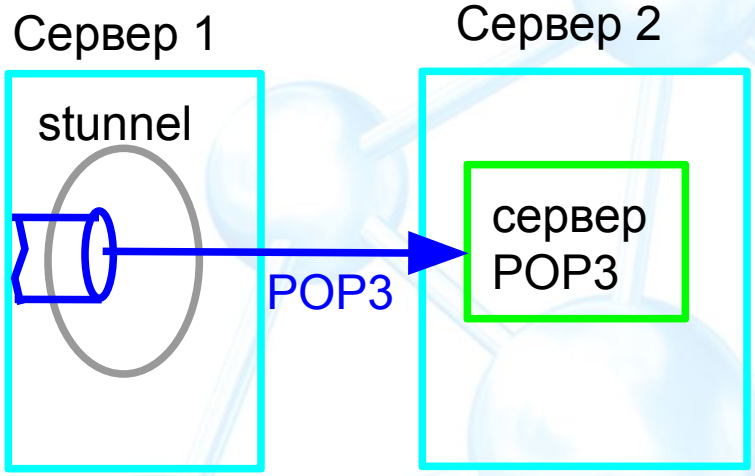
Туннелирование POP3 и IMAP



Варианты:



и т.д.

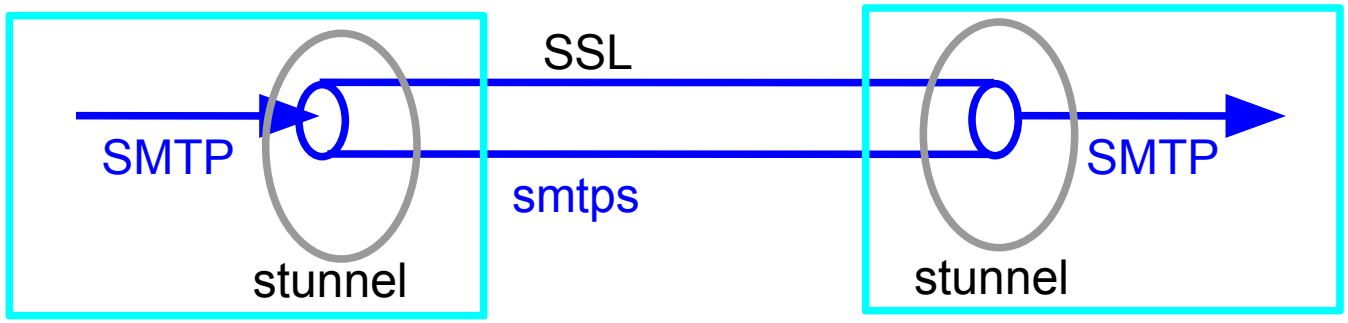


Для IMAP - аналогично

SMTP с SSL

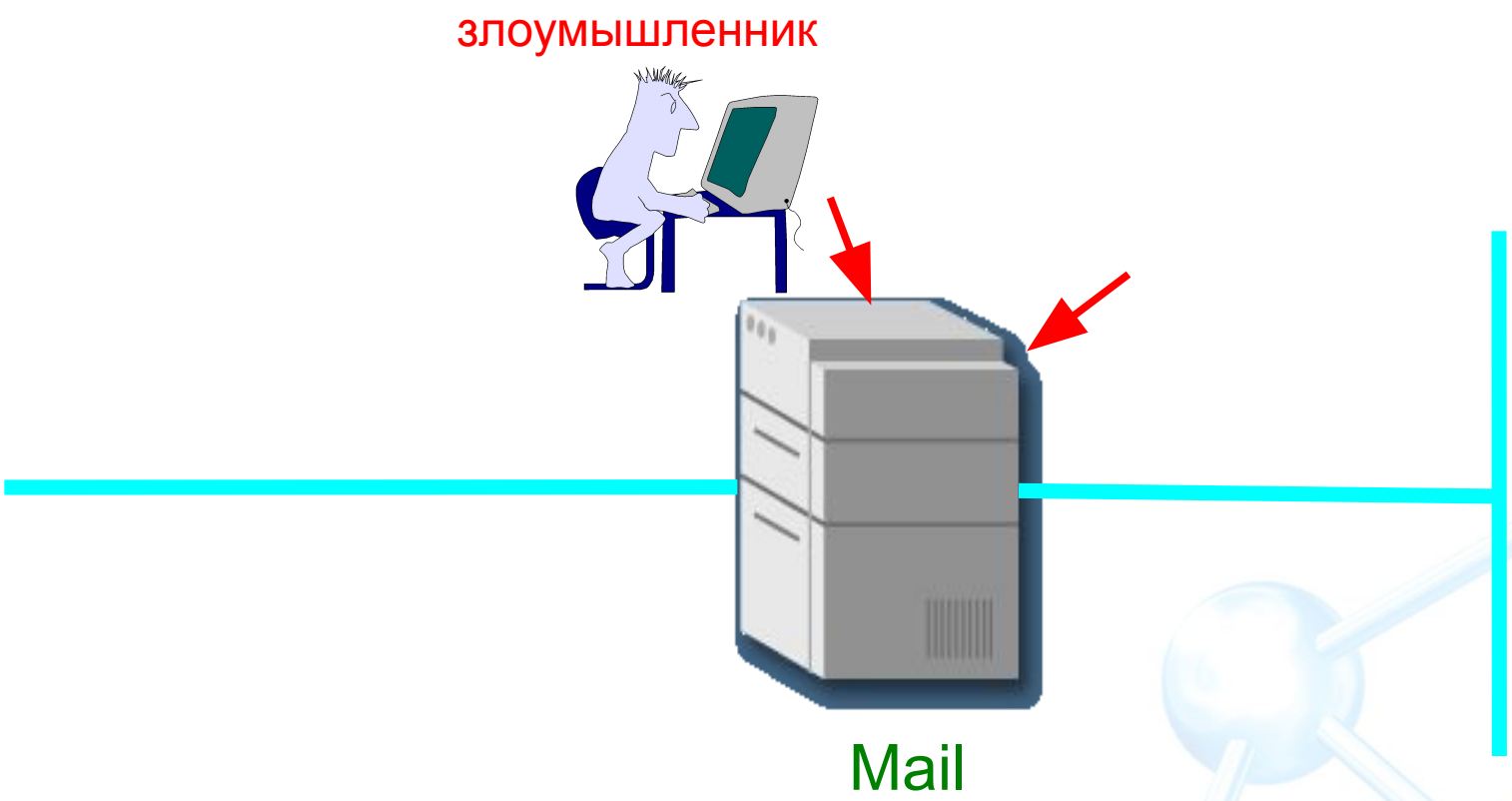
2 варианта:

1) Туннелирование аналогично POP3
(редко используемая устаревшая технология)



2) SMTP со встроенной поддержкой SSL (STARTTLS)

Локальные угрозы серверу

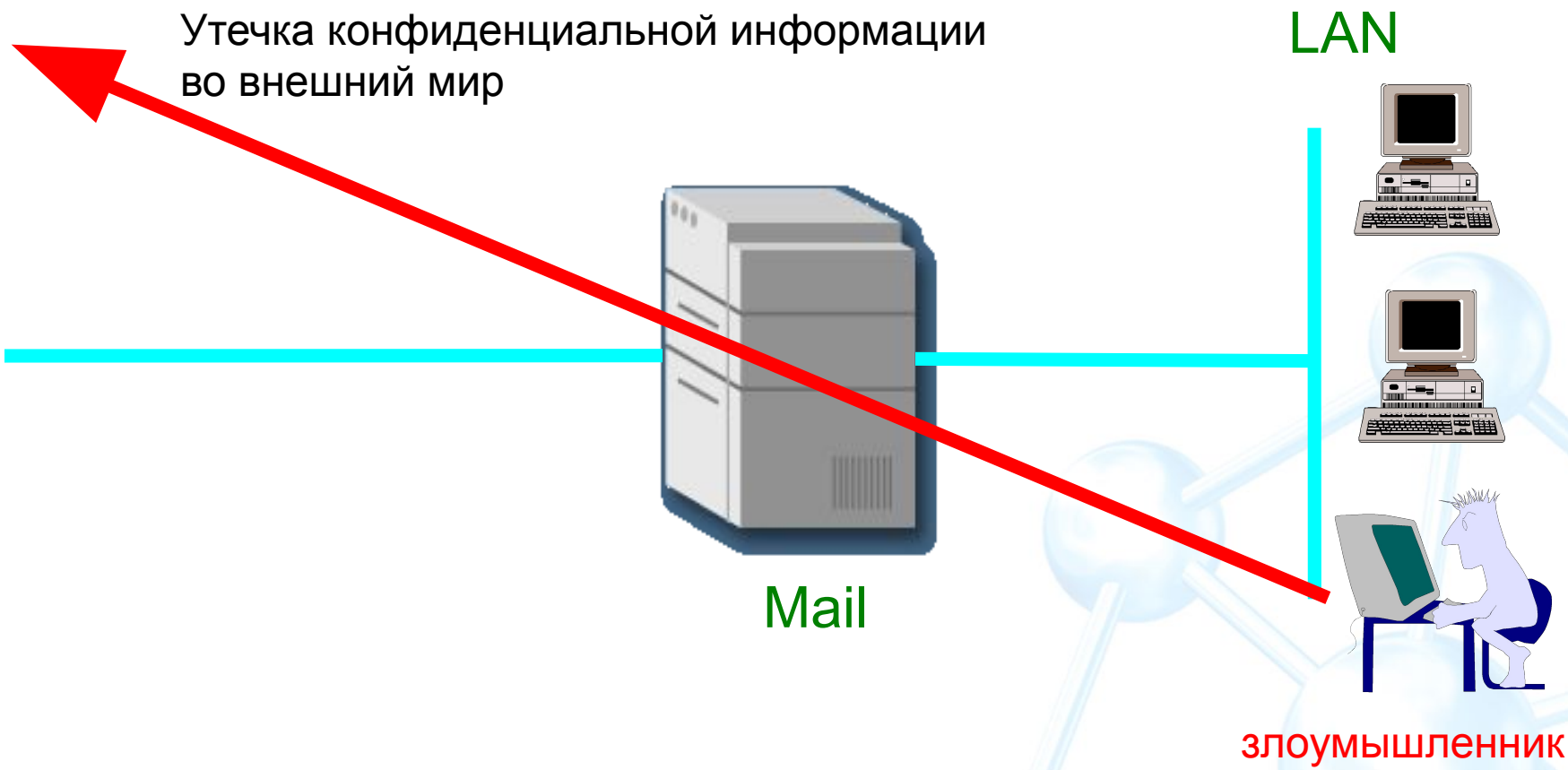


- Запуск программ посредством .forward
- Переполнение дисков
- Зацикливание автоответчиков

Защита от локальных угроз серверу

- Запрет создания или исполнения .forward
- smrsh и ее безопасная настройка
- Установка дисковых квот
- Просмотр кода программ автоответчиков и их тестирование

Утечка информации



Защита от утечки информации

Методы защиты:

- Копировать всю входящую и исходящую почту в файл или на специальный адрес email
- Проверять проходящую почту фильтровщиками, которые будут оповещать при нарушении политики безопасности
- Работа с персоналом

Существуют альтернативные каналы утечки:

- Бесплатные почтовые сервера с веб-интерфейсом
- Передача файлов по ftp
- Загрузка файла на сервер с помощью HTTP Upload
- Скрытие информации среди массива легитимных данных
- Передача информации в нестандартных сетевых пакетах
- Вынос информации на дискете, компакт-диске, жестком диске, флэш-карте USB, MP3-плеере, на распечатке

Вопросы ?