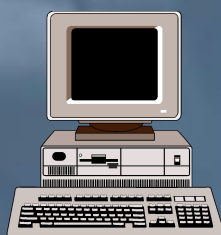


The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing the continents. In the bottom-right corner, there are several overlapping, semi-transparent white geometric shapes, including a large circle and a smaller, more complex polygonal shape. The text "Прикладные службы" is centered in the middle of the page in a bold, yellow font.

# Прикладные службы

# Реализация служб прикладного уровня



Клиент



Протокол обмена

TELNET  
FTP  
HTTP



Сервер

# Реализация службы FTP

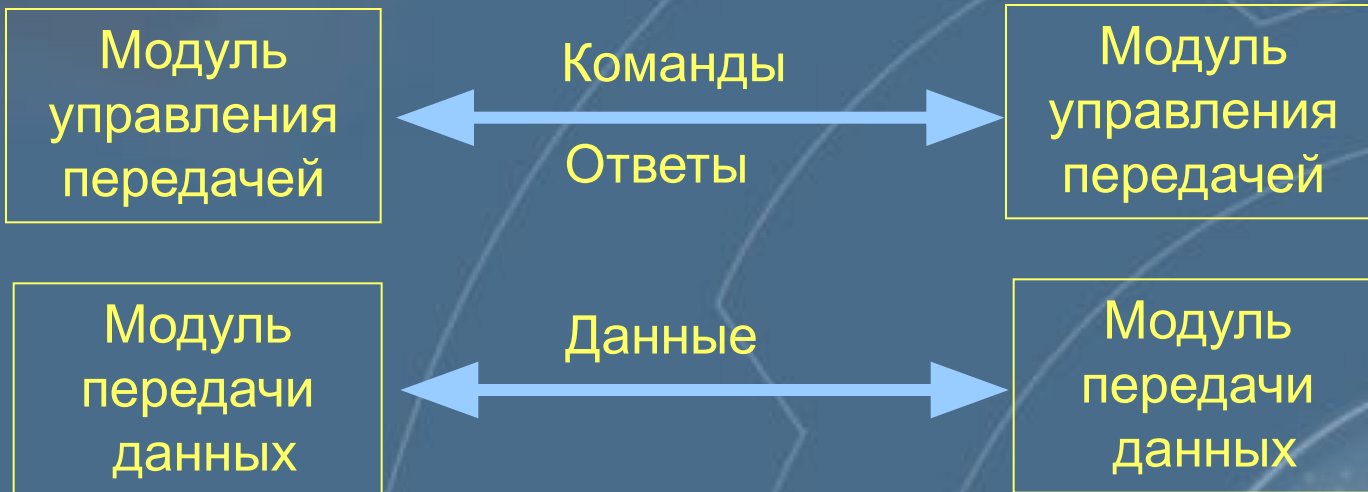


Сервер

Интерфейс  
пользователя



Клиент



# DNS - служба



telnet www.microsoft.com



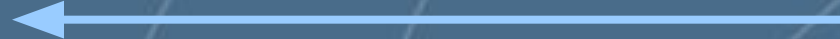
Resolver



www.microsoft.com - ?

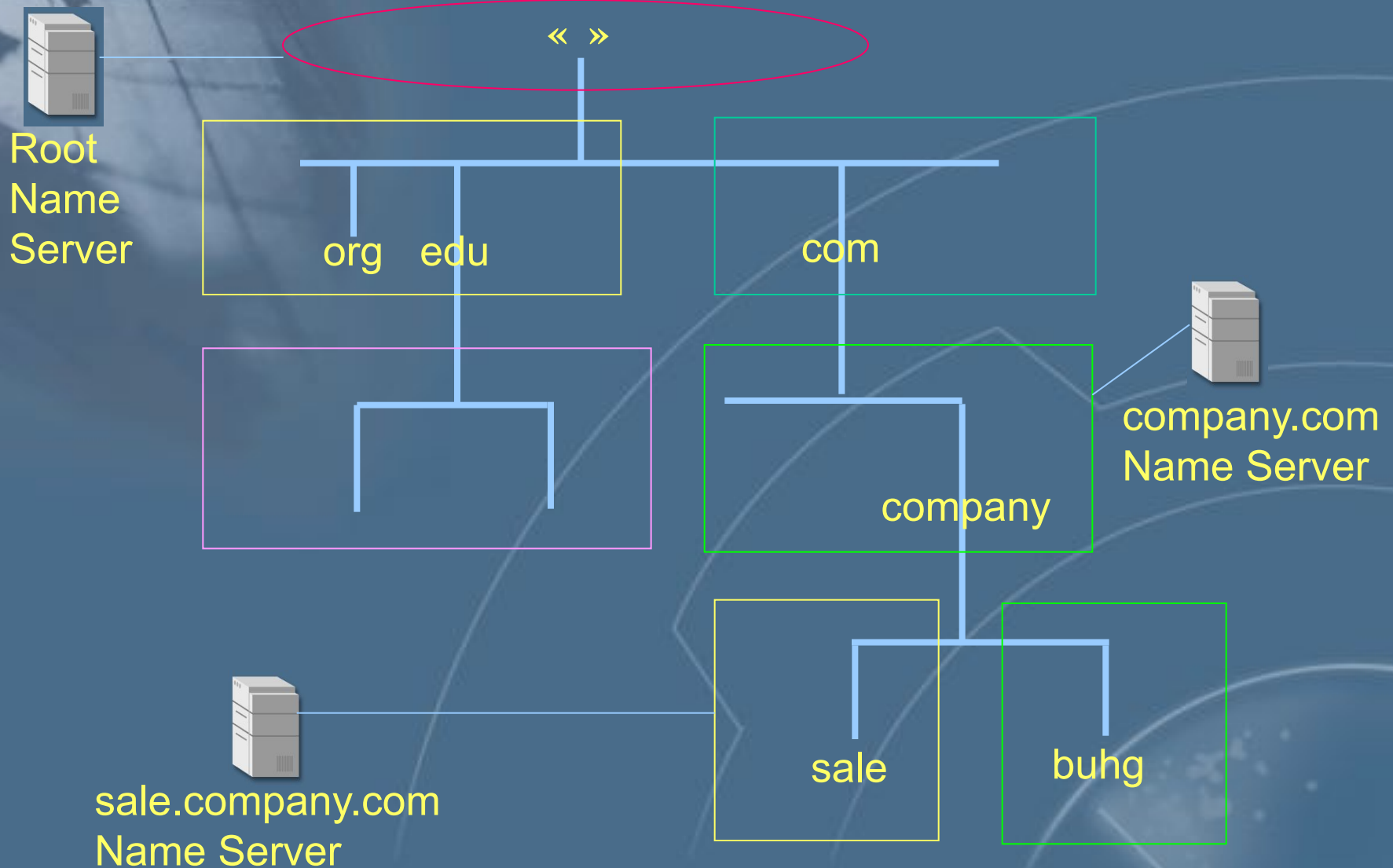


DNS Server



100.0.0.6

# Домены и поддомены



# Записи Resource Record

main.sale.company.com. IN A 100.0.0.120

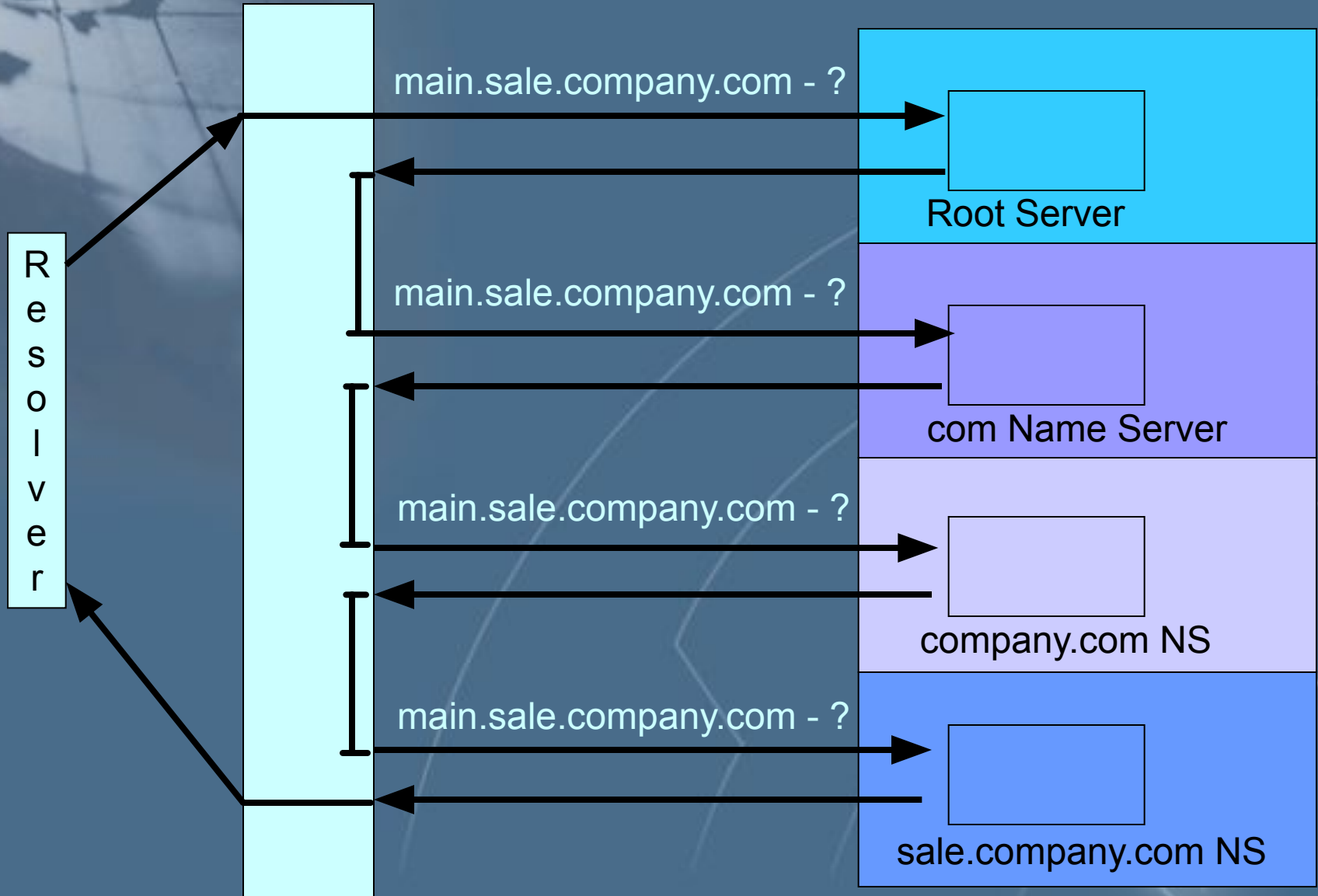
sale.company.com. IN NS ns.sale.company.com



sale.company.com  
Name Server

sale

# 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*

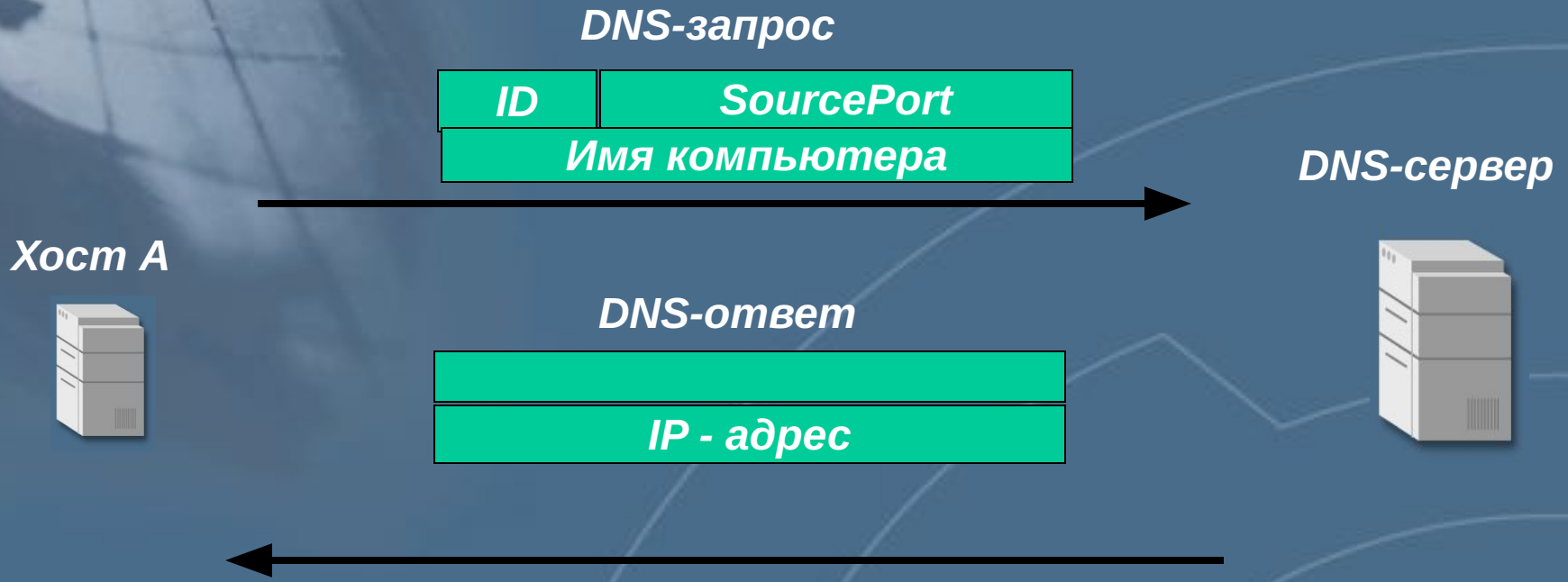
## Используемые уязвимости

*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*

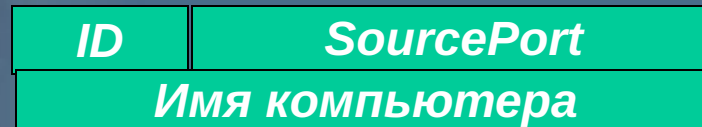
*Схема работы DNS - протокола*

# Пример атаки на IP - сеть: Атака на DNS

Хост А



DNS-запрос



DNS-сервер



Хост А посылает DNS - запрос

Хакер 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

Хост А



DNS-запрос



DNS-сервер



Хакер извлекает из запроса ID и SourcePort

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

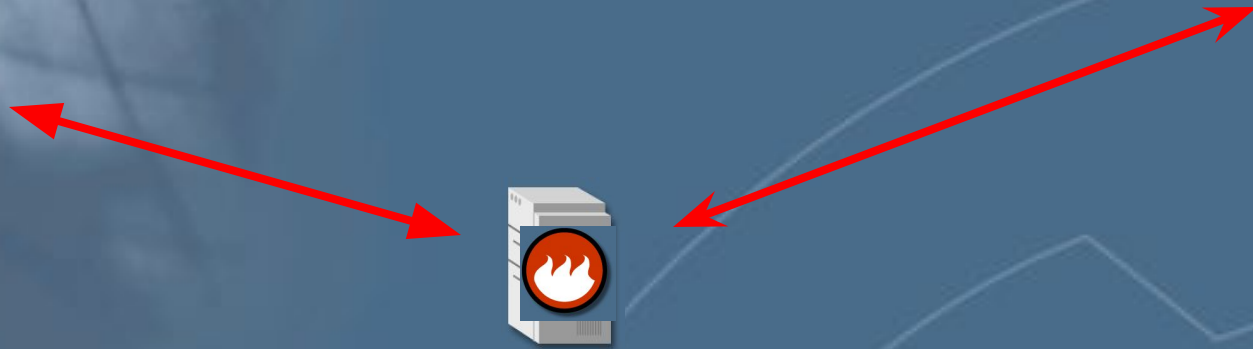
Результат: хост А имеет неправильное соответствие  
между именем компьютера и IP - адресом

# Пример атаки на IP - сеть: Атака на DNS

Хост А



Узел сети



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

# 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)

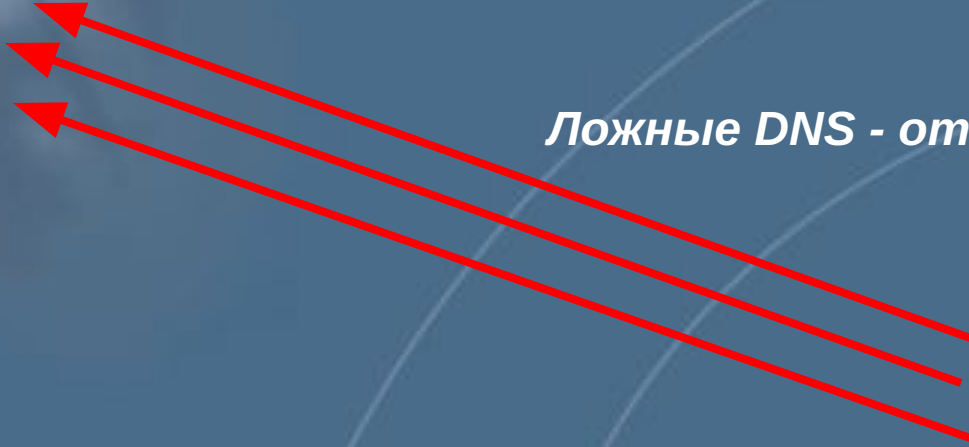
Хост А



DNS-сервер



Ложные DNS - ответы



ID	DestPort
IP - адрес	



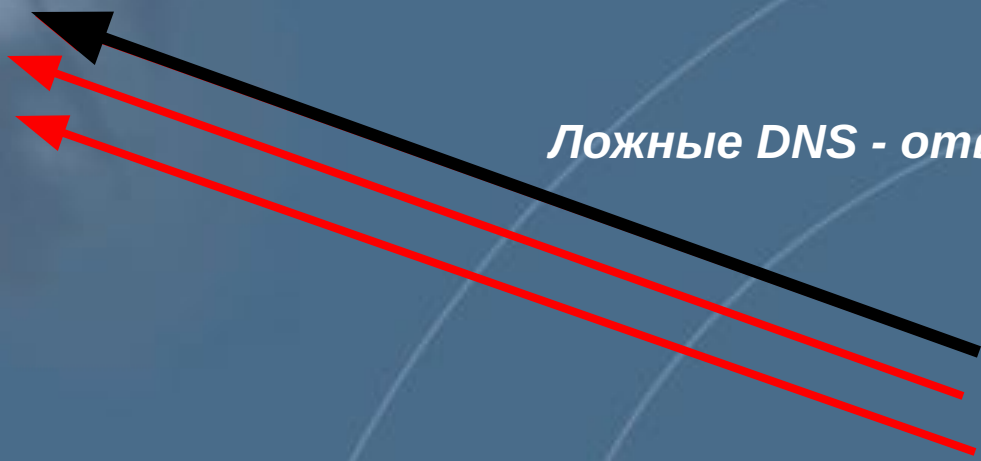
Перебор

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

Хост А



DNS-сервер



*Ложные DNS - ответы*



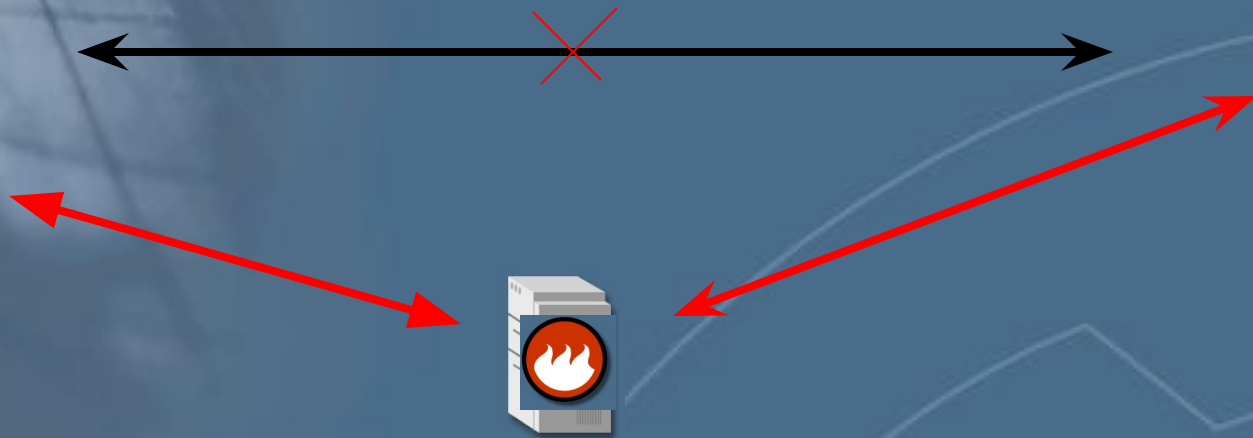


# Пример атаки на IP - сеть: Атака на DNS (вариант 2)

Хост А



Узел сети



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

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

*DNS-сервер*



*DNS-запрос*



*DNS-сервер  
следующего уровня*



*DNS-ответ*



*Кэш - таблица*



<b>193.233.70.129</b>	<b>ertr.mpei.ac.ru</b>
<b>· 194.154.77.109</b>	<b>www.infosec.ru</b>
<b>·</b>	<b>·</b>

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

DNS-сервер



DNS-сервер  
следующего уровня



DNS-запрос



Ложные DNS - ответы

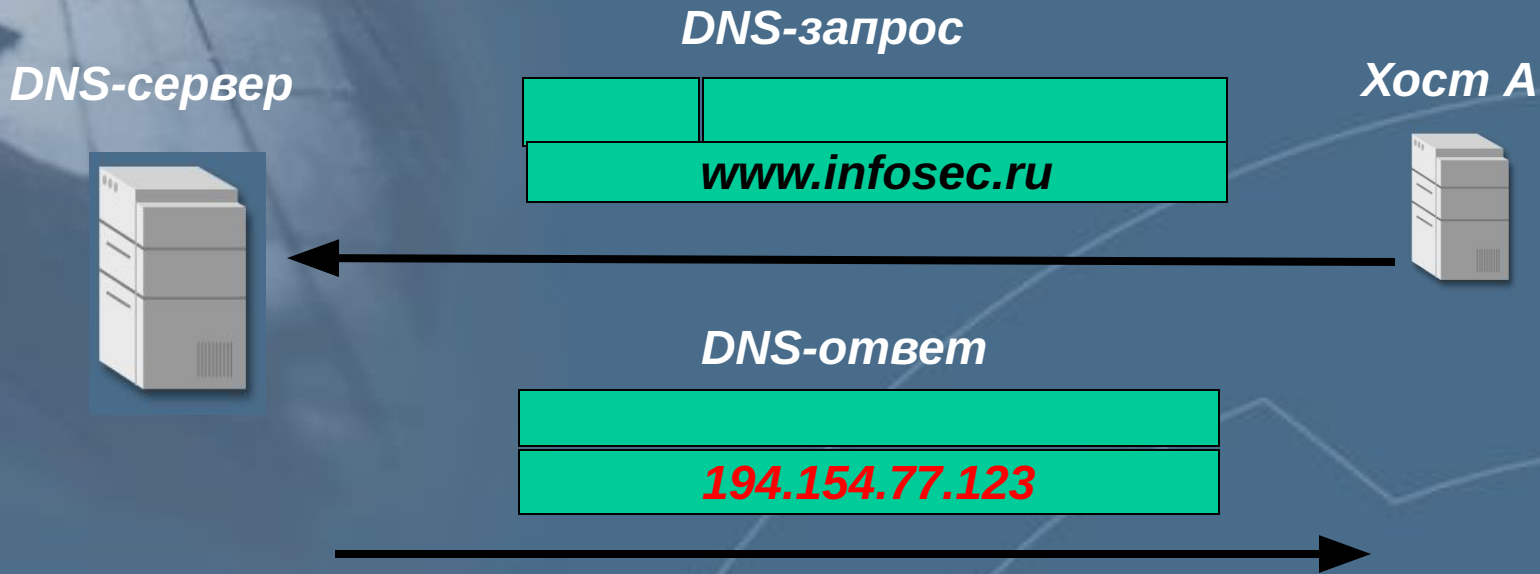


Кэш - таблица

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



# 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

Внешний узел



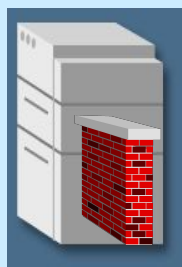
Рекурсивный запрос



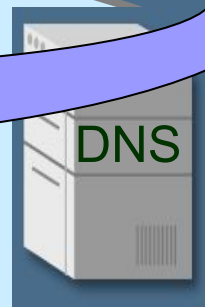
Вторичный сервер

Репликация

Рекурсивный запрос



Межсетевой экран



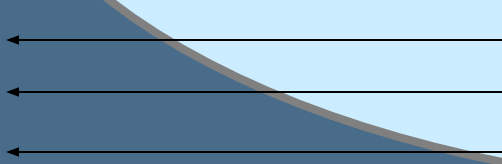
Первичный сервер (минимальная версия)

Первичный сервер (полная версия)



Внутренний узел

Итеративные запросы

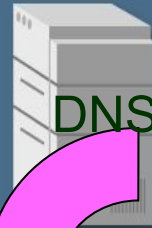


# Трёхсерверная конфигурация

Внешний узел



Рекурсивный запрос

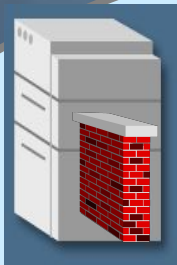


Вторичный сервер  
(минимальная версия)

Рекурсивный  
запрос



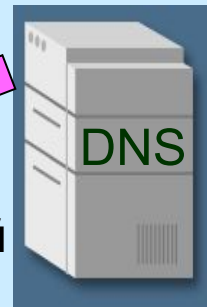
Репликация



Межсетевой  
экран



Первичный сервер  
(минимальная версия)



Первичный сервер  
(полная версия+корень)



Вторичный сервер  
(полная версия)

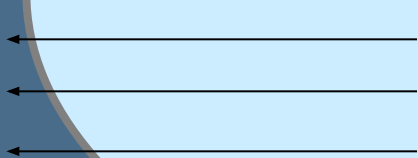


Внутренний узел  
(без Internet)



Внутренний узел  
(с Internet)

Итеративные  
запросы



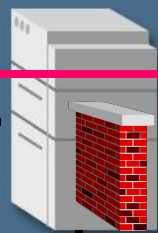


# Трёхсерверная конфигурация

Межсетевой  
экран



Internet



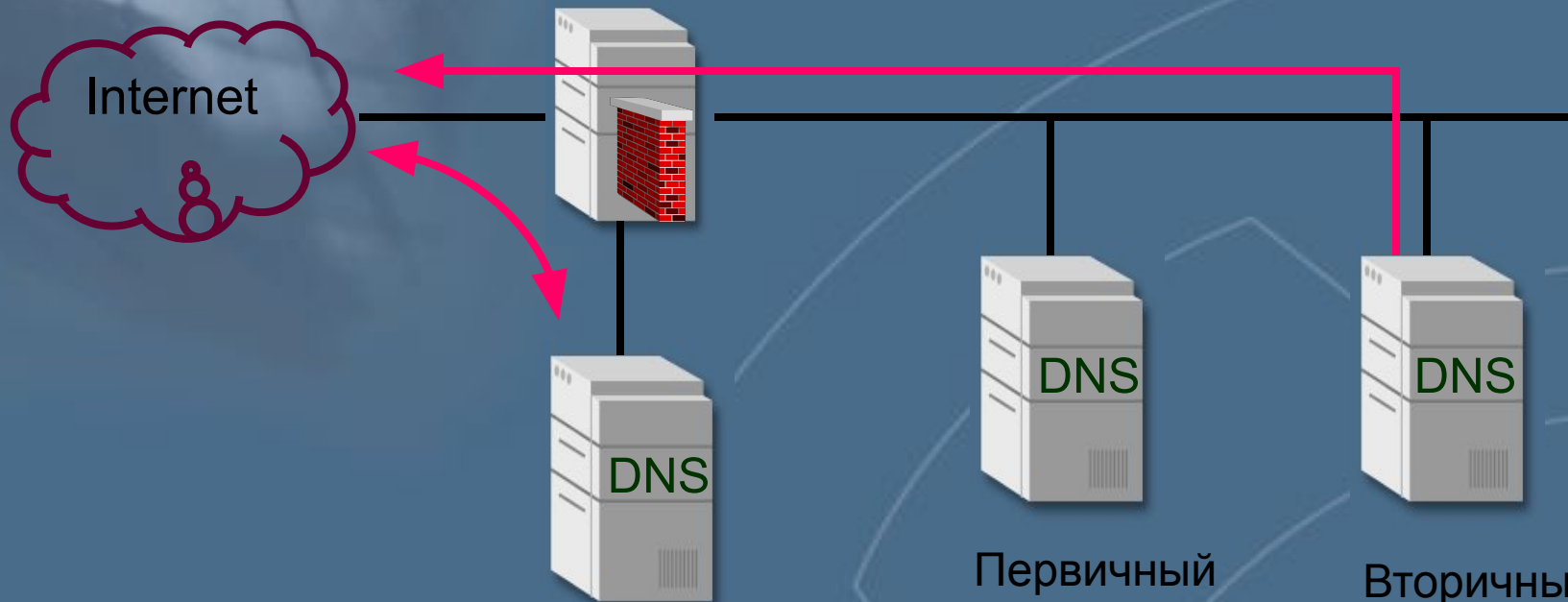
Первичный  
сервер  
(минимальная  
версия)



Первичный  
сервер  
(полная  
версия)  
+корень



Вторичный  
сервер  
(полная  
версия)



# 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
<u>Владелец</u> sale.company.com	NS	ns.sale.company.com
<u>Дополнительно</u> 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]

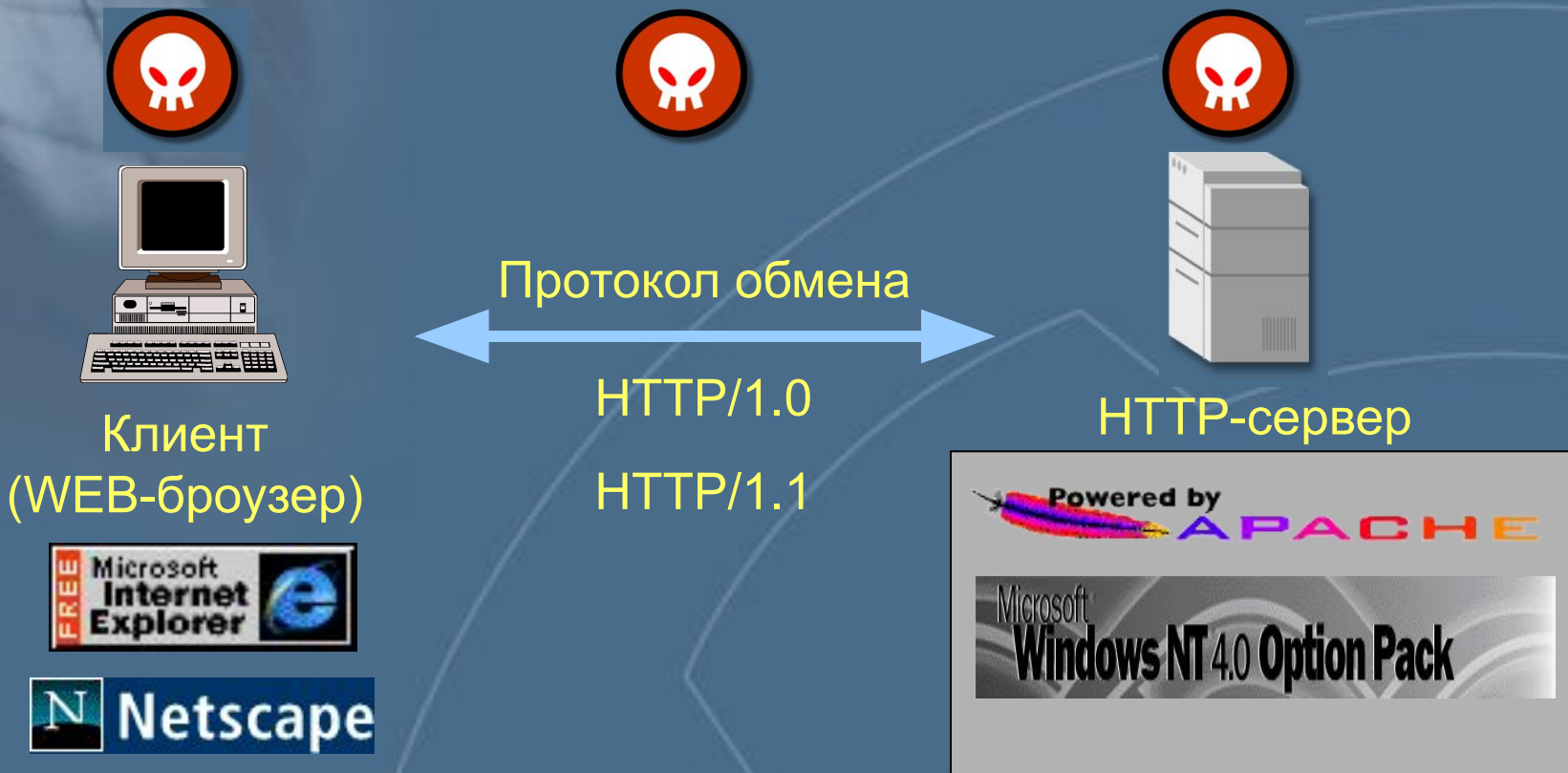
## Владелец

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

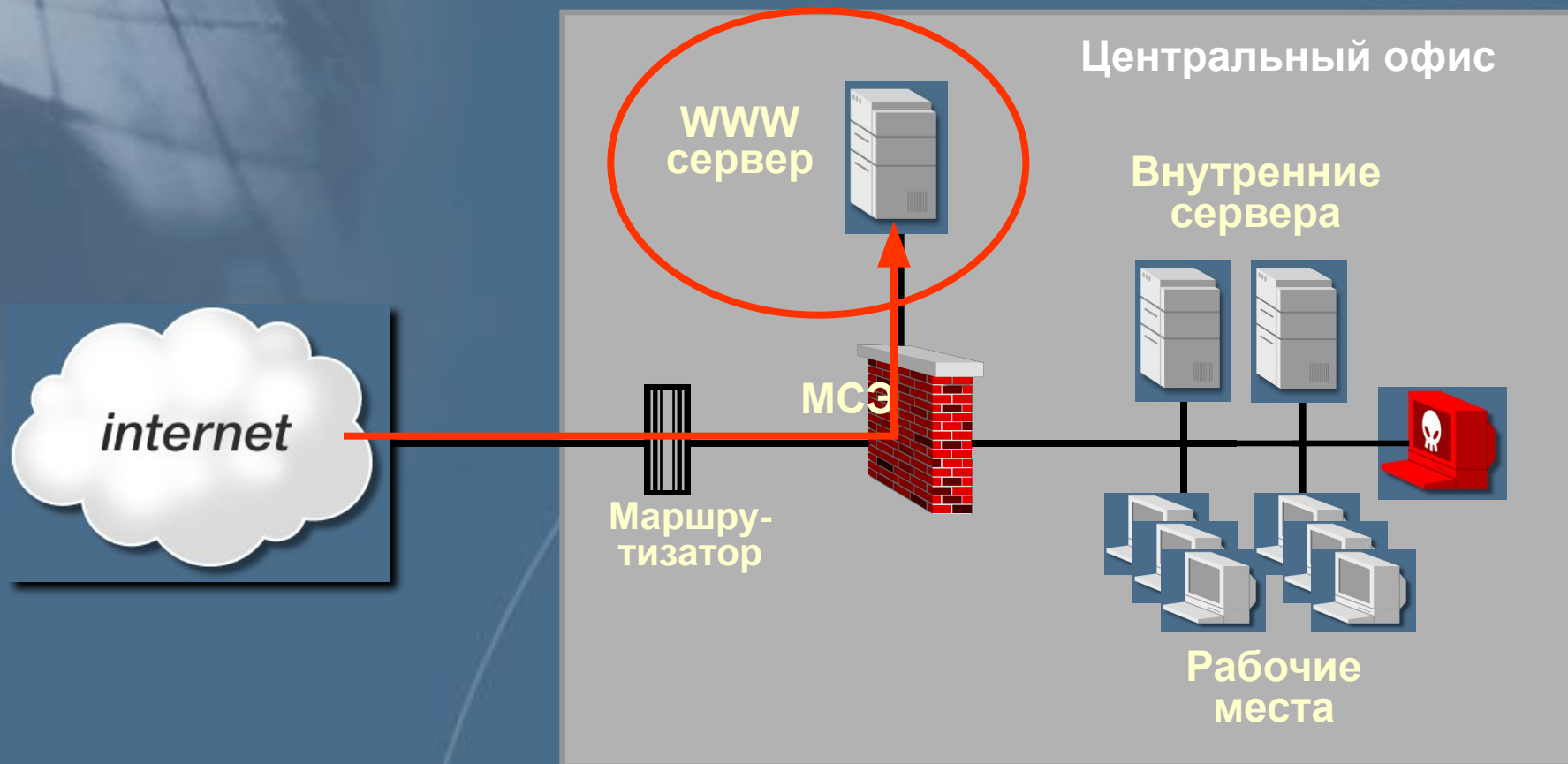
## Дополнительно

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]

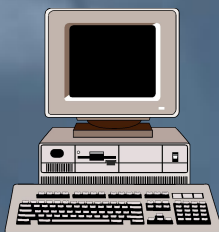
# Реализация WWW-службы



# Корпоративный WWW-сервер



# Пример уязвимости WWW-клиента



Клиент  
(WEB-браузер)



Hacker's  
Web site



C:\...\StartUp\ RunMe.hta



# Пример уязвимости протокола HTTP

HTTP - запросы

200.200.200.200

200.200.200.201

200.200.200.202



HTTP-пакеты большого размера  
С разных IP-адресов

# Уязвимости WWW-серверов

- *Уязвимости программной реализации (ошибки кода)*
- *Уязвимости информационного наполнения*
- *Ошибки обслуживания (настройки)*

# Отказ в обслуживании «IIS\_DoS»

## Цель

*Нарушение нормального функционирования объекта атаки*

## Механизм реализации

*Бесполезное расходование вычислительного ресурса  
(посылка некорректных HTTP-запросов)*

## Местонахождение атакующего

*В разных сегментах с объектом атаки*

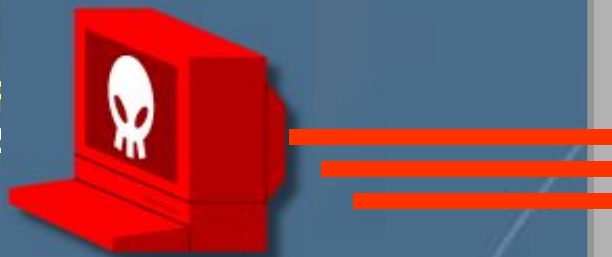
## Используемые уязвимости

*Ошибка в реализации MS Internet Information Server*

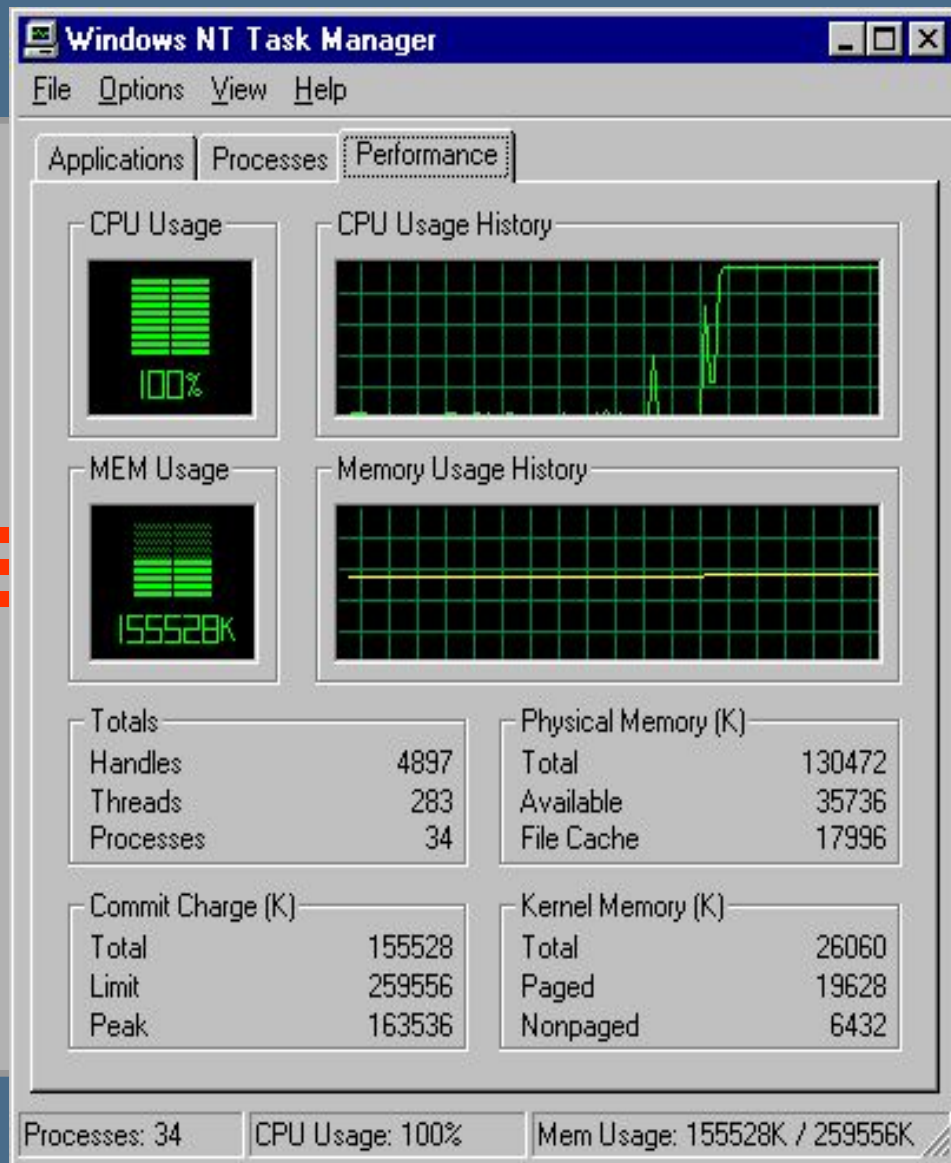
Степень риска Средняя

# Отказ в обслуживании «IIS\_DoS»

HACKER  
200.0.0.12



C:\HackTools \ iisdos.exe



# Ошибка обработки имён CGI - скриптов

## Цель

*Получение контроля над объектом атаки*

## Механизм реализации

*Запуск кода на объекте атаки*

## Местонахождение атакующего

*В разных сегментах с объектом атаки*

## Используемые уязвимости

*Ошибка в реализации MS Internet Information Server*

Степень риска Средняя

# Ошибка обработки имён CGI - скриптов

Описание уязвимости

HTTP



CVE: CAN-2000-0886

C:\dir

Опубликовано на сайте:  
NSFOCUS INFORMATION TECHNOLOGY CO.,LTD  
(<http://www.nsfocus.com>)

ИНФОРМЗАЩИТА

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

# Ошибка обработки имён НТР - файлов

Описание уязвимости

HTTP

<http://site/scripts/test.bat+.httr>



Содержимое файла  
test.bat



# Использование мобильного кода (Java, Active X ...)

## Цель

*Получение контроля над объектом атаки*

## Механизм реализации

*Запуск кода на объекте атаки  
(во время посещения Web-сайтов злоумышленников)*

## Местонахождение атакующего

*В разных сегментах с объектом атаки*

## Используемые уязвимости

*Ошибки проектирования и реализации активных  
компонентов приложений*

Степень риска **Высокая**



# Использование мобильного кода (Java, Active X ...)



**HACKER** Microsoft Word.Ink  
200.0.0.123



HTTP



200.0.0.123

Внутренняя сеть



# Запуск кода на объекте атаки (внедрение «Троянца»)



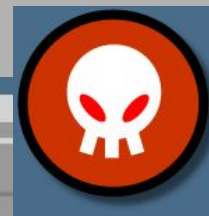
HACKER  
200.0.0.123



Запуск  
CGI – скрипта  
(PERL)

FTP

200.0.0.126



NetBus Pro<sup>®</sup> 2.0  
The easy-to-use remote administration and spy tool

Внутренняя сеть

# Запуск кода на объекте атаки (использование «Троянца»)



**HACKER**  
200.0.0.123



## Раздел 2 – Итоги

- Модель OSI. Архитектура TCP/IP.
- Сетевые анализаторы.
- Программа Internet Scanner 6.1.
- Межсетевые экраны.
- Протоколы IPSec, SSL, SSH, DNSSec
- Система обнаружения атак RealSecure 5.0.
- Службы прикладного уровня.