



НАУЧНО-
ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР

ФОРС



Сетевая безопасность



◆ Уязвимости

- Технологические;
- Конфигурационные;
- Отсутствие внятной политики безопасности.





◆ Угрозы

- Угрозы физической инфраструктуры;
- Неструктурированные угрозы;
- Структурированные угрозы;
- Внешние угрозы;
- Внутренние.





◆ Атаки

- **Разведка** (сканирование портов, анализ пакетов, запросы информации в интернете, проверка доступности (nslookup, whois, ping, Nmap, Superscan, Wireshark). **Защита:** шифрование полезной информации в пакетах; запрет на использование протоколов, восприимчивых к прослушиванию.
- **Доступ** (возможность злоумышленника получить доступ к устройству, для которого он не имеет учетной записи или пароля с помощью известных уязвимостей системы или программы) **Защита:** требовать от пользователей использовать сложные пароли, регулярно производить смену паролей.





◆ Атаки

- **Отказ в обслуживании (DoS)** (злоумышленник отключает какие-то службы или замедляет их работу до такой степени, что они перестают отвечать на запросы)

Пример: Ping смерти - ICMP пакеты с большим размером буфера (до 65536 байт);

много SYN запросов на установление TCP сессий; отправка большого количества сообщений электронной почты;

Распределенная атака с множества хостов (DDoS).

- **Черви, вирусы и трояны** (вредоносное ПО, повреждающее систему, отказывает в доступе, а также может передавать злоумышленнику конфиденциальную информацию с компьютера).





Базовая защита серверов и рабочих станций

1. После установки ОС сменить все учетные записи и пароли по умолчанию;
2. Разрешить доступ только определенным лицам;
3. Выключить все неиспользуемые службы и приложения;
4. Установить антивирус и регулярно его обновлять;
5. Поставить персональный брандмауер;
6. Регулярно проверять и устанавливать обновления для ОС;
7. Использовать системы:
 - обнаружения вторжений (IDS);
 - предотвращения вторжений (IPS).





«Колесо» сетевой безопасности

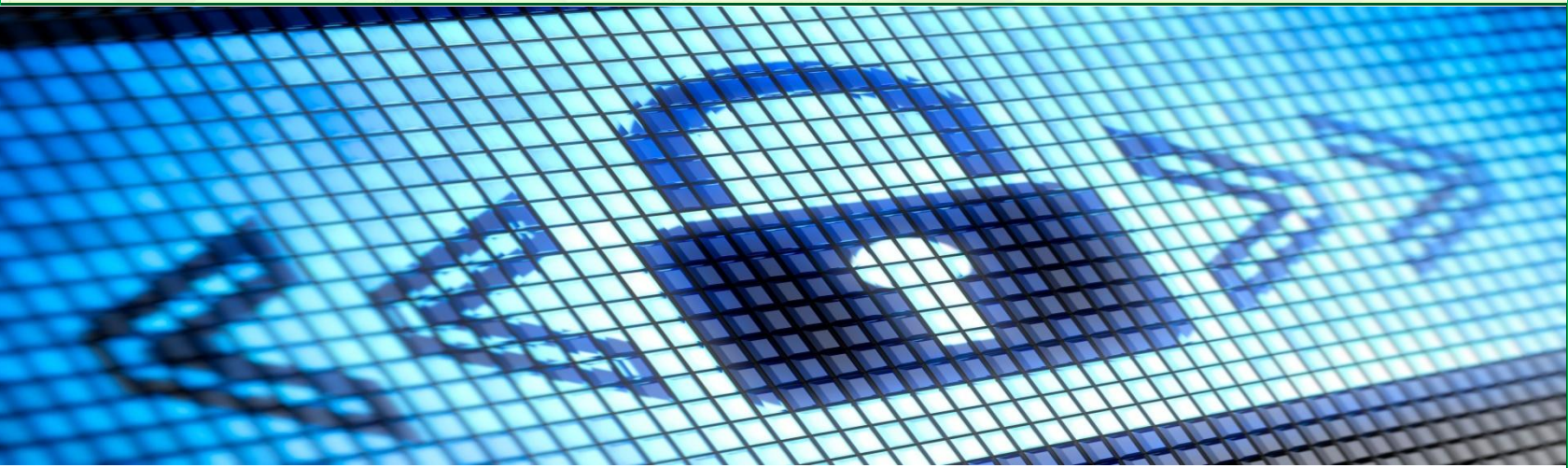
1. Защита;
 2. Мониторинг;
 3. Тестирование;
 4. Усиление защиты.
- ❖ Защита маршрутизаторов:
- физическая безопасность;
 - обновление IOS до последней стабильной версии;
 - резервное копирование IOS и конфигурации;
 - отключение неиспользуемых портов и служб.





НАУЧНО-
ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР

ФОРС



Настройка безопасности на маршрутизаторе



1. Настройка паролей на маршрутизаторе

- ❖ Уровень шифрования паролей:
 - без шифрования(0);
 - простое шифрование (7), команда:
R1(config)#service password-encryption
 - комплексное шифрование (5), команды:
R1(config)#username admin secret cisco
R1(config)#enable secret cisco

- ❖ Требования маршрутизатора по длине паролей:
R1(config)#security passwords min-length 10
(Команда будет иметь эффект только для новых паролей)





2. Настройка удаленного доступа

- ❖ На портах (линиях), через которые не будет проводиться конфигурирование, отключаем командами:
R1(config)#line aux 0
R1(config-line)#no password
R1(config-line)#login
R1(config)#line aux 0
- ❖ На виртуальных каналах (VTY) по умолчанию настроена возможность подключения через любые протоколы. Поэтому лучше оставлять возможность подключения лишь через определенные протоколы.
R1(config)#line vty 0 4
R1(config-line)#no transport input
R1(config-line)#transport input ssh





2. Настройка удаленного доступа

- ❖ **Злоумышленник может подключиться ко всем виртуальным линиям без ввода пароля, при этом администратор не сможет подключиться, т.к. все линии заняты. Решение:**
 - настроить одну виртуальную линию для работы только с конкретного IP адреса;
 - настроить тайм-аут для неиспользуемых сессий, через который виртуальные линии будут освобождаться:
R1(config)#line vty 0 4
R1(config-line)#exec-timeout 3 30 - в минутах и секундах
- ❖ **Защититься от возможности перехвата сессий Telnet:**
R1(config)#line vty 0 4
R1(config-line)#service tcp-keepalives-in





2. Настройка удаленного доступа



Настроить SSH

```
Router(config)#hostname R1
```

```
R1(config)#ip domain-name cisco.com
```

```
R1(config)#crypto key generate rsa
```

```
How many bits in the module [512]: 1024
```

```
R1(config)#username student secret cisco
```

```
R1(config)#line vty 0 4
```

```
R1(config-line)#transport input ssh
```

```
R1(config-line)#login local
```

```
R1(config)#ip ssh time-out 15 - время ожидания неактивной сессии SSH
```

```
R1(config)#ip ssh authentication-retries 2 - количество попыток ввода пароля
```





2. Настройка удаленного доступа

❖ Уязвимые службы и интерфейсы.
R1(config)#no service tcp-small-servers
R1(config)#no service udp-small-servers
R1(config)#no ip bootp server
R1(config)#no service finger
R1(config)#no ip http server
R1(config)#no snmp-server

❖ Неиспользуемые службы:
R1(config)#no cdp run
R1(config)#no service config - удаленное автоконфигурирование
R1(config)#no ip source-route
R1(config)#no ip classless





2. Настройка удаленного доступа

- ❖ Отключить неиспользуемые интерфейсы
R1(config-if)#shutdown
- ❖ Отключить на интерфейсах возможность отвечать на пакеты с поддельными адресами источника
R1(config-if)#no ip directed-broadcast
R1(config-if)#no ip proxy-arp





2. Настройка удаленного доступа

❖ Сетевые протоколы

- SNMP - использовать только версию 3 (позволяет шифровать информацию);
- NTP - отключать протокол на портах, через которые он не будет использоваться;
- DNS - по умолчанию, если DNS сервер не указан в настройках маршрутизатора, он начинает искать сервер путем рассылки широковещательных запросов.
 - явно указывать адрес DNS сервера:
R1(config)#ip name-server addresses
 - отключать рассылку широковещательных DNS запросов:
R1(config)#no ip domain-lookup.





НАУЧНО-
ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР

ФОРС



Настройка аутентификации в протоколах динамической маршрутизации



1. Настройка интерфейсов, через которые можно отправлять обновления

```
R1(config)#router rip
```

```
R1(config-router)#passive-interface default -
```

отключаем рассылку на всех интерфейсах

```
R1(config-router)#no passive-interface s0/0/0 -
```

включаем рассылку на конкретных интерфейсах.





2. Предотвращение несанкционированного приема обновлений RIP

2.1. RIP

R1(config)#key chain RIP_KEY - создаем ключевую цепочку

R1(config-keychain)#key 1

R1(config-keychain-key)#key-string cisco

R1(config)#interface s0/0/0

R1(config-if)#ip rip authentication mode md5 - указываем алгоритм шифрования

R1(config-if)#ip rip authentication key-chain RIP_KEY - привязываем цепочку к протоколу.





2.2. EIGRP

```
R1(config)#key chain EIGRP_KEY  
R1(config-keychain)#key 1  
R1(config-keychain-key)#key-string cisco  
R1(config)#interface s0/0/0  
R1(config-if)#ip authentication mode eigrp 1 md5  
R1(config-if)#ip authentication  
key-chain eigrp 1 EIGRP_KEY
```





2.3. OSPF

2.3.1. Простая аутентификация без шифрования

```
R1(config)#router ospf 1
```

```
R1(config-router)#area 0 authentication - все обновления  
в зоне 0 будут требовать аутентификации
```

```
R1(config-router)#interface S0/0/0
```

```
R1(config-if)#ip ospf authentication-key cisco123 -  
указываем ключ
```

2.3.2. MD5 аутентификация

```
R1(config)#interface s0/0/0
```

```
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
```

```
R1(config-if)#ip ospf authentication message-digest
```

```
R1(config)#router ospf 10
```

```
R1(config-router)#area 0 authentication message-digest
```





Автонастройка безопасности маршрутизатора

❖ Автонастройка безопасности маршрутизатора

```
R1# auto secure;
```

❖ The Cisco Router and Security Device Manager

```
R1# configure terminal
```

```
R1(config)# ip http server
```

```
R1(config)# ip http secure-server
```

```
R1(config)# ip http authentication local
```

```
R1(config)# username Name privilege 15 secret cisco
```

```
R1(config)# line vty 0 4
```

```
R1(config-line)# privilege level 15
```

```
R1(config-line)# login local
```

```
R1(config-line)# transport input telnet ssh
```





НАУЧНО-
ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР
ФОРС

Вопросы?

