Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

Доклад на тему:

МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ АЛГОРИТМОВ МАРШРУТИЗАЦИИ ТРАФИКА АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Докладчики: Лебедкина Т.В., Степаненко Н.Д.

ЦЕЛЬ, ОБЪЕКТ И ПРЕДМЕТ ИССЛЕДОВАНИЯ

Цель работы – обеспечение безопасности автоматизированных систем путем разработки имитационной модели для оценки защищенности алгоритмов маршрутизации трафика в системе.

Объект исследования – алгоритмы маршрутизации трафика автоматизированных систем.

Предмет исследования – защищенность алгоритмов маршрутизации трафика в автоматизированных системах.

СООТВЕТСТВИЕ АЛГОРИТМОВ МАРШРУТИЗАЦИИ ПРОТОКОЛАМ МАРШРУТИЗАЦИИ

Дистанционно-векторный алгоритм	**Routing Information protocol version 1,2 (RIP)**
Алгоритм маршрутизации состояния канала	**Open Shortest Path First (OSPF), Intermediate System – Intermediate System (IS-IS)**
Алгоритм маршрутизации по вектору состояний	**Border Gateway Protocol (BGP)**

АТАКА НА ПРОТОКОЛ RIP

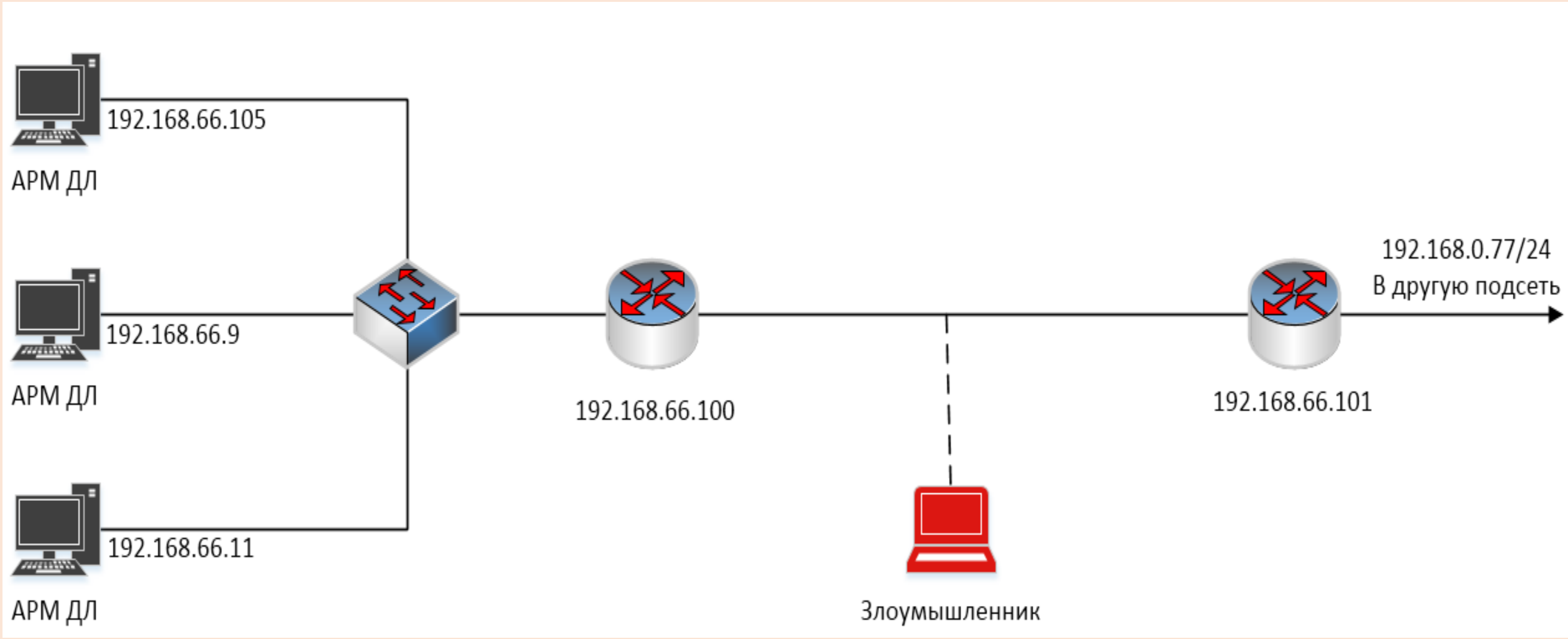
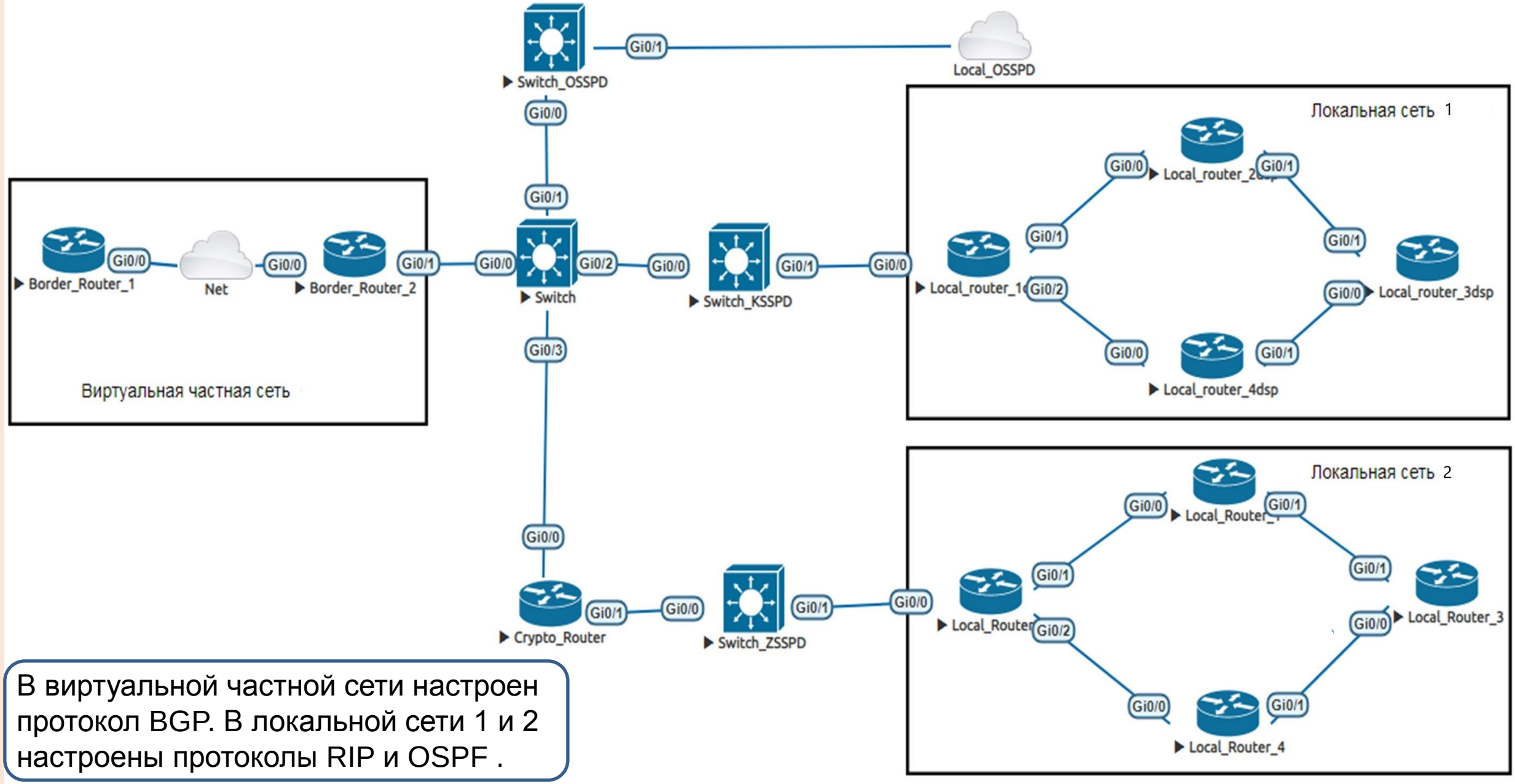


СХЕМА ИМИТАЦИОННОЙ МОДЕЛИ



В виртуальной частной сети настроен протокол BGP. В локальной сети 1 и 2 настроены протоколы RIP и OSPF .

УПРАВЛЯЮЩАЯ ЧАСТЬ В ИМИТАЦИОННОЙ МОДЕЛИ

EVE-NG

UltraVNC 1.2.1.7

Kali Linux 2018.1

Scapy 2.4.2

HashCat 5.1.0

Wireshark 2.6.8

Nmap 7.50

Metasploit Framework 4.12.22

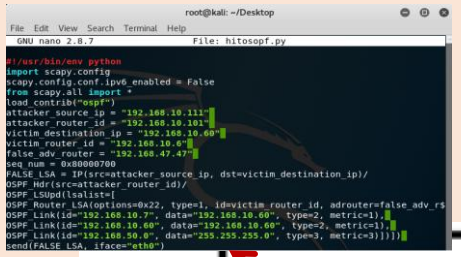
Общая последовательность действий для оценки защищенности алгоритмов маршрутизации:

- ❖ **Осуществление компьютерной атаки;**
- ❖ **Оценка защищенности с использованием метрик CVSS;**
- ❖ **Применение встроенных механизмов защиты протоколов маршрутизации;**
- ❖ **Повторное осуществление компьютерной атаки;**
- ❖ **Повторная оценка защищенности.**

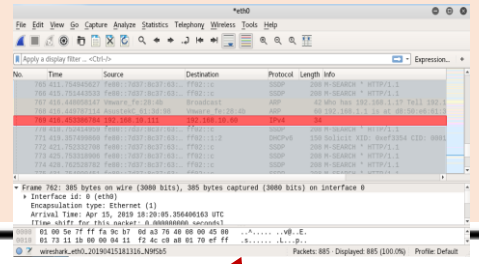
ОСУЩЕСТВЛЕНИЕ КОМПЬЮТЕРНОЙ АТАКИ НА ПРОТОКОЛ OSPF

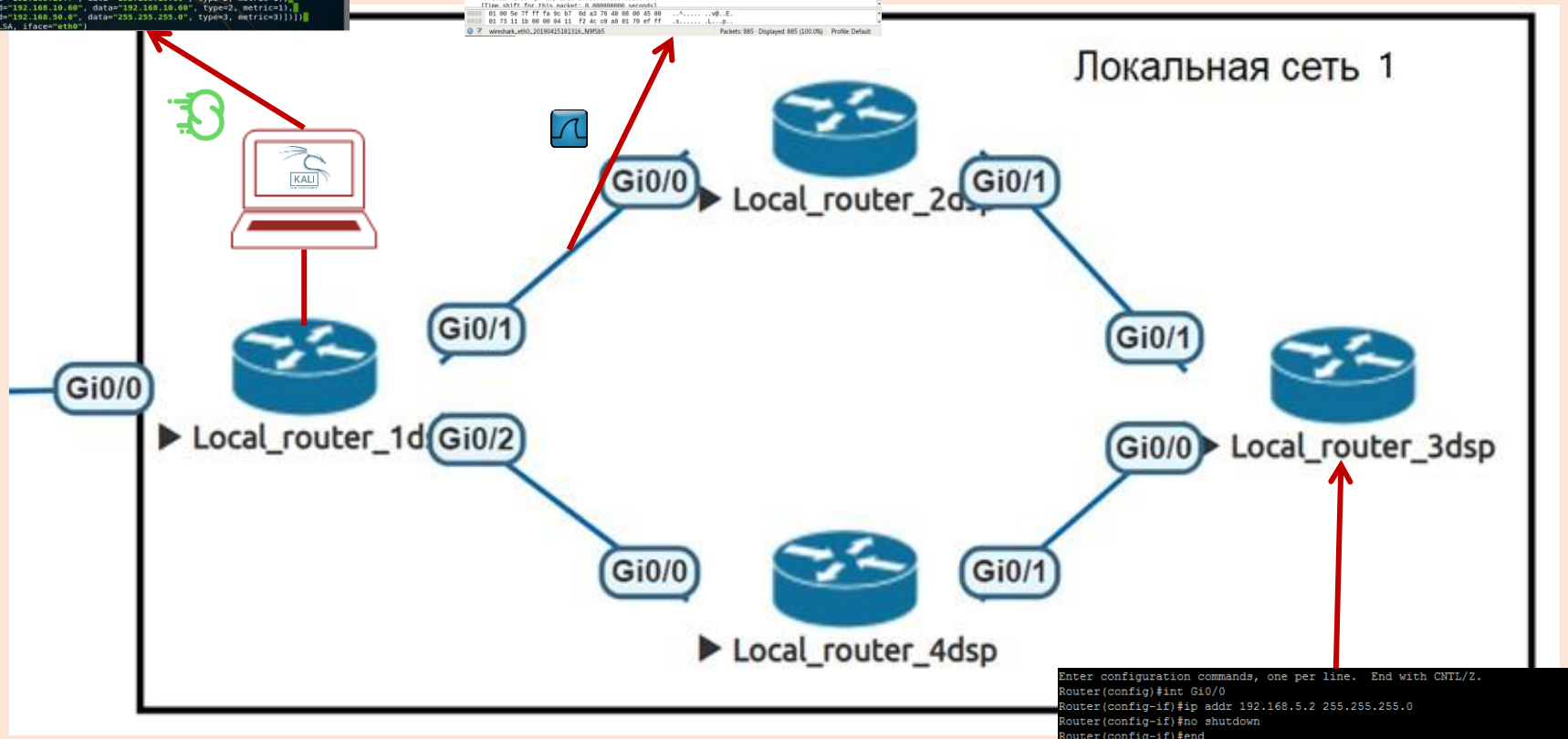
1. Создание ложного пакета LSA
2. Отправление пакета в локальную сеть

1.



2.





3. Изменение таблицы маршрутизации на атакуемом маршрутизаторе

3.

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int Gi0/0
Router(config-if)#ip addr 192.168.5.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#end
Router#ping 192.168.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/8/18 ms
Router#ping 192.168.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/5 ms
Router#
```

ВЫВОДЫ

Для оценки защищенности алгоритмов маршрутизации трафика АС была разработана имитационная модель, в которой были проведены КА на протоколы маршрутизации в локальной сети, а также осуществлена оценка защищенности алгоритмов маршрутизации, до и после применения встроенных механизмов защиты протоколов маршрутизации. Разработанная имитационная модель, за счет виртуального моделирования АС, в частности настройки протоколов маршрутизации на сетевом оборудовании, позволяет осуществить анализ защищенности АС, без наличия сетевого оборудования в максимально короткое время.

Спасибо за внимание