



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А.Н. Земцов, А.А. Турицын, Чан Зунг Хань

МОДЕРНИЗАЦИЯ СЕТИ КРЕДИТНОЙ ОРГАНИЗАЦИИ НА ОСНОВЕ ТЕХНОЛОГИИ DMVPN

(Волгоградский государственный технический университет)

В последнее время в кредитных организациях, осуществляющих финансово-кредитную деятельность на территории Российской Федерации наметился переход от традиционного документооборота к системам с электронной формой представления документов, вызванный, в том числе, необходимостью организации дистанционного взаимодействия между различными структурными подразделениями кредитных организаций [1], а также ужесточением требований к эффективности работы различных предлагаемых сервисов [2].

Перманентное увеличение количества киберпреступлений, в том числе, с участием кредитных организаций, приводит к ужесточению требований к уровню защищенности инфокоммуникационных систем кредитных организаций. Как следствие, растет актуальность поиска новых методов, средств и информационных технологий для повышения уровня защищенности информационно-коммуникационных систем такого рода.

К настоящему времени был разработан ряд подходов для обеспечения отказоустойчивости информационной безопасности сети, для чего используются различные методы повышения эффективности планирования передачи пакетов между филиалами кредитных организаций, а также методы туннелирования и шифрования трафика [3-5]. Подобный подход позволяет обеспечить возможность взаимодействия между сетями филиалов кредитных организаций, использующих различные протоколы, а также обеспечить конфиденциальность и целостность передаваемых данных, включая служебные поля заголовков пакетов.

Для достижения поставленной цели необходимо выполнить проектирование информационно-коммуникационной сети для организации сетевого взаимодействия филиалов через сеть Интернет с использованием следующих протоколов туннелирования: GRE, IPSec, GRE over IPSec и DMVPN, включая NHRP, mGRE, IPSec, OSPF, EIGRP.

Технология Cisco Systems DMVPN (Dynamic Multipoint Virtual Private Network) позволяет создавать динамические виртуальные частные сети с множественным подключением. DMVPN является дальнейшим развитием технологии VPN, и основывается на совместной работе протоколов разрешения



шлюза NHRP, протокола туннелирования mGRE, протокола шифрования IPsec и протоколов динамической маршрутизации: OSPF, ODR, RIP, EIGRP, BGP. Клиент связывается с DMVPN сервером и получает от того данные конечной точки сетевого взаимодействия, после чего между ними создаётся виртуальный туннель.

До утверждения и внедрения разработанного проекта предлагается выполнить анализ результатов на модели рассматриваемых информационно-коммуникационных систем. При построении моделей информационно-коммуникационных систем перед исследователем возникает вопрос, какой системой моделирования воспользоваться для построения своей модели, для чего был выбран эмулятор сети GNS3/Dynamips, позволяющий имитировать работу аппаратных средств реального маршрутизатора, путем загрузки и взаимодействия с реальными образами операционных систем основных производителей сетевых устройств Cisco, Mikrotik, Juniper., а также возможности подключения к внешней сети. Прототип информационно-коммуникационной системы показана на рисунке 1.

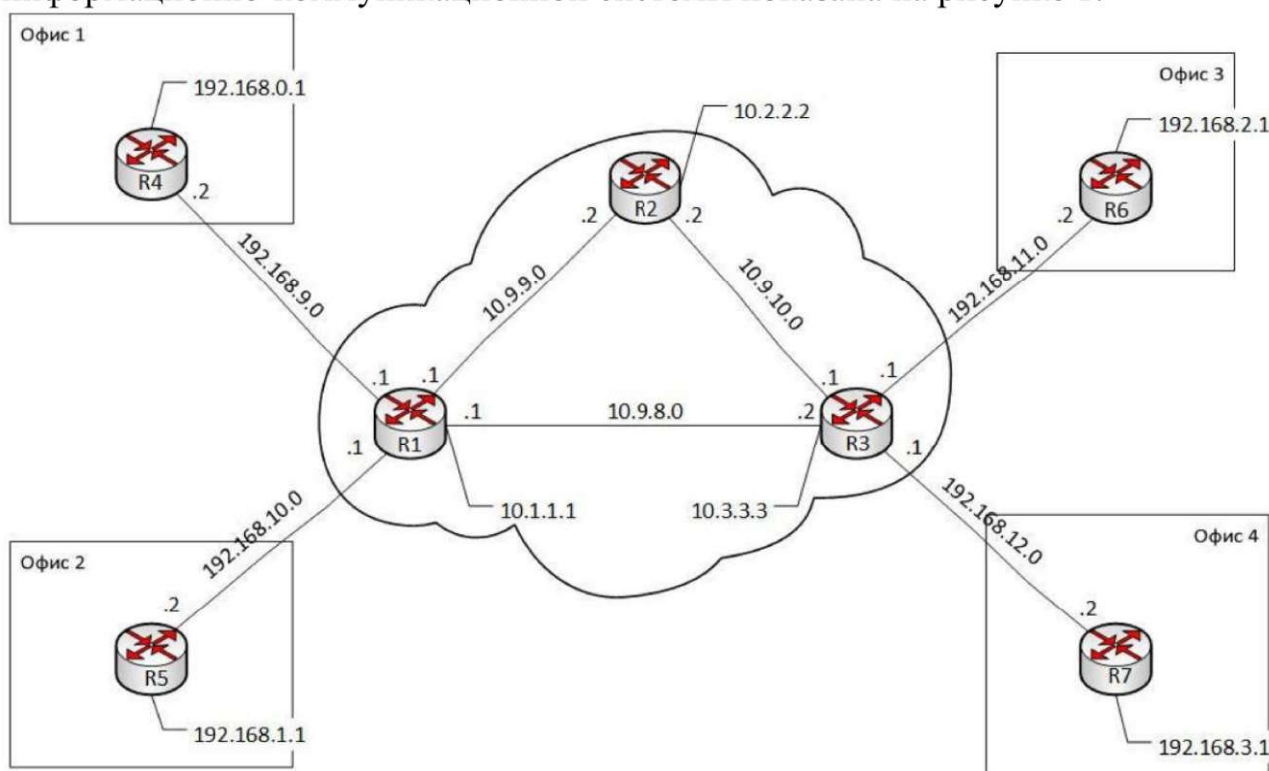


Рис. 1. Прототип информационно-коммуникационной системы

Для конфигурирования технологии DMVPN необходимо выполнить конфигурирование mGRE-туннелей, конфигурирование протоколов NHRP и IPsec, заключающееся в создании политики безопасности isakmp, и настройки профиля IPsec, а также сконфигурировать протокол динамической маршрутизации.

Проверим доступность маршрутизаторов, а также проанализируем информацию о других маршрутизаторах, полученную с помощью NHRP, как показано на рисунке 2.



```
R5#ping 192.168.100.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/52/80 ms
R5#sh ip nhrp brief
      Target                Via                NBMA                Mode    Intfc    Claimed
192.168.100.2/32          192.168.100.2      192.168.9.2         dynamic Tu1    <    >
192.168.100.3/32          192.168.100.3      192.168.11.2        dynamic Tu1    <    >
192.168.100.4/32          192.168.100.4      192.168.12.2        dynamic Tu1    <    >
R5#
```

Рис. 2. Передача пакетов и краткая таблица NHRP

По окончании выполнения конфигурирования DMVPN на сетевом оборудовании, необходимо выполнить проверку правильности функционирования защищенной информационно-коммуникационной системы. Проверка доступности узлов сети осуществлялась с помощью команд ping и traceroute. Для анализа правильности примененных настроек будем осуществлять перехват трафика с помощью sniffера Wireshark, как показано на рисунке 3.

No.	Time	Source	Destination	Protocol	Length	Info
355	1450.254110	172.16.251.0	172.16.200.1	ICMP	138	Echo (ping) reply id=0x0002, seq=0/0, ttl=255 (request in 354)
356	1450.264110	172.16.200.1	172.16.251.0	ICMP	138	Echo (ping) request id=0x0002, seq=1/256, ttl=255 (reply in 359)
357	1450.264110	c4:04:30:98:00:00	c4:04:30:98:00:00	LOOP	60	Reply
358	1450.274110	c4:02:38:44:00:00	c4:02:38:44:00:00	LOOP	60	Reply
359	1450.294110	172.16.251.0	172.16.200.1	ICMP	138	Echo (ping) reply id=0x0002, seq=1/256, ttl=255 (request in 356)
360	1450.304110	172.16.200.1	172.16.251.0	ICMP	138	Echo (ping) request id=0x0002, seq=2/512, ttl=255 (reply in 361)
361	1450.334110	172.16.251.0	172.16.200.1	ICMP	138	Echo (ping) reply id=0x0002, seq=2/512, ttl=255 (request in 360)
362	1450.344110	172.16.200.1	172.16.251.0	ICMP	138	Echo (ping) request id=0x0002, seq=3/768, ttl=255 (reply in 363)
363	1450.374110	172.16.251.0	172.16.200.1	ICMP	138	Echo (ping) reply id=0x0002, seq=3/768, ttl=255 (request in 362)
364	1450.384110	172.16.200.1	172.16.251.0	ICMP	138	Echo (ping) request id=0x0002, seq=4/1024, ttl=255 (reply in 365)
365	1450.414110	172.16.251.0	172.16.200.1	ICMP	138	Echo (ping) reply id=0x0002, seq=4/1024, ttl=255 (request in 364)
366	1459.138205	c4:02:38:44:00:00	c4:02:38:44:00:00	LOOP	60	Reply
367	1459.838206	c4:04:30:98:00:00	c4:04:30:98:00:00	LOOP	60	Reply
368	1466.178215	c4:04:30:98:00:00	CDP/VTP/DTP/PAGP/UD...	CDP	365	Device ID: Internet Port ID: FastEthernet0/0
369	1469.008219	c4:02:38:44:00:00	c4:02:38:44:00:00	LOOP	60	Reply
370	1469.918221	c4:04:30:98:00:00	c4:04:30:98:00:00	LOOP	60	Reply


```

> Frame 363: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
> Ethernet II, Src: c4:04:30:98:00:00 (c4:04:30:98:00:00), Dst: c4:02:38:44:00:00 (c4:02:38:44:00:00)
> Internet Protocol Version 4, Src: 2.2.2.1, Dst: 1.1.1.1
  * Generic Routing Encapsulation (IP)
    * Flags and Version: 0x0000
      0... .. = Checksum Bit: No
      .0.. .. = Routing Bit: No
      ..0. .... = Key Bit: No
      ...0 .... = Sequence Number Bit: No
      ....0... .. = Strict Source Route Bit: No
      ....0000 .... = Recursion control: 0
      .... ..0000 0... = Flags (Reserved): 0
      .... ..0000 = Version: GRE (0)
    Protocol Type: IP (0x0800)
  > Internet Protocol Version 4, Src: 172.16.251.0, Dst: 172.16.200.1
  > Internet Control Message Protocol

```



```

0000  c4 02 38 44 00 00 c4 04 30 98 00 00 08 00 45 00  ..8D... 0....E.
0010  00 7c 00 0d 00 00 fe 2f b6 41 02 02 02 01 01 01  ..|...../ .A.....
0020  01 01 00 00 08 00 45 00 00 64 00 0d 00 00 ff 01  ..E. .d.....
0030  a0 68 ac 10 fb 00 ac 10 c8 01 00 00 6e 68 00 02  ..h..... .nh..
0040  00 03 00 00 00 00 00 1d 17 c0 ab cd ab cd ab cd  ..
0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ..
0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ..
0070  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ..
0080  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  ..

```

Рис. 3. Анализ трафика в Wireshark



Литература

1. Лавриченко, О.В. Управление инновационными системами промышленных предприятий и разработка модели их классификации / Лавриченко О.В. // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2014. Т. 14. № 4. С. 10.
2. Земцов А.Н., Болгов Н.В., Божко С.Н. Многокритериальный выбор оптимальной системы управления базы данных с помощью метода анализа иерархий // Инженерный вестник Дона, 2014, №2. URL: <http://ivdon.ru/ru/magazine/archive/n2y2014/2360>.
3. Земцов А.Н., Ньяти Р.С. Моделирование и оценка показателей надежности и отказоустойчивости систем связи // Инженерный вестник Дона, 2019, №4. URL: <http://ivdon.ru/ru/magazine/archive/N5y2019/5995>.
4. Земцов А.Н., Чан Зунг Хань. Анализ эффективности алгоритмов планирования передачи пакета в сетях LTE // Инженерный вестник Дона, 2019, №4. URL: <http://ivdon.ru/ru/magazine/archive/n4y2019/5840>.
5. Земцов А.Н., Чан Зунг Хань. О повышении доступности шлюза по умолчанию в корпоративных сетях // Инженерный вестник Дона, 2019, №9. URL: <http://ivdon.ru/ru/magazine/archive/N9y2019/6243>.

А.Н. Земцов, В.Ю. Цыбанов

РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ЗАЩИТЫ ИЗОБРАЖЕНИЙ МЕТОДАМИ ЦИФРОВОЙ СТЕГАНОГРАФИИ

(Волгоградский государственный технический университет)

В последние годы в Российской Федерации наметился переход от традиционного документооборота к системам с электронной формой представления документов, вызванный, в том числе, необходимостью организации дистанционного взаимодействия между различными структурными подразделениями, коммерческих предприятий и государственных учреждений, что позволило повысить их производительность [1], а также реализовать комплекс концептуальных подходов и методов к оптимизации этого процесса [2].

Задача защиты изображений была актуальна с момента появления изображений, но методы защиты изображений появились относительно недавно. Актуальность разработки программных средств для защиты изображений методами цифровой стеганографии объясняется интенсивным расширением спектра атак и их возможных последствий на мультимедийные системы, а также мультимедийный контент традиционных информационных систем. Необходимо отметить, что традиционные методы защиты электронных документов являются неэффективными для защиты мультимедийных систем.