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 Для работы 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.

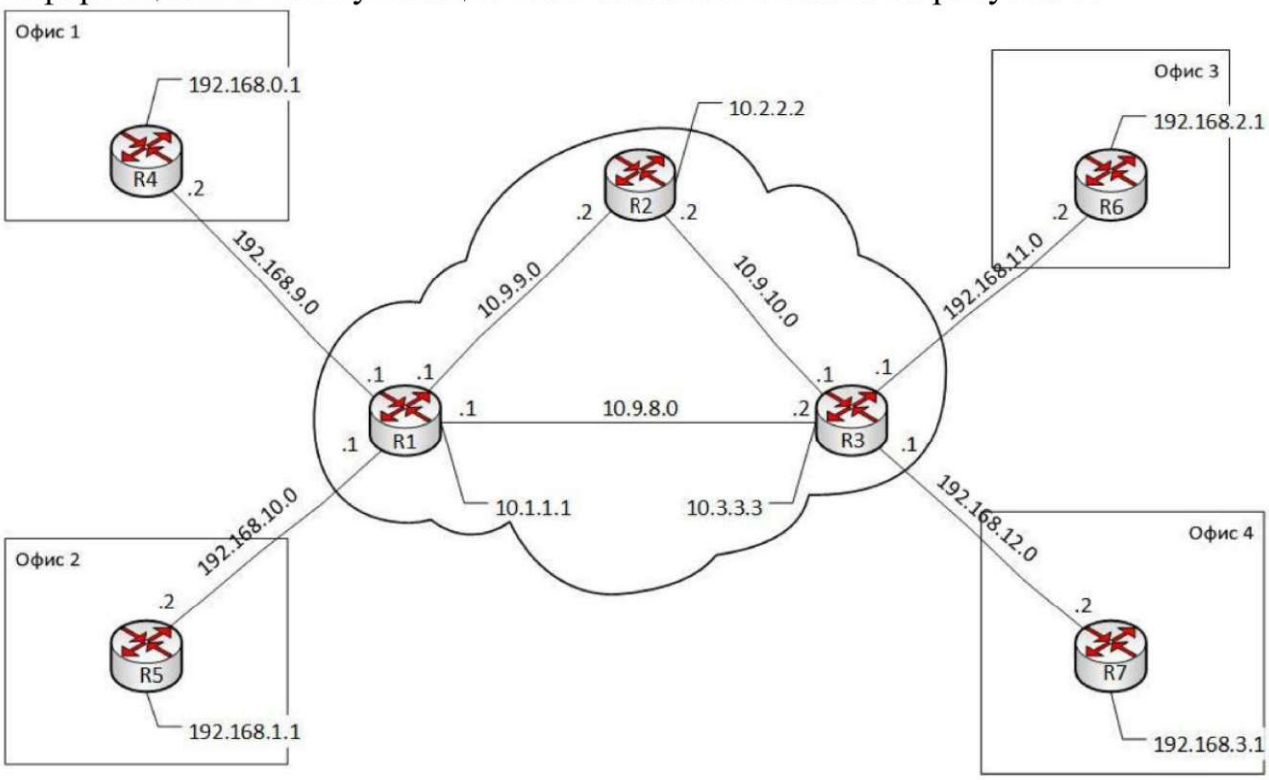

Рис. 1. Прототип информационно-коммуникационной системы

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 tracert traceroute. Для анализа правильности примененных настроек будем осуществлять перехват трафика с помощью сниффера Wireshark, как показано на рисунке 3.

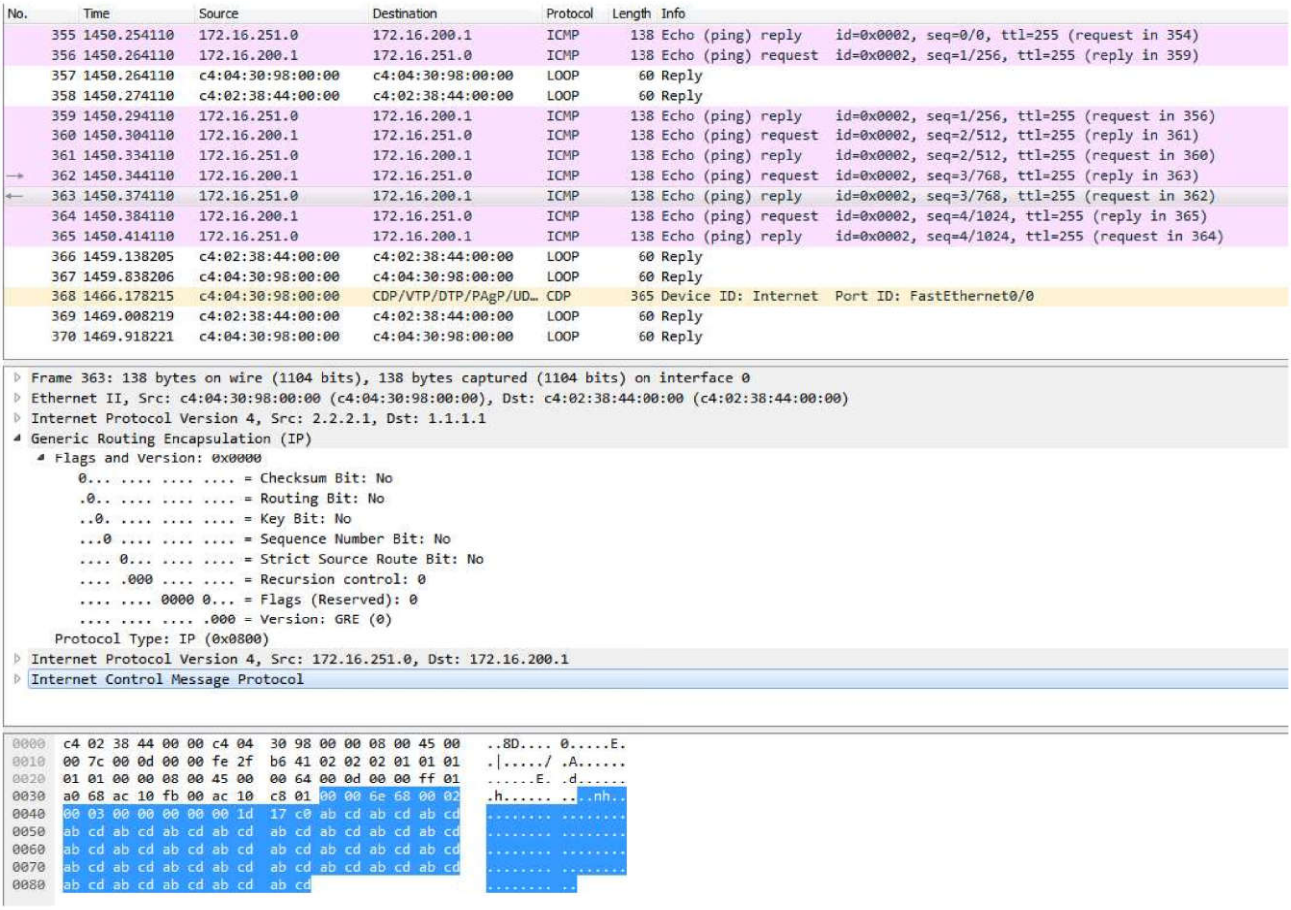

Рис. 3. Анализ трафика в Wireshark

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.