ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 621.391

ХАРАКТЕРИСТИКИ КАЧЕСТВА ЗАЩИЩЕННЫХ РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА БАЗЕ КОМПЛЕКСА «ФПСУ-IP»

А.О. Куприянов, О.В. Чечуга, С.Ю. Борзенкова

Приводятся результаты измерений и на их основе оценка степени влияния на характеристики производительности распределённых информационных сетей при применении в качестве средств защиты комплексов «ФПСУ-IP» Результаты могут быть использованы при разработке технического задания на проектирование защищённых распределённых сетей.

Ключевые слова. безопасность информации. средство криптографической защиты информации. защищённые информационно-телекоммуникационные системы.

В настоящее время становится всё более актуальной задача создания в организациях и на предприятиях эффективных информационных систем. В условиях информационного общества успешная реализация различных бизнес-проектов, организация бизнес-процессов практически невозможна без развитой информационной среды, обеспечивающей доступность необходимых данных, их целостность, а при необходимости и их конфиденциальность, юридическую значимость, актуальность, полноту и другие свойства информации. Многие предприятия создают территориально-распределённые информационные системы, что, в первую очередь, обусловлено необходимостью создания рабочих мест по предоставления услуг ближе к потенциальным заказчикам, обеспечением удалённого доступа к информационным ресурсам для своих сотрудников, созданием филиалов в других регионах и городах. Для осуществления взаимодействия между территориально-распределёнными сегментами в таких информационных системах, как правило, используются информационно-телекоммуникационные сети общего пользования, в том числе сеть Интернет.

Современные телекоммуникационные сети позволяют обеспечить скоростной удалённый доступ к информационным ресурсам организаций и предприятий или, например, размещённых на серверах в центрах обработки данных (ЦОД), предоставляющих услуги облачных вычислений. Однако использование общедоступных сетей связи для создания территориаль-но-распределённых информационных систем не гарантирует

обеспечение таких свойств передаваемой информации, как конфиденциальность и целостность.

Решение этой проблемы успешно реализуется применением виртуальных наложенных сетей, построенных с использованием криптографических средств защиты информации. В данной статье описан опыт применения программно-аппаратного комплекса ФПСУ-IP компании Амикон. Пример реально развёрнутой на базе комплекса ФПСУ-IP защищённой распределённой корпоративной сети приведён на рис. 1.

Комплексы ФПСУ-IP были установлены в трёх территориально разнесенных сегментах сети (в г. Zzz, г. Xxx и в г. Yyy) в разрыв сети, между коммутатором ЛВС и каналообразующим маршрутизатором. В защищаемых сетях установлены рабочие станции, обменивающиеся данными по протоколу TCP/IP. В сегменте Zzz установлена станция Удаленного администрирования ФПСУ. Кроме того к центральному ФПСУ-IP подключены удалённые рабочие места.

В течение достаточно длительной эксплуатации комплексов (более года) появились некоторые субъективные оценки качества работы защищённой вычислительной сети:

- задержки передачи данных между офисами не увеличились;
- трафик устойчив, передаётся надёжно;
- передача множества файлов небольшого размера, составляющих в совокупности достаточно большой объём, осуществляется быстрее, чем передача одного файла большого размера равным общему объёму множества файлов небольшого размера;
- нормальная работа с удалённых рабочих мест (ощущение присутствия на рабочем месте в офисе) обеспечивается при доступе к Интернет со скоростью не менее 2 Мбит в сек;
- при передачи файлов большого размера с удаленных рабочих мест имелись случаи сбоя VPN-клиента, последствием которого был разрыв VPN-соединения удалённого рабочего места вычислительной сетью головного офиса.

Для представления объективных характеристик качества (производительности) защищённой виртуальной наложенной сети, созданной с применением комплекса «ФПСУ-IP», были применены инструментальные и статистические методы. Измеряемыми параметрами при проведении тестовых испытаний являлись следующие статистические характеристики производительности сети:

- характеристики задержек пакетов (среднее значение задержки, джиттер, коэффициент вариации, максимальная задержка, максимальная вариация задержки, время реакции сети);

- характеристики скорости передачи (скорость передачи данных, средняя скорость передачи данных, пиковая скорость передачи данных, величина пульсации);
- характеристики потерь пакетов (доля потерянных пакетов).

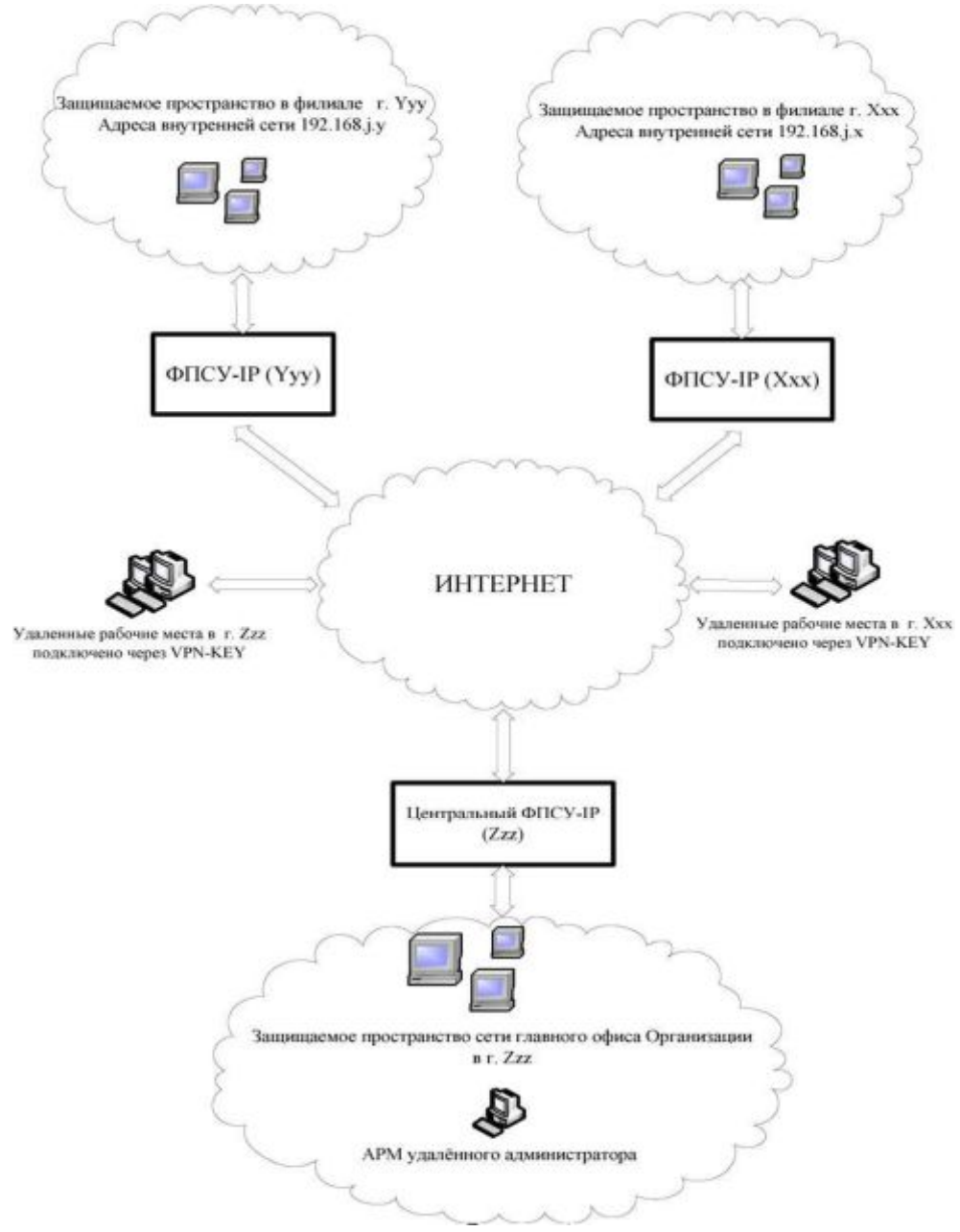

Рис. 1. Блок-схема защищенной телекоммуникационно -информационной системы

С целью измерения характеристик качества передачи трафика были организованы испытательные стенды. Схемы испытательных стендов представлены на рисунках 2 (вариант 1) и 3 (вариант 2).

Рис. 2. Схема макета сегмента вычислительной сети, имитирующего передачу данных через незащищённый канал

Рис. 3. Схема макета сегмента вычислительной сети, имитирующего передачу данных через защищенный канал

Для построения макетов использовались программно-аппаратные комплексы «ФПСУ-IP» с характеристиками, приведёнными в таблице № 1.

Таблица 1

<u>Краткие характеристики комплекса «ФПСУ-IP»</u>

№ п.п.	Описание характеристик	Параметры
	Операционная система	Linux x86 32 бит
	Максимальная скорость шифрования для одного вычислительного потока.	до 100 Мбит/с, при размере IP-пакета 1450 байт
	Кол-во стандартно задействованных вычислительных потоков	1
	Дополнительные вычислительные потоки.	Недоступны
	Сертификат ФСБ	КС1,КС2
	Сертификат ФСТЭК	Межсетевой экран 3-го класса

При проведении измерений применялись программные средства, приведенные в табл. 2.

Таблица 2

Наименования средства измерения	**Краткая характеристика**	**Примечание**
Утилита для проверки соединений в сетях на основе TCP/IP «Ping»	Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP к указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT, от англ. Round Trip Time) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах	Входит в состав операционной системы, установленной на АРМах
Кроссплатформенная консольная клиент-серверная программа «Iperf»	Генератор TCP и UDP трафика для тестирования пропускной способности сети	Лицензия: GNU General Public License. Сайт программы: iperf.fr
Утилита LAN Speed Test (Lite) v1.3.1	Измерение скорости приема и передачи файлов в сети	http://www.totusoft.com/downloads. html
Служебная программа «Traceroute»	Определение маршрутов следования данных в сетях TCP/IP	Входит в состав операционной системы, установленной на АРМах

Инструментальные программные средства

Полученные результаты измерений приведены в табл. 3 - 5.

Таблица 3

Результаты измерений утилитой «ping» и расчёты

Параметры запуска программы	**Вариант испыта-ний**	**Количество потерянных пакетов**	**Время приёма-передачи, мсек.**			**J мсек**	**CV**
			мини-мальное	**макси-мальное**	**среднее**		
ping -n 200 -l 32 192.168.0.16	**1**	**0**	**< 1**	**1**	**< 1**	**0**	**0**
ping -n 200 -l 32 192.168.0.16	**2**	**0**	**1**	**9**	**1**	**1,9**	**1,9**
ping -n 200 -l 60000 192.168.0.16	**1**	**0**	**11**	**13**	**11**	**0,3**	**0,027**
ping -n 200 -l 60000 192.168.0.16	**2**	**0**	**43**	**55**	**43**	**2,22**	**0,05**

Из табл. 3 видно, что при передаче пакетов среднее значение задержки для варианта 2 увеличилось более чем в три раза, а среднее отклонение каждой отдельной задержки от среднего значения задержки увеличилось почти два раза. Доля потерянных пакетов равна нулю.

Таблица 4

Результаты измерений программой «iperf»

Параметры запуска программы	**Вариант испытаний**	**Время передачи, сек.**	**Объём переданных данных, МБ**	**Средняя скорость передачи, Мбит/сек.**
iperf -c 192.168.0.16	1	10	67,9	57
iperf -c 192.168.0.16	2	10	47,6	39,9
iperf -n 500M -l 8K -c 192.168.0.16	1	68,7	500	61
iperf -n 500M -l 8K -c 192.168.0.16	2	90.7	500	46.2
iperf -n 500M -l 16K -c 192.168.0.16	1	44,9	500	93,5
iperf -n 500M -l 16K -c 192.168.0.16	2	46.4	500	90.4
iperf -n 500M -l 32K -c 192.168.0.16	1	44,9	500	93,5
iperf -n 500M -l 32K -c 192.168.0.16	2	46.4	500	90.4
iperf -n 500M -l 64K -c 192.168.0.16	1	41,5	500	93
iperf -n 500M -l 64K -c 192.168.0.16	2	46.4	500	90.5

Таблица 5

Результаты измерений применением утилиты LAN Speed Test

Коли-чество прини-маемы х (пере-да ваe-мых) файлов	**Раз-мер фай-лов, МБ**	**Вариант испытаний**	**Время пе-редачи од-ного файла, сек**	**Время чтения одного файла, сек**	**Общее время передачи, сек**	**Общее время чтения, сек**	**Ско-рость пере-дачи, Мбит/ сек**	**Скорость чтения, Мбит/ сек**
500	1	1	0,0878704	0.0887419	43.9351776	44.3709719	91	90,1
500	1	1	0,0879816	0.0886144	43.9908101	44.3071926	90,9	90,2
500	1	2	0,0924669	0.0905975	46.2334636	45.2987561	86,5	88,3
500	1	2	0,0925584	0.0903049	46.2792011	45.152459	86,4	88,5
1	500	1	43,7138838	44.4220905	43.7138838	44.4220905	91,5	90
1	500	1	43,7196064	44.5070361	43.7196064	44.5070361	91,5	89,8
1	500	2	46,1193363	45.2688449	46.1193363	45.2688449	86,7	88,3
1	500	2	46,147057	45.3261713	46.147057	45.3261713	86,6	88,2

Средняя скорость при передаче файлов с длиной пакетов данных малого размера менее 16 Кб значительно уменьшается - на 30 %, а при передаче файлов с длиной пакетов 16 Кб и более средняя скорость уменьшается не более чем на 5%.

Измерения на реально действующей распределённой информационно-телекоммуникационной сети (рис. 1) проводились по той же методике. Результаты измерений приведены в таблицах 6-8. Упрощённые схемы вариантов макетов сети для тестирования приведены на рис. 4 и 5.

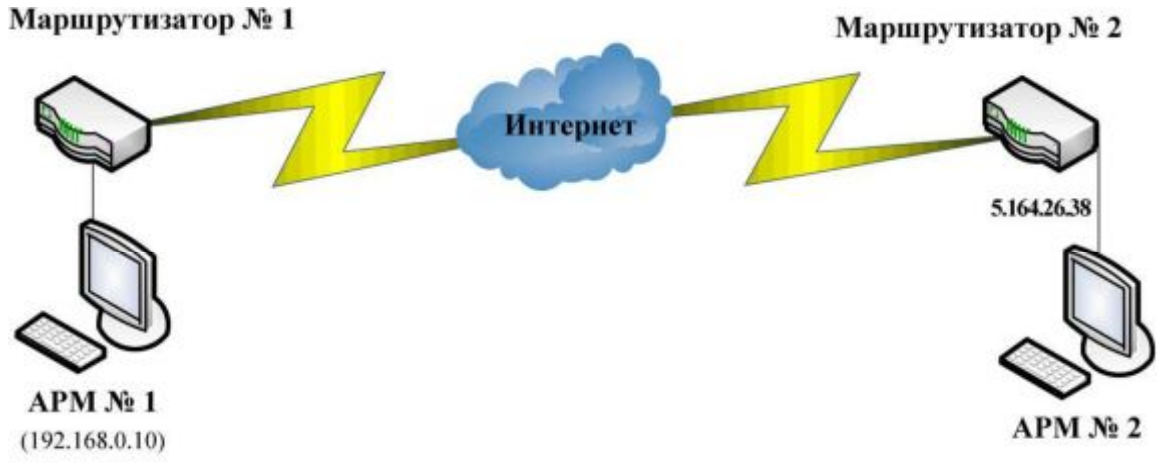

Рис. 4. Схема макета сегмента телекоммуникационно-информационной системы, имитирующего передачу данных через незащищённый канал

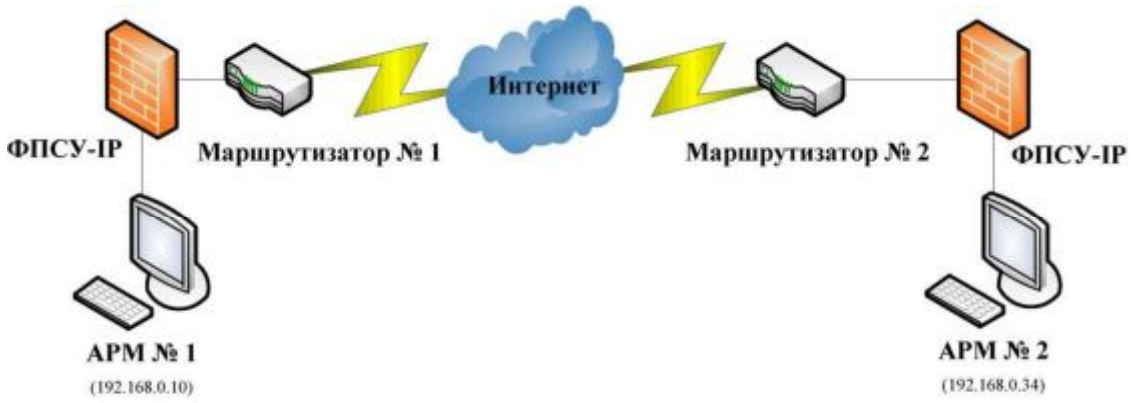

Рис. 5. Схема макета сегмента телекоммуникационно-информационной системы, имитирующего передачу данных через защищённый канал

Таблица 6

Результаты измерений и расчётов

Параметры запуска программы	Вариант испытаний	Количество потерянных пакетов	Время приёма-передачи, мсек.			J, мсек	CV
			минимальное	максимальное	среднее		
ping -n 200 -l 32 5.164.26.38	**1**	**0**	**6**	**303**	**24**	**46,1**	**1,9**
ping -n 200 -l 32 192.168.0.34	**2**	**0**	**9**	**239**	**32**	**31,02**	**0,97**
ping -n 200 -l 5000 5.164.26.38	**1**	**0**	**31**	**350**	**83**	**77,88**	**0,94**
ping -n 200 -l 5000 192.168.0.34	**2**	**1**	**34**	**237**	**45**	**24,5**	**0,54**

Таблица 7

Результаты испытаний

Параметры запуска программы	Схема испытаний	Время передачи, сек.	Объём переданных данных, МБ	Средняя скорость передачи, Мбит/сек.
iperf -c 192.168.0.34	**1**	**10**	**1,03**	**0,834**
iperf -c 192.168.0.34	**2**	**10**	**1,016**	**0,812**
iperf -n 500M -c 192.168.0.34	**1**	**1585**	**150**	**0,794**
iperf -n 500M -c 192.168.0.34	**2**	**1551,6**	**150**	**0,811**

Таблица 8

Результаты испытаний

Количество принимаемых-передаваемых файлов	Размер файлов, МБ	Схема испытаний	Время передачи одного файла, сек	Время чтения одного файла, сек	Общее время передачи, сек	Общее время чтения, сек
200	**1**	**1**	**9,6795937**	**2,3540883**	**1 935,918737**	**470,8176596**
200	**1**	**2**	**9,7089458**	**2,0190807**	**1 941,789150**	**403,8161339**
1	**200**	**1**	**2 091, 832319**	**364,0628138**	**2091,832319**	**364,0628138**
1	**200**	**2**	**2 020, 693691**	**606,1998629**	**2 020,693691**	**606,1998629**

По результатам измерений установлено, что средняя скорость передачи данных через реальный канал связи (при передачи данных через Интернет) с использованием комплекса «ФПСУ-IP» уменьшается не более

чем 5%, а среднее значение задержки пакетов увеличилось незначительно. Установлено, что шифрованный канал работает стабильнее (среднее отклонение каждой отдельной задержки от среднего значения задержки уменьшилось).

Список литературы

1. Олифер В.Г. , Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 4-ое изд. СПб.: Питер, 2010. 940 с.

2. ООО «Амикон», ООО «Фирма «Инфокрипт». Средство криптографической защиты информации «ТУННЕЛЬ 2.0». Программно-аппаратный комплекс «ФПСУ-IP». Межсетевой экран "ФПСУ-IP" r.2.61. Руководство администратора. 36567521.4012.003-03 94. 122 с.

3. Борзенкова С.Ю., Чечуга О.В., Селищев В. А Модель ситуативного управления при организации системы защиты информации. Известия ТулГУ. Технические науки. Вып.3: Тула: Изд-во ТулГУ, 2013. С.471-478.

Куприянов Александр Олегович, генеральный директор, Россия, Москва, Общество с ограниченной ответственностью «Научно-технический центр «ВЕЛЕС»,

Чечуга Ольга Владимировна, канд. техн. наук, доц., tppzi@tsu.tula.ru, Россия, Тула, Тульский государственный университет,

Борзенкова Светлана Юрьевна, канд. техн. наук, доц., tppzi@tsu.tula.ru, Россия, Тула, Тульский государственный университет

CHARACTERISTICS OF QUALITY OF THE PROTECTED DISTRIBUTED INFORMATION SYSTEMS ON THE BASIS OF THE FPSU-IP COMPLEX

A. O. Kupriaynov, O. V. Chechuga, S. Y. Borzenkova

The results of the measurements and on the basis of their assessment of the degree of influence on the performance of distributed information networks when used as a means of protection systems «FPSU-IP». Results can be used when developing the specification on design of the protected distributed networks.

Key words: information security, cryptographic information protection facility, the protected information and telecommunication systems.

Kupriaynov Alexander Olegovich, General Director, Russia, Moscow, limited liability Company «Scientific and technical center «VELES»

Chechuga Olga Vladimirovna, candidate of technical sciences, docent, tppzi@tsu.tula.ru, Russia, Tula, Tula State University,

Borzenkova Svetlana Yurevna, candidate of technical sciences, docent, tppzi@tsu.tula.ru, Russia, Tula, Tula State University