СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ МОНИТОРИНГА, СБОРА И ОБРАБОТКИ СТАТИСТИКИ ДЛЯ ЗАЩИЩЕННОЙ КОРПОРАТИВНОЙ СЕТИ КНИТУ

CREATING AN AUTOMATED SYSTEM FOR MONITORING, COLLECTION AND PROCESSING STATISTICS FOR A PROTECTED CORPORATE NETWORK KNITU

V. Bogomolov
I. Pervuhin

Summary. The article discusses the creation of an automated system for monitoring, collecting and processing statistics of a protected corporate network of the Kazan National Research Technological University (KNRTU), created on DionisNX national crypto routers, and is a training and testing ground based on the KNITU corporate network. For complete control of the network status, it was necessary to create an automated system for monitoring, collecting and processing statistics. The article describes in detail the system of monitoring and collecting statistics.

Keywords: Crypto routers, corporate networks, import substitution, firewall, virtual private networks, high-availability clusters, training ground, testing software and hardware systems, DionisNX, secure channels, protected networks, network security, Nagios, MRTG, monitoring, statistics collection.

Богомолов Владислав Афанасьевич
К.т.н., доцент, Казанский национальный исследовательский технологический университет
vladbogomolov72@mail.ru
Первухин Илья Дмитриевич
К.т.н., главный электроник, Казанский национальный исследовательский технологический университет
pervuhin@kstu.ru

Аннотация. В статье рассматривается создание автоматизированной системы для мониторинга, сбора и обработки статистики защищенной корпоративной сети Казанского национального исследовательского технологического университета (КНИТУ), созданной на отечественных крипто-маршрутизаторов DionisNX, и является учебно-испытательным полигоном на базе корпоративной сети КНИТУ. Для полного контроля состояния сети необходимо было создать автоматизированную систему для мониторинга, сбора и обработки статистики. В статье подробно рассмотрена созданная система мониторинга и сбора статистики, и приведен анализ собранной статистики.

Ключевые слова: Крипто-маршрутизаторы, корпоративные сети, импортозамещение, межсетевые экраны, виртуальные частные сети, отказоустойчивые кластеры, учебный полигон, тестирование программно-аппаратных комплексов, DionisNX, защищенные каналы, защищенные сети, безопасность сетей, Nagios, MRTG, мониторинг, сбор статистики.

Введение

В работе изложен опыт создания автоматизированной системы для мониторинга, сбора и обработки статистики для работающего прототипа защищенной сети на базе модернизированной корпоративной сети КНИТУ. После модернизации корпоративной сети КНИТУ были использованы криптомаршрутизаторы Dionis-NX. Криптомаршрутизаторы требуются для защиты информации при передаче по открытым каналам связи [1]. Теперь корпоративная сеть КНИТУ может использоваться для имитационного моделирования нагрузки, атак и защиты сети [2–4].

Для полного контроля состояния сети необходимо было создать автоматизированную систему для мониторинга, сбора и обработки статистики.

Цель и задачи

Цель данной работы — создать автоматизированную систему для мониторинга, сбора и обработки статистики в корпоративной сети КНИТУ и протестировать в реальной эксплуатации работающий прототип защищенной сети передачи данных с использованием криптомаршрутизаторов на базе корпоративной сети КНИТУ.

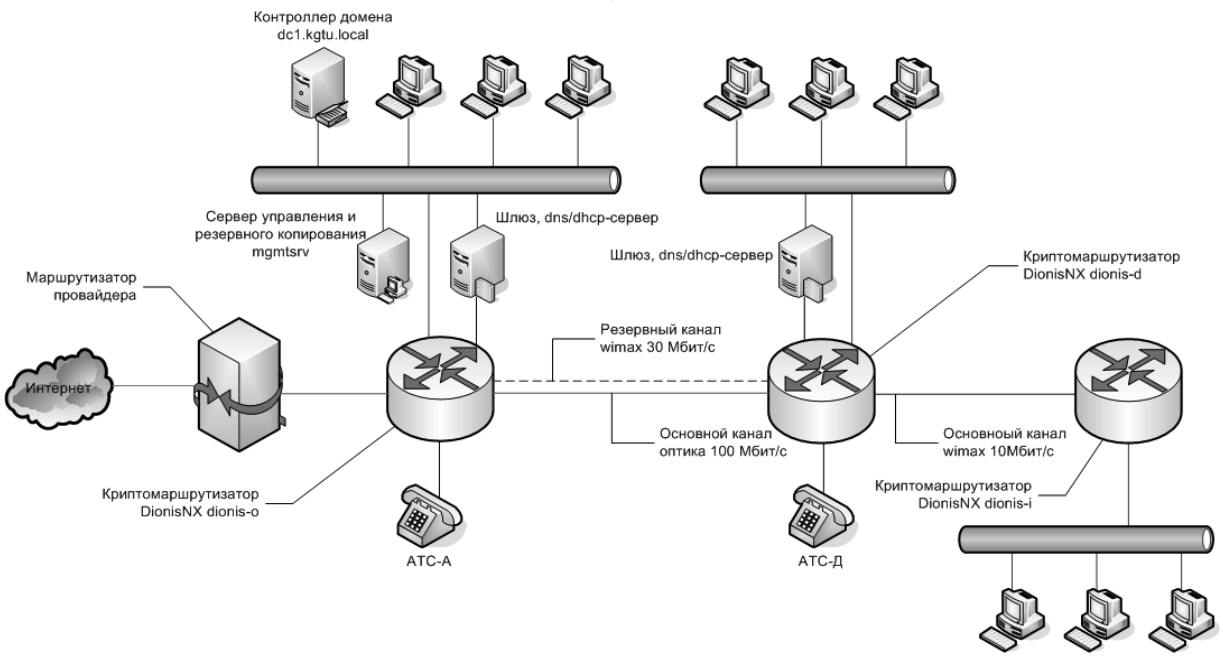
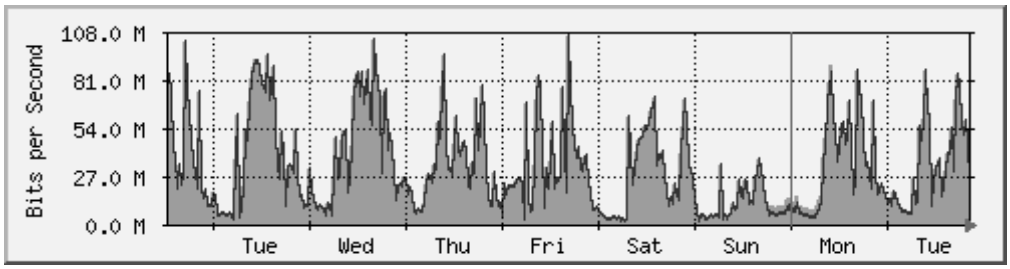
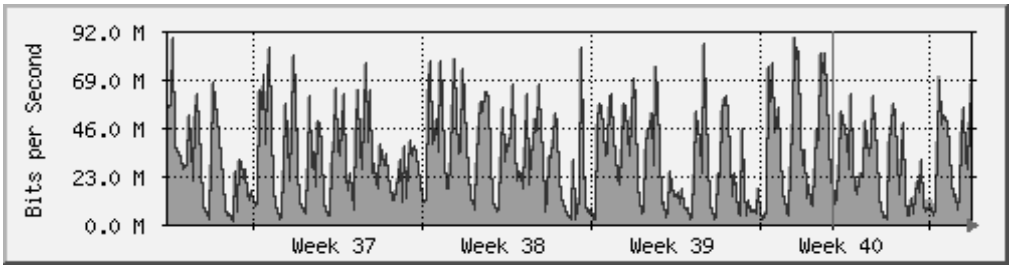


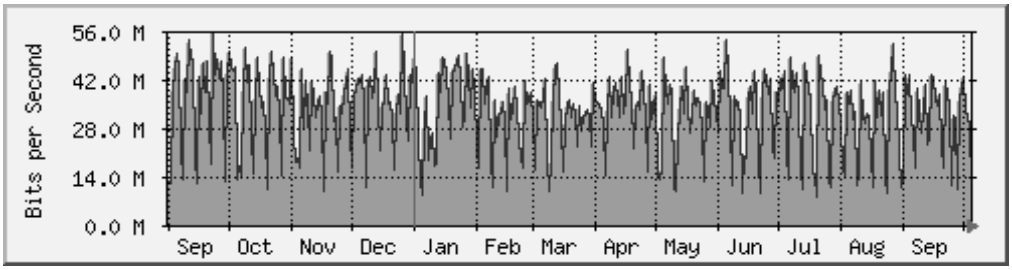
Рис. 1. Техническая схема КСПД КНИТУ



а)



б)



в)

Рис. 2. График загрузки интерфейса bond0 узла dionis-o:
а) за неделю (среднее за 30 минут); б) за месяц (среднее за 2 часа); в) за год (среднее за сутки).

Host 'Switch_129'

01-01-2013 00:00:00 to 01-09-2013 00:00:00
Duration: 243d 0h 0m 0s

[Availability report completed in 0 min 2 sec]

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	242d 19h 54m 50s	99.981%	99.981%
	Scheduled	0d 3h 0m 0s	0.051%	0.051%
	Total	**242d 22h 54m 50s**	**99.981%**	**99.981%**
DOWN	Unscheduled	0d 0h 6m 20s	0.002%	0.002%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 6m 20s**	**0.002%**	**0.002%**
UNREACHABLE	Unscheduled	0d 0h 58m 50s	0.017%	0.017%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 58m 50s**	**0.017%**	**0.017%**
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	243d 0h 0m 0s	100.000%	100.000%

Рис. 3. Доступность Cisco Catalyst 3750 на ул. Толстого, 68 за период с 1.01.2013 по 31.08.2013 (до замены)

Для достижения цели необходимо выполнить следующие задачи:

1. Создать автоматизированный сбор статистики в корпоративной сети КНИТУ.
2. Провести анализ собранной статистики.

Корпоративная сеть передачи данных КНИТУ с использованием криптомаршрутизаторов

Корпоративная сеть КНИТУ объединяет локальные вычислительные сети отдельных корпусов в единую сеть передачи данных, в том числе, телефонию. Основные корпуса объединены в 3 кластера:

1. На ул. Толстого 68 и 72 корпуса: "А","Б","В","О","К";
2. На ул. Сиб.Тракт 12, ул. Попова 10 корпуса: "Д","Е","Л","М","Г";
3. На ул. Сиб.Тракт 41 корпус "И".

Между собой кластеры соединены различным способом:

- ул. Толстого 68 и ул. Сиб. Тракт 12 соединены оптическим каналом пропускной способностью 100 Мбит/с и резервным беспроводным каналом 30 Мбит/с по технологии WiMAX.
- ул. Сиб. Тракт 12 и ул. Сиб. Тракт 41 соединены по технологии WiMAX, пропускная способность канала — 10 Мбит/с.

Текущая схема КСПД КНИТУ представлена на рис. 1.

Создание автоматизированной системы для мониторинга, сбора и обработки статистики КСПД

Для мониторинга работы сети необходима система сбора и обработки статистики.

Анализ статистики позволяет выявить аномалии работы в корпоративной сети под реальной нагрузкой. В дальнейшем обнаружить ошибки проектирования или настройки и устранить их.

Для сбора статистики по работе сетевых интерфейсов, был создан специальный сервер, на котором установлены и настроены следующие системы:

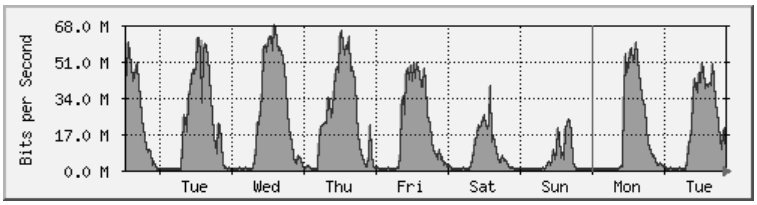
Host 'dionis-O-channel'

01-01-2015 00:00:00 to 10-06-2015 23:15:34
Duration: 278d 23h 15m 34s

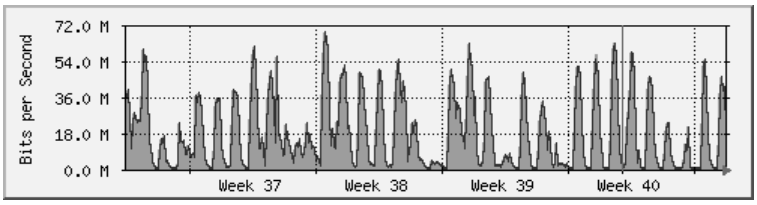
Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	278d 19h 17m 54s	99.941%	99.941%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	278d 19h 17m 54s	99.941%	99.941%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 3h 57m 40s	0.059%	0.059%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 3h 57m 40s	0.059%	0.059%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	278d 23h 15m 34s	100.000%	100.000%

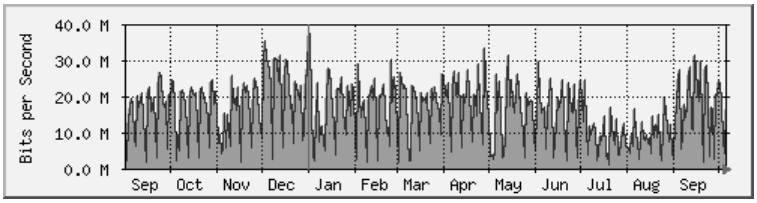
Рис. 4. Доступность узла dionis-o за период с 1.01.2015 по 6.10.2015



а)



б)



в)

Рис. 5. График загрузки интерфейса bond0 узла dionis-d:
а) за неделю (среднее за 30 минут); б) за месяц (среднее за 2 часа); в) за год (среднее за сутки).

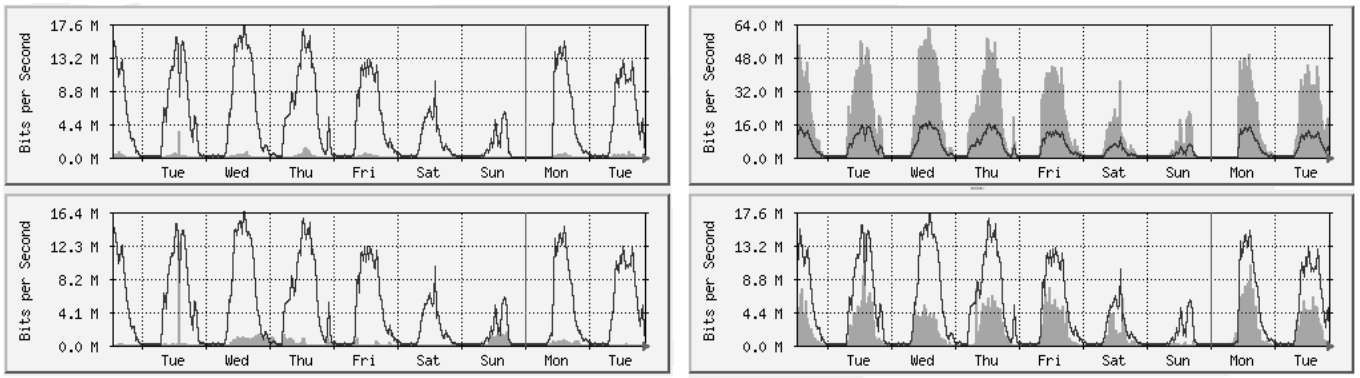


Рис. 5г. График недельной загрузки (среднее за 30 минут) составляющих агрегированного канала bond0 узла dionis-d

Host 'Switch_161'

01-01-2013 00:00:00 to 01-09-2013 00:00:00
Duration: 243d 0h 0m 0s

[Availability report completed in 0 min 0 sec]

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	138d 12h 49m 12s	98.800%	98.800%
	Scheduled	101d 13h 11m 17s	41.790%	41.790%
	Total	**240d 2h 0m 29s**	**98.800%**	**98.800%**
DOWN	Unscheduled	2d 8h 31m 20s	0.969%	0.969%
	Scheduled	0d 5h 23m 51s	0.093%	0.093%
	Total	**2d 13h 55m 11s**	**1.062%**	**1.062%**
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.138%	0.138%
	Scheduled	0d 8h 4m 20s	0.138%	0.138%
	Total	**0d 8h 4m 20s**	**0.138%**	**0.138%**
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	243d 0h 0m 0s	100.000%	100.000%

Рис. 6. доступность Cisco Catalyst 3750 на ул. Сиб. Тракт, 12 за период с 1.01.2013 по 31.08.2013 (до замены)

MRTG (The Multi Router Traffic Grapher) — сбор и обработка статистики [5–8],

Nagios — мониторинг за доступностью криптомаршрутизаторов [9–10].

После замены магистральных коммутаторов Cisco Catalyst 3750G на криптомаршрутизаторы DionisNX прошло больше 2 лет. За этот период не было отмечено проблем с математическим обеспечением криптомаршрутизаторов. Недоступность устройств dionis-o и dionis-d (см. рис. 4 и 7) связана с аварией на электрической подстанции КНИТУ. Пятидневная недоступность узла dionis-i (см. рис. 10) вызвана проблемами в сети оператора связи, предоставляющего радиоканал. За вычетом вышеука-

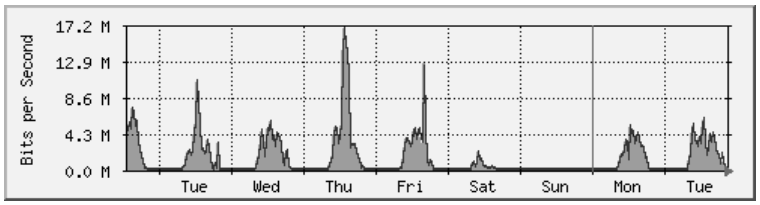
Host 'dionis-d'

01-01-2015 00:00:00 to 10-06-2015 23:06:24
Duration: 278d 23h 6m 24s

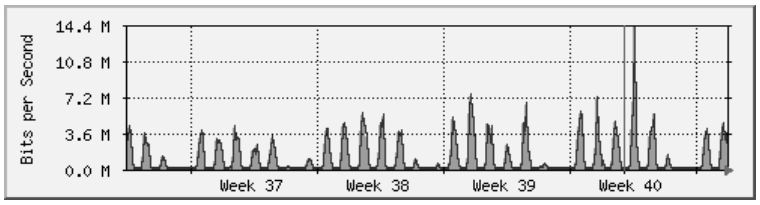
Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	278d 19h 7m 24s	99.941%	99.941%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	278d 19h 7m 24s	99.941%	99.941%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 3h 59m 0s	0.059%	0.059%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 3h 59m 0s	0.059%	0.059%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	278d 23h 6m 24s	100.000%	100.000%

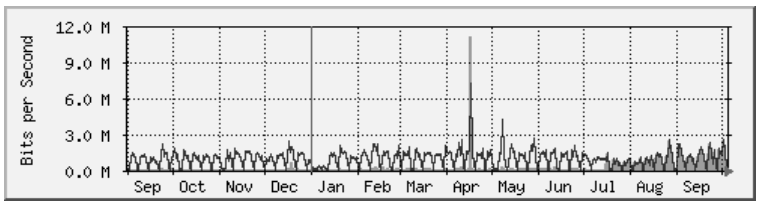
Рис. 7. доступность узла dionis-o за период с 1.01.2015 по 6.10.2015



а)



б)



в)

Рис. 8. график загрузки интерфейса bond0 узла dionis-i:
а) за неделю (среднее за 30 минут); б) за месяц (среднее за 2 часа); в) за год (среднее за сутки).

Host 'Gateway1'

01-01-2013 00:00:00 to 01-09-2013 00:00:00
Duration: 243d 0h 0m 0s

[Availability report completed in 0 min 0 sec]

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	138d 7h 50m 42s	98.736%	98.736%
	Scheduled	101d 14h 27m 39s	41.812%	41.812%
	Total	**239d 22h 18m 21s**	**98.736%**	**98.736%**
DOWN	Unscheduled	0d 4h 47m 0s	0.082%	0.082%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 4h 47m 0s**	**0.082%**	**0.082%**
UNREACHABLE	Unscheduled	2d 8h 42m 50s	1.182%	1.182%
	Scheduled	0d 12h 11m 49s	0.209%	0.209%
	Total	**2d 20h 54m 39s**	**1.182%**	**1.182%**
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	243d 0h 0m 0s	100.000%	100.000%

Рис. 9. доступность шлюза корпуса И за период с 1.01.2013 по 31.08.2013

Host 'dionis-i'

01-01-2015 00:00:00 to 10-06-2015 23:06:49
Duration: 278d 23h 6m 49s

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	273d 2h 17m 39s	97.897%	97.897%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	273d 2h 17m 39s	97.897%	97.897%
DOWN	Unscheduled	5d 16h 50m 0s	2.044%	2.044%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	5d 16h 50m 0s	2.044%	2.044%
UNREACHABLE	Unscheduled	0d 3h 59m 10s	0.060%	0.060%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 3h 59m 10s	0.060%	0.060%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	278d 23h 6m 49s	100.000%	100.000%

Рис. 10. доступность узла dionis-i за период с 1.01.2015 по 6.10.2015

занных проблем, доступность криптомаршрутизаторов составила более 99,95% всего времени. Для сравнения приведены отчеты по доступности их предшественников: Cisco Catalyst 3750 на ул. Толстого, 68 (рис. 3) и ул. Сиб. Тракт, 12 (рис. 6) и предыдущего шлюза корпуса И (рис. 9).

В качестве примера загрузки сетевых интерфейсов приведены отчеты по загрузке агрегированных интерфейсов bond0 узлов dionis-o (рис. 2), dionis-d (рис. 5) и dionis-i (рис. 8), через которые проходит весь маршрутизируемый трафик.

Анализ полученных данных позволяет говорить, что замена магистрального оборудования, в целом, не ухудшила работоспособность сети.

Заключение

В проведенной работе создана автоматизированная система для мониторинга, сбора и обработки статистики для модернизированной корпоративной сети, созданной на криптомаршрутизаторах НПП "Фактор-ТС" — DionisNX. Полученный опыт может быть использован при эксплуатации и модернизации любой корпоративной сети.

Тестирование показало полную работоспособность системы для мониторинга, сбора и обработки статистики в корпоративной сети.

Система позволяет контролировать работу модернизированной корпоративной сети КНИТУ и позволит в дальнейшем:

- тестировать криптомаршрутизаторы DionisNX под реальной нагрузкой;
- проводить эксперименты по имитационному моделированию нагрузки, атак и защиты сети;
- обучать студентов, в виде прохождения практики и выполнения дипломных работ на работающей корпоративной сети.

ЛИТЕРАТУРА

1. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/54–144
2. Селезнёв С., Иванов М., Ершов Р., Яковлев Д., Чеботарёв Н., Яковлев В. "Организация защищённого межсистемного информационного взаимодействия в распределённых АС предприятия на основе технологии DIONIS ANYCONNECT" // Методы и технические средства обеспечения безопасности информации — 2016. № 25. С. 28–29.
3. Кисельников Д. А. "Анализ эффективности защиты информации, обрабатываемой криптографическими маршрутизаторами DIONIS FW 16000 KB2, в условиях реализации различных сетевых атак" // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем Сборник материалов Всероссийской научно-практической конференции. — 2014. С. 97–98.
4. Руководство администратора DionisNX, НПП "Фактор-ТС", 2013.
5. Перов А. А., Сорокин А. А., Дмитриев В. Н. "Мониторинг сетей связи с динамической топологией на основе программы NAGIOS" // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2010. № 1. С. 99–102.
6. Порсев Ю. А., Султанов Р. О. "Система мониторинга компьютерной сети организации NAGIOS" // В сборнике: Информационные технологии в науке, промышленности и образовании Сборник трудов региональной научно-технической конференции. 2018. С. 193–202.
7. Миннивалиев Ш. Р., Шагаипов Д. Р. "Система мониторинга корпоративной сети NAGIOS" // В сборнике: Современные тенденции развития науки и производства IV Международная научно-практическая конференция: в 2-х томах. 2016. С. 134–136.
8. Шардаков К. С. "Сравнительный анализ популярных систем мониторинга сетевого оборудования, распространяемых по лицензии GPL" // Интеллектуальные технологии на транспорте. 2018. № 1 (13). С. 44–48.
9. Дугин А. "Мониторинг CISCO IDS/IPS на примере модуля IDSM2 с помощью MRTG" // Системный администратор. 2009. № 5 (78). С. 22–24.
10. Колисниченко Д. "Учет трафика с помощью программ MRTG и LAN BILLING" // Системный администратор. 2003. № 6 (7). С. 20–25.

Журнал «Современная наука: актуальные проблемы теории и практики»