СОЗДАНИЕ ПОЛИГОНА ЗАЩИЩЕННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТО-МАРШРУТИЗАТОРОВ DIONISNX НА БАЗЕ КОРПОРАТИВНОЙ СЕТИ КНИТУ

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 перевод корпоративной сети Казанского национального исследовательского технологического университета (КНИТУ) на отечественные крипто-маршрутизаторов DionisNX разработанные НПП "Фактор-ТС" и создание учебно-испытательного полигона на базе корпоративной сети КНИТУ. В статье подробно рассмотрена корпоративная сеть до модернизации и после модернизации. Сделан отказоустойчивый центральный узел за счёт использования кластера из 2-х устройств DionisNX.

Ключевые слова: Крипто-маршрутизаторы, корпоративные сети, импортзамещение, мэжсетевые экраны, виртуальные частные сети, отказоустойчевые кластеры, учебный полигон, тестирование программно-аппаратных комплексов, DionisNX, защищенные каналы, защищенные сети, безопасность сетей.

CREATING TESTING GROUND OF A PRIVATE NETWORK OF DATA TRANSMISSION NETWORK WITH THE USE OF DIONISNX CRYPTO-ROUTERS BASED ON THE CORPORATE NETWORK OF KNITU

V. Bogomolov
I. Pervuhin

Summary. The article discusses the transfer of the corporate network of the Kazan National Research Technological University (KNRTU) to domestic DionisNX crypto routers developed by "Factor-TS" and the creation of a training and testing ground based on the KNRTU corporate network. The article discusses in detail the corporate network before the upgrade and after the upgrade. A high-availability central node is made by using a cluster of 2 DionisNX devices.

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.

Введение

Корпоративная сеть передачи данных (КСПД) конкретной организации объединяет сети передачи данных этой организации в единую сеть, в том числе локальные вычислительные сети (ЛВС — LAN (Local Area Network)).

Цель построения корпоративной сети передачи данных — обеспечение доступа к территориально распределенным приложениям и защиты передаваемых данных. К приложениям могут относиться:

- базы данных;
- информационные порталы;
- электронная почта;
- файловый обмен;
- телефония;
- видеоконференцсвязь;
- системы дистанционного обучения.

Основным методом защиты данных, передаваемых по открытым каналам связи, является криптография. При этом разрешается использовать только сертифицированные средства криптографической защиты [1]. Такие средства разрабатываются только российскими организациями.

КНИТУ необходимо в будущем защитить свою корпоративную сеть. Для этого необходимы: сертифицированное оборудование, подготовленные специалисты с опытом работы, методика построения и обслуживания защищенной сети.

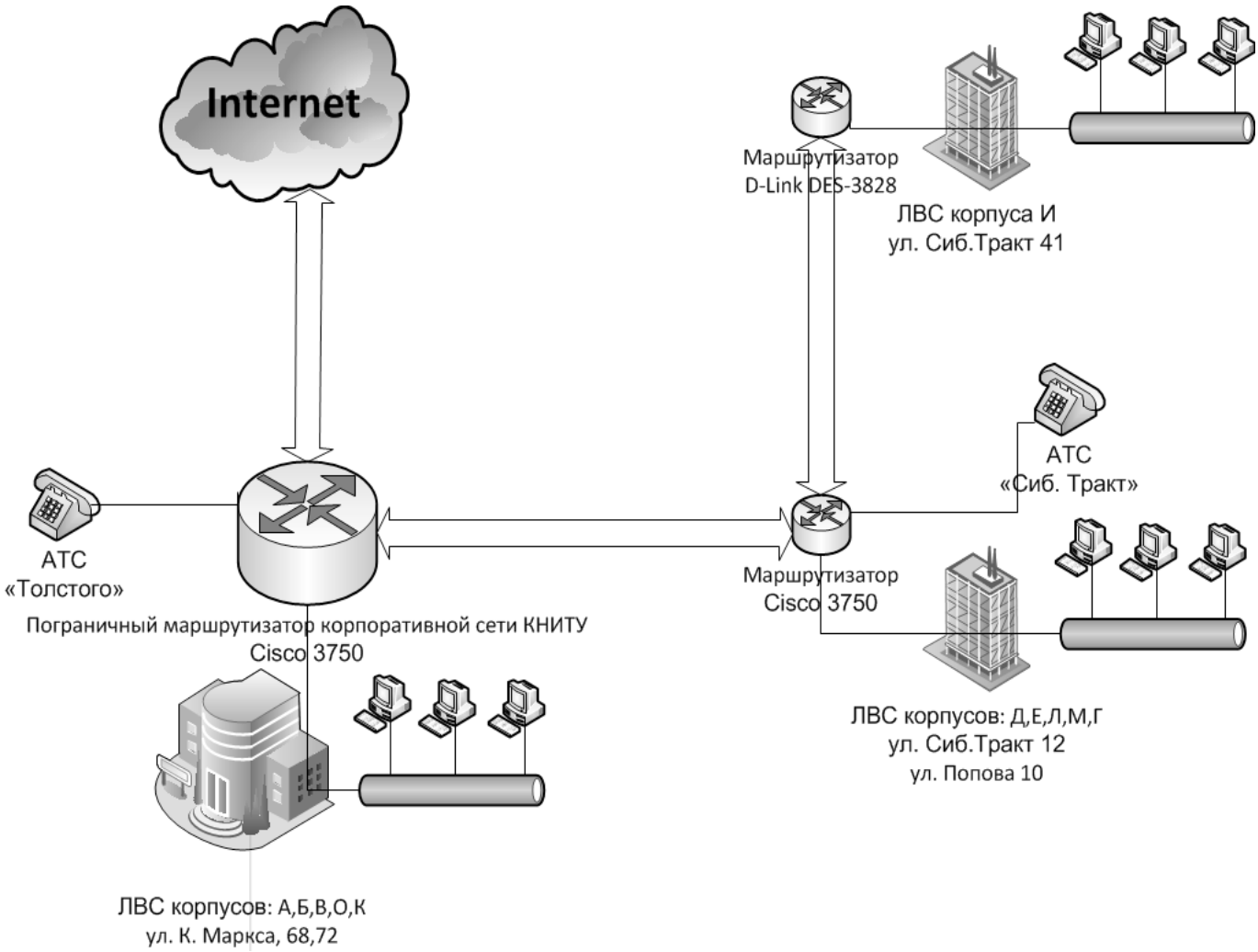

Рис. 1. Общая схема корпоративной сети КНИТУ.

Для создания защищенной корпоративной сети необходимы маршрутизаторы со встроенными средствами криптографической защиты. Такие маршрутизаторы называют крипто-маршрутизаторами.

Подобные крипто-маршрутизаторы разрабатывает НПП "Фактор-ТС" [2–3], с которым у КНИТУ давние отношения по тестированию разработок НПП "Фактор-ТС" и использования продуктов в учебных целях.

С одной стороны, для НПП "Фактор-ТС" необходим работающий прототип защищенной сети на базе реальной корпоративной сети большой организации, с достаточно большим сетевым трафиком. Для этих целей нельзя использовать реально защищаемую сеть, например, какого-то министерства. Корпоративная сеть ВУЗа является самым подходящим решением.

С другой стороны КНИТУ необходимы:

- оборудование для модернизации своей корпоративной сети передачи данных;
- защита передаваемых данных по корпоративной сети;
- Методика и опыт эксплуатации защищенной сети;
- площадка для обучения студентов.

НПП "Фактор-ТС" предоставляет бесплатно для КНИТУ крипто-маршрутизаторы, которые КНИТУ сможет использовать для модернизации своей корпоративной сети, отработки методики защиты сети и для подготовки специалистов.

Цель и задачи

Цель данной работы — разработать проект работающего прототипа защищенной сети передачи данных с использованием крипто-маршрутизаторов на базе корпоративной сети КНИТУ.

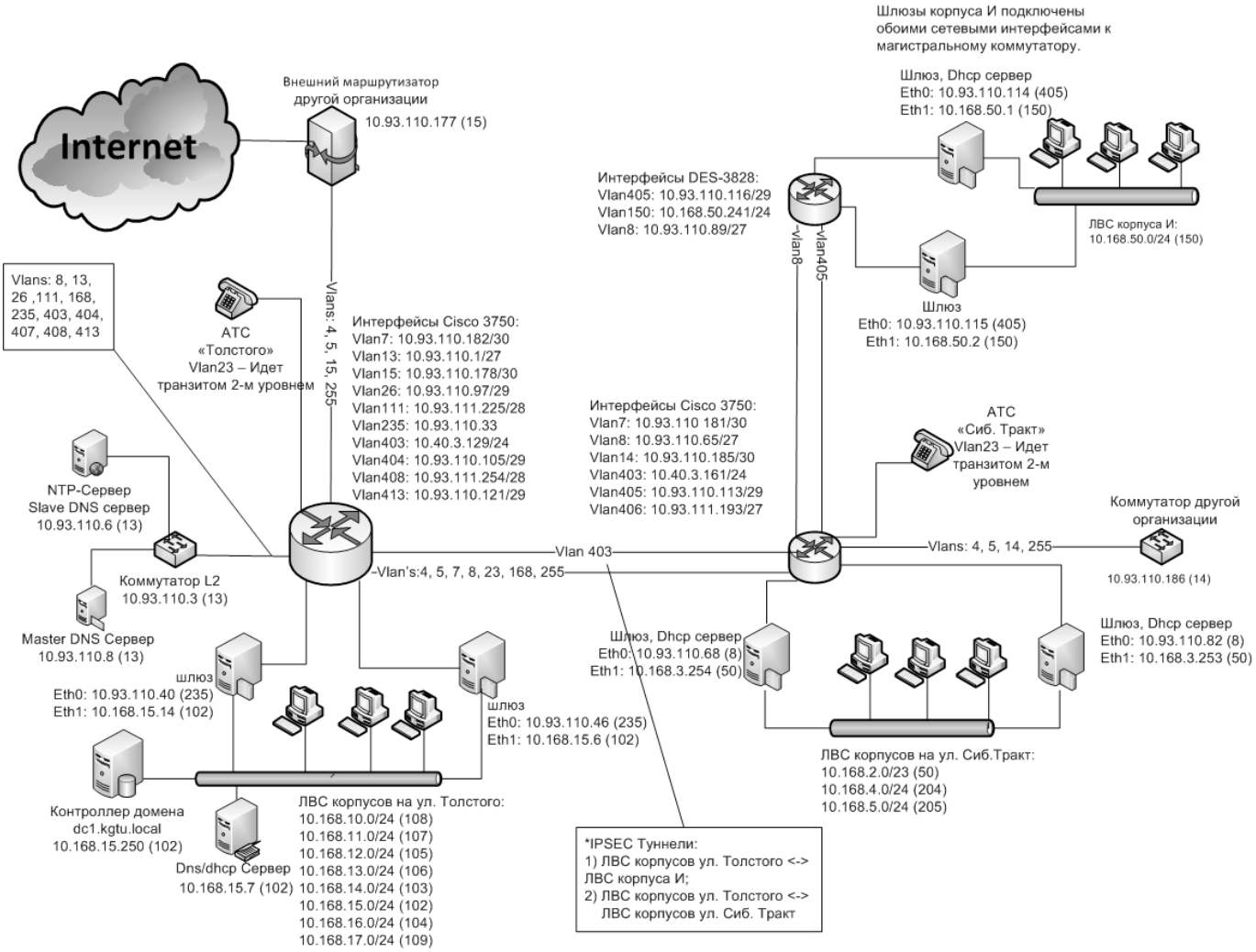

Рис. 2. Техническая схема корпоративной сети КНИТУ.

Для достижения цели необходимо выполнить следующие задачи:

1. Проанализировать существующую корпоративную сеть передачи данных КНИТУ.
2. Спроектировать модернизацию сети для создания защищенной сети передачи данных с использованием крипто-маршрутизаторов.
3. Корпоративная сеть КНИТУ на состояние 1.05.2013.

Корпоративная сеть КНИТУ Рис. 1. 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, пропускная способность резервного DSL-канала составляет 1 Мбит/с.

Маршрутизация пакетов в сети обеспечивается коммутаторами третьего уровня:

- Cisco Catalyst 3750 — на ул. Толстого.
- Cisco Catalyst 3750 — на ул. Сиб.Тракт 12.
- D-Link DES-3828 — на ул. Сиб.Тракт 41

Доступ персональных компьютеров из локальных сетей в глобальную сеть обеспечивается посредством

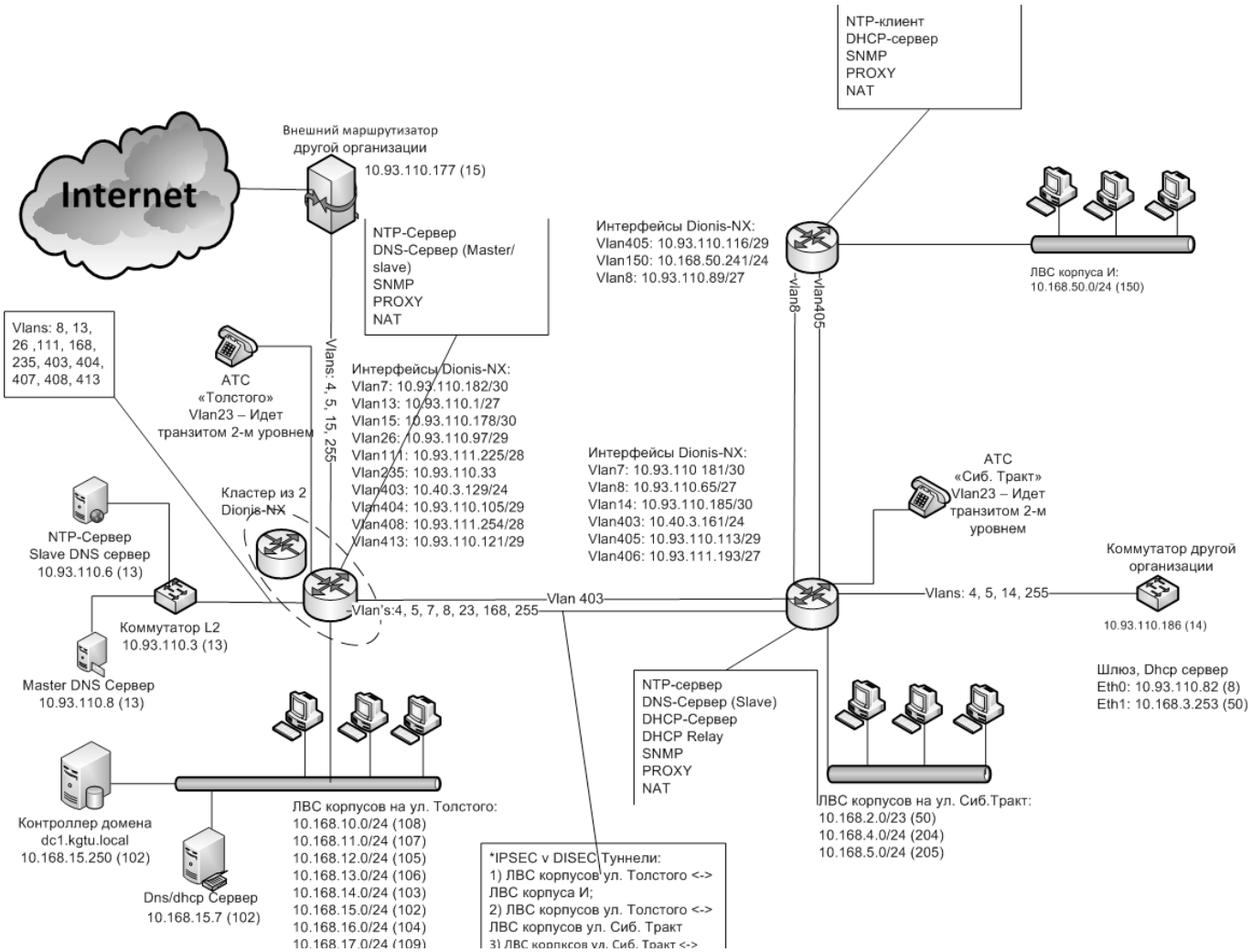

Рис. 3. Техническая схема корпоративной сети КНИТУ после модернизации.

шлюзовых машин. Они же осуществляют пробросы отдельных сегментов локальных сетей между зданиями, с помощью технологии «виртуальная частная сеть» VPN (Virtual Private Network).

Кроме шлюзов в каждом кластере функционируют серверы динамической конфигурации хостов (DHCP).

Используемая в КНИТУ единая система электронного документооборота требует подключение к домену kgtu.local. Как следствие, интеграция подсистемы «Деканат» в единую систему электронного документооборота влечет за собой включение в домен kgtu.local персональных компьютеров деканатов, которые территориально разбросаны по всем трём кластерам. Трафик между персональными компьютерами пользователей удаленных кластеров и контроллером домена необходимо передавать по защищенным каналам связи, что приведёт к увеличению нагрузки на шлюзовые устройства.

Следует отметить, что шлюзы корпуса «И» собраны на базе процессора Intel Pentium III и требуют модернизации.

Полная техническая схема сети приведена на Рис. 2.

Проект защищенной корпоративной сети передачи данных КНИТУ с использованием крипто-маршрутизаторов

Крипто-маршрутизатор НПП “Фактор-ТС” — DionisNX сочетает в себе функции различных устройств, используемых для построения TCP/IP сетей. Маршрутизатор DionisNX построен на базе ядра ОС Linux 3.0.xx и обладает следующими возможностями [4]:

1. Поддержка статической маршрутизации TCP/IP (v4);
2. Поддержка возможности задания статических ARP записей;

3. Поддержка фильтрации пакетов на основе различных критериев и их комбинаций, применительно к интерфейсу или системе в целом:
   a. протокола;
   b. адресов и портов источника/назначения;
   c. mac адреса источника;
   d. времени;
   e. поля TOS/DSCP;
   f. содержимого пакета;
   g. состояния соединения;
   h. состоянию флагов TCP;
4. Поддержка различных вариантов трансляции IP адресов (SNAT/DNAT);
5. Поддержка криптографической защиты данных, передаваемых по каналам связи сетей общего пользования, использующих протоколы семейства TCP/IP (компоненты СКЗИ):
6. создание и поддержка статических криптотуннелей между узлами Dionis NX с шифрованием и имитозащитой передаваемых IP-пакетов с инкапсуляцией их в протокол «IP в IP»;
7. реализация протоколов IPSEC ГОСТ (IKEv1, ESP), позволяющая создавать статические и динамические туннели IPSEC между узлами Dionis NX;
8. Поддержка протоколов динамической маршрутизации (OSPF, BGP, RIP);
9. Поддержка протоколов групповой передачи (Multicasting): IGMP (Протокол управления группами Интернет) и DVMRP (Дистанционно-векторный протокол многоадресной маршрутизации);
10. Поддержка механизмов качества обслуживания (QoS);
11. Поддержка виртуальных локальных компьютерных сетей (VLAN);
12. Поддержка аггрегации интерфейсов (bonding);
13. Поддержка инкапсуляции IP пакетов в туннели GRE;
14. Поддержка сервера доменных имен (DNS);
15. Поддержка сервера динамической конфигурации узла (DHCP);
16. Поддержка прокси-сервера HTTP/FTP с возможностями прозрачного перехвата и фильтрации трафика;
17. Поддержка сервера и клиента удаленного доступа SSH;
18. Поддержка сервера/клиента синхронизации часов по сети (NTP);
19. Поддержка сервера удаленного мониторинга (SNMP);
20. Поддержка протоколирования событий фильтрации IP пакетов;
21. Поддержка протоколирования цикла обработки IP пакетов при прохождении их через маршрутизатор;
22. Поддержка механизма контроля целостности программных компонентов маршрутизатора;
23. Поддержка процедур резервного архивирования и восстановления;
24. Поддержка функционирования узлов Dionis NX в режиме отказоустойчивого кластера.

В качестве основной системы управления маршрутизатором используется CISCO-подобный интерфейс командной строки.

Функциональные возможности DionisNX позволяют заменить коммутаторы Cisco Catalyst 3750 и D-Link DES-3828, а также переложить такие функции, как DHCP, трансляцию адресов и т.д. с отдельных серверов на единое устройство — DionisNX.

После модернизации полная техническая схема корпоративной сети КНИТУ будет выглядеть так Рис. 3.

Из схемы видно, что маршрутизаторы DionisNX возьмут на себя следующие функции:

- Маршрутизация
- Криптографическая защита пересылаемых данных
- Отказоустойчивый кластер
- NTP-сервер
- DNS-сервер
- DHCP-сервер
- SNMP
- PROXY
- NAT

Заключение

Проведенная работа показала возможность модернизации корпоративной сети КНИТУ используя крипто-маршрутизаторы НПП "Фактор-ТС" — DionisNX.

Модернизация корпоративной сети КНИТУ позволит:

- уменьшить количество устройств в сети;
- привести магистральную сеть КНИТУ к единой «элементной базе»;
- повысить отказоустойчивость центрального узла за счёт использования кластера из 2-х устройств DionisNX;

Кроме этого, будет создан работающий прототип защищенной сети передачи данных с использованием крипто-маршрутизаторов на базе корпоративной сети КНИТУ, что позволит:

- тестировать маршрутизаторы «Дионис»;
- отработать методику построения защищенной сети;
- обучать студентов.

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 — № 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.

© Богомолов Владислав Афанасьевич (vladbogomolov72@mail.ru), Первухин Илья Дмитриевич (pervuhin@kstu.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»

Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ