

Коберниченко В.Г., Золотых М.О.

Kobernichenko V.G., Zolotyh M.O.

ИЗУЧЕНИЕ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

КОМПЬЮТЕРНЫХ СЕТЕЙ НА БАЗЕ СОВРЕМЕННОГО

ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

STUDYING OF METHODS OF SAFETY OF COMPUTER NETWORKS ON

THE BASIS OF THE MODERN TELECOMMUNICATION EQUIPMENT

kobern@rtf.ustu.ru

ГОУ ВПО «Уральский государственный технический университет –

УПИ имени первого Президента России Б.Н.Ельцина»

г. Екатеринбург

Рассматривается организация лабораторного практикума по изучению компьютерных сетей и методов обеспечения их безопасности с использованием современного телекоммуникационного оборудования. В качестве объектов для изучения выбраны устройства производства Cisco Systems и D-Link Corporation.

The organisation of laboratory works on studying of computer networks and methods of maintenance of their safety with use of the modern telecommunication equipment is considered. As objects for studying devices of manufacture Cisco Systems and D-Link Corporation are chosen.

Современные телекоммуникационные системы строятся на основе широкого использования сетевых компьютерных технологий. В этой связи среди профессиональных компетенций, которые должны быть сформированы в процессе подготовки специалиста, как в области телекоммуникаций, так и в области информационной безопасности важными являются компетенции, связанные со способностью оценивать и обеспечивать уровень защищенности локальных вычислительных сетей и инфотелекоммуникационных систем. В их числе: установка, настройка и обслуживанию технических и программно-аппаратных средств; организация защиты информации техническими и программными средствами; конфигурирование межсетевых экранов, аудит безопасности сети; осуществление безопасной передачи данных через сети общего пользования.

Для формирования этих компетенций недостаточно только теоретических знаний об особенностях эталонной модели взаимодействия открытых систем, механизмах реализации атак в сетях; программно-аппаратных средствах обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях; протоколах и интерфейсах, используемые в инфотелекоммуникационных системах. Необходимо уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Необходимо овладеть навыками

- конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств;
- анализа сетевого трафика;
- анализа результатов работы средств обнаружения вторжений;
- маршрутизации и управления потоками в сетях передачи информации.

Эти навыки можно получить только в ходе практической работы на современном сетевом оборудовании. Лабораторная база для изучения механизмов обеспечения безопасности локальных сетей должна включать наиболее распространённое в практическом применении оборудование известных производителей. На рынке управляемых сетевых устройств для обработки больших объёмов информации лидирующие позиции занимает фирма Cisco Systems (32.6% мирового рынка в 2008 году по данным аналитической компании In-stat). На втором месте по объёму продаж находится фирма D-Link corporation (17.2% мирового рынка). В сегменте устройств для домашнего использования D-Link занимает первое место (33.6% рынка).

В результате реализации инновационной образовательной программы на кафедре теоретических основ радиотехники УГТУ-УПИ, выпускающей специальность «Информационная безопасность телекоммуникационных систем» была создана лаборатория защищённых информационных систем, включающая в себя два компьютерных класса, укомплектованных современным сетевым оборудованием производства фирм Cisco и D-Link. В состав оборудования классов входят рабочие места студентов, управляемые коммутаторы и маршрутизаторы, межсетевые экраны, точки доступа Wi-Fi и оборудование IP-телефонии.

Сетевое оборудование Cisco Systems:

1. Коммутатор уровня ядра Cisco Catalyst 6504 – 1 шт.
2. Коммутатор уровня распределения Cisco Catalyst 2960 – 6 шт.
3. Коммутатор 3-го уровня Cisco Catalyst 3560 – 1 шт.
4. Маршрутизатор Cisco 1841 – 4 шт.
5. Маршрутизатор Cisco 2811 – 2 шт.
6. Межсетевой экран Cisco ASA 5510 – 2 шт.
7. Межсетевой экран Cisco PIX 501 – 1 шт.
8. Система обнаружения и предотвращения атак Cisco MARS – 1 шт.
9. Wi-Fi точка доступа Cisco Aironet 1231 – 2 шт.
10. Wi-Fi точка доступа Cisco Aironet 1310 – 2 шт.
11. IP телефон Cisco 7941 – 3 шт.
12. Маршрутизатор 2811 с функциями VoIP шлюза – 2 шт.
13. Маршрутизатор 2811 с 16 асинхронными интерфейсами (RS-232) – 1 шт.

Сетевое оборудование D-Link:

1. Управляемый коммутатор DES-2108 – 6 шт.
2. Точка доступа DWL-2100AP – 4 шт.
3. Маршрутизатор DI-804(HV) – 2 шт.
4. Беспроводной маршрутизатор DI-824(VUP+) – 2 шт.
5. Межсетевой экран DFL-210 – 2 шт.

6. VoIP шлюз DVX-7090 – 2 шт.
7. IP телефон DPH-150S – 2 шт.
8. IP телефон DPH-300S – 2 шт.
9. Направленная Wi-Fi антенна ANT24-0600 – 2 шт.

Кроме того имеется также VPN сервер АМИКОН ФПСУ-IP, сертифицированный ФСБ и ФСТЭК, и применяемый в учреждениях Сбербанка РФ.

Указанное оборудование объединено в учебную компьютерную сеть, распределенную в двух компьютерных классах. Первоначальный вариант учебной сети был создан в 2007 году, в 2008 году были проведены первые лабораторные работы по дисциплинам «Операционные системы», «Компьютерные сети» и «Защита информации в компьютерных сетях». По результатам проведения работ были сформированы предложения по улучшению функционирования сети, которые были реализованы в 2009 году при создании новой версии учебной сети. В настоящее время сеть включает около 80 узлов различного типа. Оборудование Cisco Systems расположено в 19” телекоммуникационных стойках, а оборудование фирмы D-Link (относящиеся к классу SOHO), на специальных стендах, на стенах аудитории. На каждом стенде находится один маршрутизатор и один управляемый коммутатор. Стенды разработаны и изготовлены сотрудниками кафедры.

Всё используемое оборудование можно подразделить на несколько больших групп, по функциональному назначению:

1. Рабочие станции.
2. Управляемые коммутаторы.
3. Маршрутизаторы.
4. Межсетевые экраны.
5. Wi-Fi оборудование.
6. Оборудование VoIP.

Компьютерная сеть связана с учебной телефонной сетью, так же создаваемой на кафедре – это позволяет изучать технологии VoIP и процессы, происходящие на стыках аналоговых, цифровых и пакетных линий передачи голосовой информации.

В ходе лабораторных работ могут быть имитированы самые разнообразные компьютерные сети без физической коммутации оборудования, поскольку в топологию сети внесена избыточность, которая позволяет менять конфигурацию сети на программном уровне, включая и отключая различные связи между узлами. Это позволяет автоматизировать процесс подготовки лабораторных работ (путём написания программ, автоматически проверяющих готовность сети и исправляющих ошибки), сокращает время подготовки для каждой конкретной лабораторной работы и повышает срок службы оборудования (не происходит износа разъёмов).

Все устройства находятся в поле зрения студентов, однако физического контакта с оборудованием в ходе учебных работ не предусматривается, все элементы сети надёжно закреплены на стенах аудиторий и в телекоммуникационных стойках, защищённых прозрачными дверцами, позволяющими видеть состояние индикации оборудования.

Лабораторное оборудование позволяет изучать:

1. Процессы маршрутизации и коммутации в локальных компьютерных сетях.
2. Методы обнаружения и предотвращения сетевых атак.
3. Методы построения виртуальных частных сетей.
4. Способы межсетевого экранирования.
5. Функционирование беспроводных сетей.
6. Функционирование VoIP и аналоговых телефонных сетей.
7. Функционирование мультисервисные сетей с передачей видео, голосового и трафика данных.
8. Функционирование протоколов предназначенных для работы между автономными системами Интернет: MPLS, BGP.
9. Вопросы безопасности в сетях на основе протокола IPv6.

В частности, в настоящее время для студентов специальности «Информационная безопасность телекоммуникационных систем» проводятся лабораторные работы:

- «Знакомство с ОС IOS».
- «Изучение работы Ethernet коммутатора».
- «Настройка статической маршрутизации».
- «Настройка DHCP сервера».
- «Настройка IPsec туннеля».
- «Настройка ACL».

Ресурсы лаборатории защищенных информационных систем могут быть использованы не только при изучении вопросов безопасности, но и при обучении студентов других специальностей и направлений, в перечень компетенций которых попадает перечисленные выше способности, умения и навыки.

Коноваленко О.М.

Konovalenko O.M.

СОВРЕМЕННЫЕ ИНСТРУМЕНТЫ РЕАЛИЗАЦИИ ПРИНЦИПА
НАГЛЯДНОСТИ В УСЛОВИЯХ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-
КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ОБРАЗОВАНИИ,
MODERN TOOLS OF REALIZATION OF THE PRINCIPLE OF
PRESENTATION IN CONDITIONS OF INFORMATION COMMUNICATION
TECHNOLOGIES IN EDUCATION

konovalenko1005@yandex.ru

*ГОУ ВПО «Уральский государственный технический университет –
УПИ имени первого Президента России Б.Н.Ельцина»*

г. Каменск-Уральский

Показано развитие принципа наглядности при использовании современных технологий представления информационно-методических материалов в виде мультимедиаданных. Рассматриваются такие средства реализации данного принципа в новых условиях применения информационно-