

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины
Безопасность компьютерных сетей

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем (в сфере информационных технологий)»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 26 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Целью изучения дисциплины «Безопасность компьютерных сетей» является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Задачи дисциплины:

- изучение типовых угроз безопасности в компьютерных сетях;
- изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
- овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

Данный курс, позволяет путем изучения угроз безопасности в компьютерных сетях, методов сетевых атак и вторжений, а также уязвимостей информационных систем, выработать у студентов убежденность в необходимости принятия адекватных мер защиты российских объектов информатизации, предоставляет достаточные знания и навыки, требуемые для этого.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность компьютерных сетей» относится к обязательной части образовательной программы.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» - знание основных понятий информатики;

«Основы информационной безопасности» - знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации, владение профессиональной терминологией в области информационной безопасности;

«Компьютерные сети» - знание эталонной модели взаимодействия открытых систем, типовых структур и принципов организации компьютерных сетей, основ Интернет-технологий, владение навыками конфигурирования локальных компьютерных сетей и реализации сетевых протоколов с помощью программных средств;

«Криптографические методы защиты информации» - знание основных видов симметричных и асимметричных криптографических алгоритмов, средств и методов хранения аутентификационной информации, владение криптографической терминологией.

Знания и навыки, полученные в ходе изучения дисциплины «Безопасность компьютерных сетей», могут непосредственно использоваться при работе по специальности.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции		
ОПК- 1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях	И-ОПК-1.2.1 Знает порядок реализации методов и средств межсетевого экранирования, методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации	Знать: - типы сетевых атак и методы борьбы с ними; - типы брандмауэров, их отличия и варианты использования; - программные и аппаратные возможности анализа сетевого трафика; - программные и аппаратные возможности защиты сетевой инфраструктуры;
	И-ОПК-1.2.3 Владеет управлением функционированием программно-аппаратных средств защиты информации в компьютерных сетях; И-ОПК-1.2.4 Владеет контролем над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение	Владеть навыками: - анализа сетевого трафика и навыками решения проблем при использовании физического оборудования и Cisco Packet Tracer; - внедрения AAA на маршрутизаторах; - устранения угроз для маршрутизаторов и сетей с помощью списков управления доступом (ACL); - внедрения VPN типа «сеть-сеть»; - внедрения VPN с удаленным доступом; - проектирования, внедрения и поддержки мер безопасности для обеспечения защиты и целостности сетевых устройств; - настройки и администрирования аппаратных межсетевых экранов Cisco ASA.
Профессиональные компетенции		
ПК-3 Способен обеспечивать контроль над соблюдением требований по защите информации	И-ПК-3.1 Знает и понимает нормативные требования по защите информации И-ПК-3.2 Умеет осуществлять оценку и контроль исполнения требований по защите информации И-ПК-3.3 Владеет навыками осуществления контроля над соблюдением требований по защите информации	Знать: нормативные требования по защите информации Уметь: осуществлять оценку и контроль исполнения требований по защите информации Владеть навыками: осуществления контроля над соблюдением требований по защите информации

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Обеспечение безопасности сетей.	5	4	2		1		4	Задания для самостоятельной работы
2	Мониторинг и управление устройствами.	5	4	6		1		4	Задания для самостоятельной работы
3	ACL и брандмауэры.	5	4	6		1		6	Задания для самостоятельной работы
4	Предотвращение вторжений.	5	2	1		1		4	
5	Уровень 2 и безопасность конечных устройств.	5	6	3		1		4	Задания для самостоятельной работы
6	Криптография.	5	4	4		1		4	Задания для самостоятельной работы
7	VPN.	5	4	4		1		4	Задания для самостоятельной работы
8	Cisco ACA	5	4	6		1		6	Задания для самостоятельной работы
						2	0,5	33,5	Экзамен
	Всего		32	32		10	0,5	69,5	

Содержание разделов дисциплины:

Раздел 1. Обеспечение безопасности сетей.

1. Защита сетей.

1.1. Введение. Заявление об этическом взломе. Текущее положение дел. Сети — это цели. Причины сетевой безопасности. Векторы сетевых атак. Потери данных.

1.2. Обзор топологии сети. Сети кампуса. Сети малого офиса и домашнего офиса. Глобальные сети. Сети центров обработки данных. Облачные сети и виртуализация. Развивающиеся сетевые границы.

2. Сетевые угрозы.

2.1. Кто атакует нашу сеть? Угроза, уязвимость и риск. Хакер против злоумышленника. Эволюция субъектов угроз. Киберпреступники. Задачи кибербезопасности. Индикаторы киберугроз. Обмен угрозами и повышение осведомленности о кибербезопасности.

2.2. Инструменты субъекта угроз. Введение инструментов атаки. Эволюция инструментов безопасности. Категории атак.

2.3. Вредоносное ПО. Типы вредоносных программ. Вирусы. Троянские кони. Черви. Компоненты червя. Программы-вымогатели. Другое вредоносное ПО. Распространенное поведение вредоносных программ.

2.4. Распространенные сетевые атаки — разведка, доступ и социальная инженерия. Типы сетевых атак. Разведывательные атаки. Атаки доступа. Атаки социальной инженерии. Укрепление самого слабого звена.

2.5. Сетевые атаки — отказ в обслуживании, переполнение буфера и уклонение. DoS- и DDoS-атаки. Компоненты DDoS-атак. Ботнет Mirai. Атака на переполнение буфера. Методы уклонения, используемые злоумышленниками.

3. Снижение угроз.

3.1. Защита сети. Специалисты по сетевой безопасности. Сообщества сетевого анализа. Сертификаты сетевой безопасности. Коммуникационная безопасность.

3.2. Политики сетевой безопасности. Домены сетевой безопасности. Деловая политика. Политика безопасности. Политики BYOD. Соответствие нормативным требованиям и стандартам.

3.3. Инструменты безопасности, платформы и сервисы. "Лук" безопасности и "Артишок" безопасности. Инструменты тестирования безопасности. Платформы безопасности данных. демонстрация Cisco SecureX. Охранные услуги.

3.4. Противодействие распространенным сетевым атакам. Защита сети. Защита от вредоносных программ. Борьба с червями. Смягчение разведывательных атак. Смягчение атак доступа. Смягчение DoS-атак.

3.5. Платформа защиты Cisco Network Foundation. Структура. Защита уровня управления. Защита уровня данных.

4. Безопасный доступ к устройствам.

4.1. Защита пограничного маршрутизатора. Защита сетевой инфраструктуры. Подходы к обеспечению безопасности пограничных маршрутизаторов. Три области безопасности маршрутизатора. Безопасный административный доступ. Безопасный локальный и удаленный доступ.

4.2. Настройка безопасного административного доступа. Пароли. Настройка. Шифрование. Дополнительная защита паролем. Алгоритмы секретного пароля.

4.3. Настройка усиленной безопасности для виртуальных входов. Настройка функций расширения входа. Улучшения входа. Журнал неудачных попыток входа.

4.4. Включение SSH. Повышение безопасности входа по SSH. SSH между маршрутизаторами. SSH хост-маршрутизатор.

Раздел 2. Мониторинг и управление устройствами.

5. Назначение административных ролей.

5.1. Настройка уровней привилегий. Ограничение доступности команд. Настройка и назначение уровней привилегий. Ограничения уровней привилегий.

5.2. Доступ к интерфейсу командной строки на основе ролей. Представления на основе ролей. Настройка представлений на основе ролей. Настройка супервизоров CLI на основе ролей. Проверка представлений CLI на основе ролей.

6. Мониторинг и управление устройствами.

6.1. Безопасный образ Cisco IOS и файлы конфигурации. Функция отказоустойчивой конфигурации Cisco IOS. Включение функции устойчивости образа IOS. Образ основного загрузочного набора. Настройка безопасного копирования. Восстановление пароля маршрутизатора.

6.2. Блокировка маршрутизатора с помощью AutoSecure. Протоколы обнаружения CDP и LLDP. Настройки протоколов и служб. Автозащита Cisco. Синтаксис команды Cisco AutoSecure. Пример конфигурации Cisco AutoSecure.

6.3. Аутентификация протокола маршрутизации. Протоколы динамической маршрутизации. Подмена протокола маршрутизации. Аутентификация протокола маршрутизации OSPF MD5. Аутентификация протокола маршрутизации OSPF SHA.

6.4. Безопасное управление и отчетность. Типы доступа к управлению. Внеполосный и внутриволосный доступ.

6.5. Введение в системный журнал. Операции системного журнала. Формат сообщений системного журнала. Средства системного журнала. Настройка временных меток системного журнала. Системы системного журнала. Конфигурация системного журнала.

6.6. Службы времени и календаря. Операции NTP. Настройка и проверка NTP.

6.7. Введение в SNMP. SNMP-операции. База управленческой информации (MIB). Версии SNMP. SNMP-уязвимости. SNMPv3. Конфигурация безопасности SNMPv3. Проверка SNMPv3.

7. Аутентификация, авторизация и учет (AAA).

7.1. Аутентификация без AAA. Компоненты AAA. Режимы аутентификации. Авторизация. Учёт.

7.2. Настройка локальной аутентификации AAA. Аутентификация административного доступа. Методы аутентификации. Методы по умолчанию и именованные методы. Тонкая настройка конфигурации аутентификации.

7.3. Сравнение локальных и серверных реализаций AAA. Механизм служб идентификации Cisco (ISE). Протоколы TACACS+ и RADIUS. TACACS+ Аутентификация. RADIUS-аутентификация.

7.4. Действия по настройке аутентификации AAA на основе сервера. Настройка серверов TACACS+. Настройка серверов RADIUS. Аутентификация для команд конфигурации сервера AAA.

7.5. Введение в серверную авторизацию AAA. Конфигурация авторизации AAA. Введение в серверный учет AAA. Конфигурация учета AAA.

Раздел 3. ACL и брандмауэры.

8. Списки контроля доступа (ACL).

8.1. Что такое ACL? Пакетная фильтрация. Нумерованные и именованные ACL. Операция со списком контроля доступа.

8.2. Обзор подстановочной (обратной) маски. Типы подстановочных масок. Вычисление подстановочной маски. Маска подстановочных знаков: Ключевые слова.

8.3. Создание списка контроля доступа (ACL). Нумерованный стандартный синтаксис ACL IPv4. Именованный стандартный синтаксис ACL IPv4. Синтаксис нумерованного расширенного списка контроля доступа IPv4. Протоколы и номера портов. Примеры настройки протоколов и номеров портов. TCP - установка расширенного ACL.

8.4. Два метода изменения ACL. Метод текстового редактора. Метод порядкового номера.

8.5. Рекомендации по настройке ACL-списков. Применение ACL. Где размещать ACL. Стандартный пример размещения ACL. Пример размещения расширенного ACL.

8.6. Смягчение атак с помощью ACL. Смягчение спуфинговых атак. Разрешение необходимого трафика через брандмауэр. Смягчение ICMP-атак. Смягчение SNMP-атак.

8.7. Обзор списка контроля доступа IPv6. Синтаксис ACL IPv6. Настройка списков контроля доступа IPv6.

9. Технологии межсетевых экранов.

9.1. Брандмауэры. Типы брандмауэров. Преимущества и ограничения брандмауэра с фильтрацией пакетов. Преимущества и ограничения брандмауэра с отслеживанием состояния.

9.2. Общие архитектуры безопасности. Многоуровневая защита.

10. Межсетевые экраны на основе политик зон (ZPF).

10.1. Преимущества ZPF. Проектирование ZPF.

10.2. Действия ZPF. Правила транзитного движения. Правила прохождения в собственную зону.

10.3. Настройка ZPF. Проверка конфигурации ZPF. Рекомендации по конфигурации ZPF.

Раздел 4. Предотвращение вторжений.

11. IPS-технологии.

11.1. Атаки нулевого дня. Отслеживание атак. Устройства предотвращения и обнаружения вторжений (IDS и IPS). Преимущества и недостатки IDS и IPS.

11.2. Типы IPS. Сетевые IPS. Способы развертывания.

11.3. IPS на Cisco ISR. Компоненты IPS. IPS-система Cisco IOS. Snort IPS. Операции Snort IPS. Особенности Snort IPS. Системные требования Snort.

11.4. Методы мониторинга сети. Сетевые ответвители (Network Taps). Зеркалирование трафика и SPAN. Настройка SPAN Cisco.

12. Эксплуатация и внедрение IPS.

12.1. Атрибуты сигнатур IPS. Типы сигнатур. Сигнатурные тревоги IPS. Действия сигнатур IPS. Оценка предупреждений.

12.2. Cisco Snort IPS. Варианты службы IPS. NGIPS. Snort IPS. Компоненты и правила Snort. Приложения-контейнеры ISR. Аварийные сигналы правил Snort IPS. Действия правила Snort IPS. Параметры правил заголовка Snort IPS. Действия Snort IPS.

12.3. Настройка Snort IPS.

Раздел 5. Уровень 2 и безопасность конечных устройств.

13. Обзор безопасности конечных устройств.

13.1. Безопасность элементов локальной сети. Традиционная защита конечных устройств. Сеть без границ. Безопасность конечных устройств в сети без границ. Сетевая защита от вредоносных программ. Аппаратное и программное шифрование локальных данных. Контроль доступа к сети. Функции NAC.

13.2. Безопасность с использованием аутентификации на основе портов 802.1X. Управление состоянием авторизации 802.1X. Конфигурация 802.1X.

14. Вопросы безопасности уровня 2.

14.1. Описание уязвимости уровня 2 модели OSI. Переключение категорий атак.

14.2. Атаки по таблице MAC-адресов. Основы работы коммутатора. Коммутатор: обучение и переадресация. Фильтрация кадров. Заполнение таблицы MAC-адресов.

14.3. Безопасность неиспользуемых портов. Противодействие атакам на таблицу MAC-адресов. Включение безопасности порта. Ограничение и изучение MAC-адресов. Устаревание безопасности портов. Режимы нарушения безопасности портов. Порты в отключенном состоянии из-за ошибки. Проверка безопасности порта. Уведомление о MAC-адресе по SNMP

14.4. Смягчение атак VLAN. Атаки VLAN Hopping. Атака с использованием двойного тегирования VLAN. Смягчение атак с использованием двойного тегирования. Частные виртуальные локальные сети (PVLAN). Пограничные функции PVLAN. Настройка граничного PVLAN (PVLAN Edge).

14.5. DHCP-атаки. Защита от DHCP-атак. Шаги по реализации DHCP Snooping (Отслеживание DHCP). Пример настройки отслеживания DHCP.

14.6. ARP-атаки. Спуфинг ARP. Динамическая проверка ARP (DAI). Руководство по внедрению DAI. Пример конфигурации DAI.

14.7. Адресные спуфинговые атаки. Противодействие атаке с подменой MAC-адреса. Настройка защиты IP (IP Source Guard).

14.8. Протокол связующего дерева (STP). Пересчет STP. Циклы. Роли порта STP. Корневой мост STP. Стоимость пути STP. Выбор корневого моста.

14.9. STP-атака. Смягчение STP-атак. Настройка PortFast. Настройка защиты BPDU. Настройка корневой защиты (Root Guard). Настройка защиты от петель (STP Loop Guard).

Раздел 6. Криптография.

15. Службы криптографии.

15.1. Аутентификация. Целостность данных. Конфиденциальность данных.

15.2. Криптография. Создание зашифрованного текста. Шифры перестановки. Подстановочные шифры. Более сложный шифр замены. Шифры с одноразовым блокнотом.

15.3. Криптоанализ. Методы взлома кода. Пример взлома кода.

15.4. Криптология. Создание и взлом секретных кодов. Криптоаналитики. Секретность ключей.

16. Базовая целостность и подлинность.

16.1. Безопасная связь. Криптографические хеш-функции. Криптографическая хэш-операция. MD5 и SHA. Аутентификация происхождения.

16.2. Характеристики управления ключами. Длина ключа и пространство ключей. Типы криптографических ключей. Выбор криптографических ключей.

16.3. Конфиденциальность данных. Симметричное шифрование. Асимметричное шифрование. Асимметричное шифрование — конфиденциальность, аутентификация, целостность. Диффи-Хеллман.

17. Криптография с открытым ключом.

17.1. Обзор цифровой подписи. Цифровые подписи для подписи кода. Цифровые подписи для цифровых сертификатов.

17.2. Управление открытым ключом. Инфраструктура открытых ключей. Система полномочий PKI. Система доверия PKI. Совместимость различных поставщиков PKI. Регистрация сертификата, аутентификация и отзыв.

17.3. PKI-приложения. Зашифрованные сетевые транзакции. Шифрование и мониторинг безопасности.

Раздел 7. VPN.

18. VPN.

18.1. Виртуальные частные сети. Преимущества VPN.

18.2. Топологии VPN. VPN с удаленным доступом. SSL VPN. Сеть-сеть IPsec VPN (Site-to-Site IPsec VPN).

18.3. Обзор IPsec. Технологии IPsec. Инкапсуляция протокола IPsec. Конфиденциальность. Целостность. Аутентификация. Безопасный обмен ключами с использованием протокола Диффи-Хеллмана (DH). Транспортный и туннельный режимы IPsec.

18.4. Обзор протокола IPsec. Заголовок аутентификации. Протокол безопасности инкапсуляции (ESP). ESP шифрование и аутентификация. Транспортный и туннельный режимы.

18.5. Обмен ключами через Интернет. Протокол IKE.

19. Внедрение Site-to-Site IPsec VPN.

19.1. IPsec-согласование. Топология Site-to-Site IPsec VPN. Задачи настройки IPsec VPN. Существующие конфигурации ACL. Обработка широковещательного и многоадресного трафика.

19.2. Политики ISAKMP по умолчанию. Синтаксис для настройки новой политики ISAKMP. Конфигурация предварительного общего ключа.

19.3. Политики IPsec. Определение интересующего трафика. Настройка набора преобразований IPsec.

19.4. Синтаксис для настройки криптографической карты (Crypto Map). Конфигурация криптографической карты. Применение и проверка криптографической карты.

19.5. IPsec VPN. Отправка интересующего трафика. Проверка туннелей ISAKMP и IPsec.

Раздел 8. Cisco ASA.

20. Введение в ASA.

20.1. Модели брандмауэров ASA. Межсетевые экраны нового поколения Cisco ASA. Расширенные функции брандмауэра ASA. Обзор брандмауэров в сетевом дизайне. Режимы работы брандмауэра ASA. Лицензионные требования ASA.

20.2. Обзор ASA 5506-X. Уровни безопасности ASA. Сценарии развертывания ASA 5506-X.

21. Конфигурация брандмауэра ASA.

21.1. Основные настройки ASA. Конфигурация ASA по умолчанию. Мастер инициализации интерактивной установки ASA.

21.2. Настройка параметров управления и служб. Вход в режим глобальной конфигурации. Настройка основных параметров. Настройка интерфейсов. Настройка статического маршрута по умолчанию. Настройка служб удаленного доступа. Настройка служб протокола сетевого времени. Настройка служб DHCP.

21.3. Введение в объекты и группы объектов. Настройка сетевых объектов. Настройка сервисных объектов. Группы объектов. Настройка общих групп объектов.

21.4. ACL ASA. Типы фильтрации списков ASA ACL. Типы списков ASA ACL. Синтаксис для настройки ACL ASA. Синтаксис для применения списка управления доступом ASA. Примеры ACL ASA. ACL и группы объектов. ACL с использованием примеров групп объектов.

21.5. Обзор ASA NAT. Настройка динамического NAT. Настройка динамического PAT. Настройка статического NAT.

21.6. Обзор AAA. Локальная база данных и серверы. Конфигурация AAA.

21.7. Обзор MPF. Настройка карт классов. Определение и активация политики.

22. Тестирование сетевой безопасности.

22.1. Операционная безопасность. Тестирование и оценка сетевой безопасности. Типы сетевых тестов. Применение результатов сетевого тестирования.

22.2. Инструменты для тестирования сети. Nmap/Zenmap. SuperScan. SIEM.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- Linux Ubuntu (GNU GPL v.3);
- OpenOffice (GNU LGPL);
- Cisco Packet Tracer 8.1.0 (доступен бесплатно для участников Программы Сетевой Академии Cisco);

- Cisco SDM (доступен бесплатно для участников Программы Сетевой Академии Cisco);
- Cisco Network Assistant (доступен бесплатно для участников Программы Сетевой Академии Cisco);
- Cisco Configuration Professional (доступен бесплатно для участников Программы Сетевой Академии Cisco);
- Wireshark (GNU GPL 2+);
- Snort (GNU GPL);
- Oracle VirtualBox (GNU GPL 2);
- Google Chrome (freeware).

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используется:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»
<https://www.studentlibrary.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Учебно-методическое пособие в LMS NetAcad. Режим доступа: свободный для участников Программы Сетевой Академии Cisco (<https://www.netacad.com/>)
2. Нестеров, С. А. Основы информационной безопасности: учебник для вузов — Санкт-Петербург: Лань, 2021. <https://reader.lanbook.com/book/165837>
3. Шелухин О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов - Москва: Горячая линия - Телеком, 2013. <https://www.studentlibrary.ru/ru/doc/ISBN9785991203234-SCN0000/000.html>
4. Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М. Технологии защиты информации в компьютерных сетях - Москва: Национальный Открытый Университет "ИНТУИТ", 2016.
https://www.studentlibrary.ru/ru/doc/intuit_384-SCN0000/000.html

б) дополнительная литература

1. А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для вузов - Москва: Горячая линия - Телеком, 2016.
<https://www.studentlibrary.ru/ru/doc/ISBN9785991204705-SCN0000/000.html>
2. А. И. Костюк, Д. А. Беспалов Администрирование баз данных и компьютерных сетей: учебное пособие. — Ростов-на-Дону: ЮФУ, 2020.
<https://www.studentlibrary.ru/ru/doc/ISBN9785927535774-SCN0000/000.html>

3. Платонов В.В. «Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей»: учебное пособие для вузов - М.: Академия, 2006.

в) ресурсы сети «Интернет»

1. <http://netacad.com>
2. <http://cisco.com>
3. <http://learningnetwork.cisco.com/>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- компьютерный класс, оборудованный ПЭВМ класса не ниже Intel i5-7400, 8gb RAM, 1Tb HDD с установленным программным обеспечением: Windows 7/8/10, Linux, Packet Tracer 8.0 (и новее), Cisco SDM, Cisco Network Assistant, Cisco Configuration Professional. Из расчета одна ПЭВМ на одного человека.
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

Ассистент кафедры нелинейной динамики

О.Е. Бизин

Приложение № 1 к рабочей программе дисциплины «Безопасность компьютерных сетей»

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Пример задания для самостоятельной практической работы
(Задания размещаются в ЭУК «Компьютерные сети» в LMS Moodle и выполняются в программе эмуляции сети «Cisco Packet Tracer (доступен бесплатно для участников Программы Сетевой Академии Cisco)»)

Во время выполнения работы студент может видеть свой прогресс в процентном соотношении. Большинство работ сопровождаются методическими материалами.

Тема: Настройка и проверка Site-to-Site IPsec VPN
(в части внедрения Site-to-Site IPsec VPN))

Цели:

Проверьте подключение по всей сети.

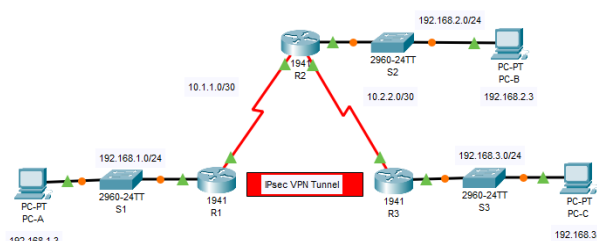
Настройте R1 для поддержки межсайтовой IPsec VPN с R3.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

- Verify connectivity throughout the network.
- Configure R1 to support a site-to-site IPsec VPN with R3.



Правила интерпретации результатов выполнения самостоятельной практической работы:

Практическая работа считается выполненной (засчитывается), если достигнуты все поставленные цели.

Пример теста для самопроверки
(тест проводится в ЭУК «Компьютерные сети» в LMS NetAcad)

В тесте представлены задания на проверку знаний по теме «Базовая конфигурация коммутатора и оконечного устройства». В тесте по каждой теме в среднем 15 вопросов.

Количество попыток выполнения не ограничено.

Время на прохождение теста не ограничено.

Итоги прохождения теста не оцениваются.

Вопросы теста:

1. При применении ACL к интерфейсу маршрутизатора какой трафик обозначается как исходящий?

- Трафик, который идет с IP-адреса назначения на маршрутизатор
- Трафик, который покидает маршрутизатор и направляется к узлу назначения
- Трафик, для которого маршрутизатор не может найти запись в таблице маршрутизации
- Трафик, поступающий с исходного IP-адреса на маршрутизатор

2. Как быстрее всего удалить одну запись ACE из именованного ACL?

- Скопируйте ACL в текстовый редактор, удалите ACE, затем скопируйте ACL обратно в маршрутизатор.
- Используйте ключевое слово *no* и порядковый номер ACE, который нужно удалить.
- Используйте команду *no access-list*, чтобы удалить весь ACL, а затем воссоздайте его без ACE.
- Создайте новый ACL с другим номером и примените новый ACL к интерфейсу маршрутизатора.

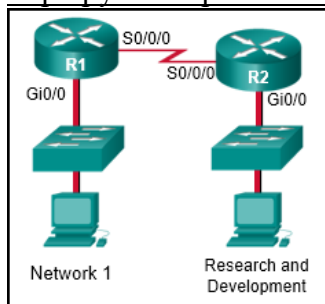
3. Входящие сообщения ICMP какого типа следует блокировать?

- Недостижимый
- Гашение источника
- Эхо-ответ
- Эхо

4. Какой сценарий приведет к неправильной настройке ACL и запрету всего трафика?

- Примените именованный ACL к линии VTY.
- Примените стандартный ACL во входящем направлении.
- Примените стандартный ACL с помощью команды *ip access-group out*.
- Примените ACL, в котором есть все *запрещающие* операторы ACE.

5. Сетевой администратор хочет создать стандартный ACL, чтобы предотвратить передачу трафика Сети 1 в сеть исследований и разработок. На каком интерфейсе маршрутизатора и в каком направлении следует применять стандартный ACL?



- R1 S0/0/0 исходящий

- R2 G0/0 входящий
- R2 S0/0/0 входящий
- R1 G0/0 входящий
- R1 G0/0 исходящий
- R2 G0/0 исходящий

6. Какие два утверждения описывают соответствующие общие рекомендации по настройке и применению ACL? (Выберите два.)

- Наиболее специфичные операторы ACL следует вводить первыми из-за последовательного характера списков ACL сверху вниз.
- Если ACL не содержит **разрешений**, весь трафик по умолчанию запрещается.
- К интерфейсу можно применить несколько ACL для каждого протокола и направления.
- Если один ACL должен применяться к нескольким интерфейсам, он должен быть настроен с уникальным номером для каждого интерфейса.
- Стандартные списки ACL располагаются ближе всего к источнику, тогда как расширенные ACL располагаются ближе всего к месту назначения.

7. Какая обратная маска будет соответствовать сетям с 172.16.0.0 по 172.19.0.0?

- 0.0.3.255
- 0.3.255.255
- 0.252.255.255
- 0.0.255.255

8. Какой оператор используется в настройке ACL для сопоставления пакетов определенного приложения?

- gt
- established
- eq
- lt

Правильные ответы

Вопрос №	Вариант ответа		Вопрос №	Вариант ответа
1	2		5	6
2	2		6	1,2
3	4		7	2
4	4		8	3

Самостоятельные работы в виде тестовых заданий.

Тесты проводятся в ЭУК «Компьютерные сети» в LMS NetAcad

В каждом тесте в среднем 30 вопросов по пройденным темам (2-4).

Количество попыток выполнения - 5. Время на прохождение теста - 1,5 часа.

При завершении теста показываются ошибки (если есть) и какую тему и раздел смотреть, чтобы разобраться и исправить ошибку. Итоги прохождения теста оцениваются.

(в части знаний о возможных сетевых атаках и методах борьбы с ними, возможностях различных типов брандмауэров)

Примеры вопросов:

1. Какие две части информации требуются при создании стандартного списка контроля доступа? (Выберите два.)

- номер списка доступа от 1 до 99
- исходный адрес и обратная маска
- адрес назначения и подстановочная маска
- маска подсети и подстановочная маска
- номер списка доступа от 100 до 199

2. Какие два шага обеспечивают самый быстрый способ полного удаления ACL-списка с маршрутизатора? (Выберите два.)

- Удаление ACE — единственный необходимый шаг.
- Измените номер ACL, чтобы он не совпадал с ACL, связанным с интерфейсом.
- Скопируйте ACL в текстовый редактор, добавьте по перед каждым ACE, затем скопируйте ACL обратно в маршрутизатор.
- Удалите входящую/исходящую ссылку на ACL из интерфейса.
- Используйте команду no access-list для удаления всего ACL.
- Используйте ключевое слово no и порядковый номер каждого ACE в именованном ACL, который нужно удалить.

3. Какие два типа адресов следует запрещать входящим на интерфейс маршрутизатора, подключенный к Интернету? (Выберите два.)

- частные IP-адреса
- любой IP-адрес, начинающийся с цифры 127
- любой IP-адрес, начинающийся с цифры 1
- IP-адреса, переведенные с помощью NAT
- общедоступные IP-адреса

4. Каковы два возможных ограничения использования брандмауэра в сети? (Выберите два.)

- Он обеспечивает доступ к приложениям и конфиденциальным ресурсам для внешних ненадежных пользователей.
- Это усложняет управление безопасностью, поскольку требует разгрузки управления сетевым доступом к устройству.
- Неправильно настроенный брандмауэр может создать единую точку отказа.
- Производительность сети может снизиться.
- Он не может дезинфицировать потоки протоколов.

5. Брандмауэр какого типа использует прокси-сервер для подключения к удаленным серверам от имени клиентов?

- межсетевой экран с отслеживанием состояния
- межсетевой экран без сохранения состояния
- межсетевой экран с фильтрацией пакетов
- брандмауэр шлюза приложений

6. Какие два утверждения описывают две модели конфигурации межсетевых экранов Cisco IOS? (Выберите два.)

- ZPF должен быть включен в конфигурации маршрутизатора перед включением классического брандмауэра IOS.
- Классический брандмауэр IOS и ZPF не могут быть объединены на одном интерфейсе.
- Классические брандмауэры IOS и модели ZPF могут быть включены на маршрутизаторе одновременно.

- Обе модели IOS Classic Firewall и ZPF требуют ACL для определения политик фильтрации трафика.
- Перед включением ZPF необходимо включить классические брандмауэры IOS в конфигурации маршрутизатора.

7. Специалист по безопасности разрабатывает ACL, чтобы запретить доступ к веб-серверу всем сотрудникам отдела продаж. Персоналу отдела продаж назначается адресация из подсети IPv6 2001:db8:48:2c::/64. Веб-серверу назначается адрес 2001:db8:48:1c::50/64. Какие три команды потребуются для настройки списка контроля доступа WebFilter на интерфейсе LAN для торгового персонала? (Выберите три.)

- permit tcp any host 2001:db8:48:1c::50 eq 80
- deny tcp host 2001:db8:48:1c::50 any eq 80
- deny tcp any host 2001:db8:48:1c::50 eq 80
- permit ipv6 any any
- deny ipv6 any any
- ip access-group WebFilter in
- ipv6 traffic-filter WebFilter in

8. Каковы два различия между межсетевыми экранами с сохранением состояния и без сохранения состояния? (Выберите два.)

- Брандмауэр без сохранения состояния может фильтровать сеансы, использующие динамическое согласование портов, в то время как брандмауэр с отслеживанием состояния не может.
- Брандмауэр без сохранения состояния будет проверять каждый пакет отдельно, в то время как межсетевой экран с отслеживанием состояния наблюдает за состоянием соединения.
- Брандмауэр без сохранения состояния предоставляет больше информации для журналов, чем брандмауэр с отслеживанием состояния.
- Брандмауэр с отслеживанием состояния предотвратит спуфинг, определив, принадлежат ли пакеты существующему соединению, в то время как брандмауэр без сохранения состояния следует предварительно настроенным наборам правил.
- Брандмауэр без сохранения состояния обеспечивает более строгий контроль над безопасностью, чем брандмауэр с отслеживанием состояния.

9. В чем преимущество HIPS, которого нет в IDS?

- Система HIPS обеспечивает быстрый анализ событий посредством подробного ведения журналов.
- HIPS развертывает датчики в точках входа в сеть и защищает критически важные сегменты сети.
- HIPS отслеживает сетевые процессы и защищает важные файлы.
- HIPS защищает важные системные ресурсы и отслеживает процессы операционной системы.

10. Какую информацию должна отслеживать IPS, чтобы обнаруживать атаки, соответствующие составной сигнатуре?

- общее количество пакетов в атаке
- состояние пакетов, связанных с атакой
- период атаки, используемый злоумышленником
- пропускная способность сети, потребляемая всеми пакетами

11. Какой инструмент может выполнять анализ трафика и портов в реальном времени, а также обнаруживать сканирование портов, снятие отпечатков и атаки переполнения буфера?

- SIEM
- Nmap
- Snort
- Netflow

12. Какая процедура рекомендуется для снижения вероятности спуфинга ARP?

- Включение отслеживания DHCP для выбранных VLAN.
- Включение IP Source Guard на доверенных портах.
- Включение DAI в VLAN управления.
- Включение защиты портов глобально.

Правила выставления оценки по результатам самостоятельной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное

- задание с 1 вариантом ответа – 1 балл;
- задание с множественным выбором – 2 балла, 1 балл - если только один ответ верный, 0 баллов – если нет правильных ответов или выбрано больше вариантов, чем необходимо;
- задание с сопоставлением – 2 балла.

Полностью неправильно выполненное задание – 0 баллов.

Набранное количество баллов интерпретируется в процентное соотношение и оценивается. От 70-100% - работа засчитана, менее 70% – работа не засчитана (знания и умения на данном этапе освоения дисциплины не сформированы).

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

На момент проведения промежуточной аттестации должно быть выполнено и засчитано не менее 70% домашних работ.

Правила выставления оценки на экзамене.

Экзамен состоит из двух частей.

1 часть:

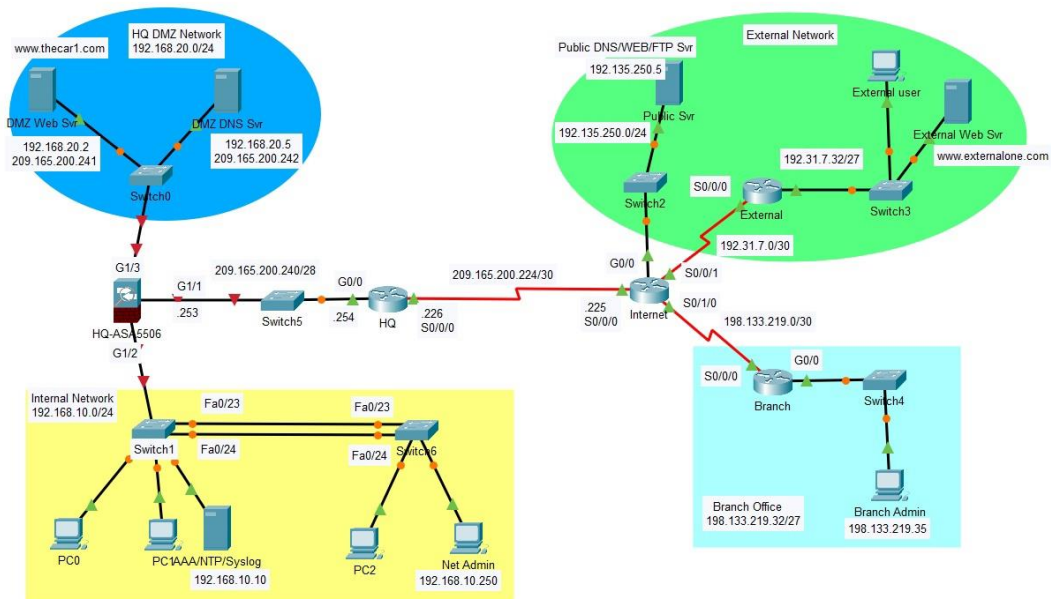
Выполнение практической работы в программе Cisco Packet Tracer.

Цели:

Настроить брандмауэр ASA для реализации политик безопасности.

Настроить безопасность уровня 2 на коммутаторе локальной сети.

Настроить межсайтовый IPsec VPN.



Каждая цель включает в себя определенное количество настроек, которые необходимо выполнить. За каждую верно выполненную настройку начисляются баллы. Максимальное количество баллов – 95. Набранные баллы интерпретируются в проценты от максимального количества баллов.

Работа считается выполненной если студент выполнил 70% требования.

Временное ограничение на выполнение практической работы – 90 минут.

При условии успешного выполнения работы студент переходит ко второй части экзамена.

2 часть:

Итоговый тест

В тесте представлены задания на проверку знаний по курсу «Основы построения защищенных компьютерных сетей». В тесте в среднем 60 вопросов.

Количество попыток выполнения - 1.

Время на прохождение теста – 90 минут.

Примеры вопросов:

1. Сетевой администратор настраивает реализацию AAA на устройстве ASA.

На что указывает опция link3?

```
ciscoasa# config terminal
ciscoasa(config)# aaa-server TACACS-GRP protocol tacacs+
ciscoasa(config-aaa-server-group)# aaa-server TACACS-GRP (link3) host 192.168.1.10
ciscoasa(config-aaa-server-group)# exit
```

- сетевое имя, в котором находится сервер AAA
- конкретное имя сервера AAA
- последовательность серверов в группе серверов AAA
- имя интерфейса

2. Что обеспечивает безопасную сегментацию и защиту от угроз в решении Secure Data Center?

- Программное обеспечение Cisco Security Manager
- AAA-сервер
- Адаптивное устройство безопасности

- Система предотвращения вторжений

3. Что будет результатом неудачных попыток входа в систему, если на маршрутизаторе будет введена следующая команда?

login block-for 150 attempts 4 within 90

- Все попытки входа будут заблокированы на 150 секунд, если в течение 90 секунд будет 4 неудачных попытки.
- Все попытки входа будут заблокированы на 90 секунд, если в течение 150 секунд будет 4 неудачных попытки.
- Все попытки входа будут заблокированы на 1,5 часа при 4 неудачных попытках в течение 150 секунд.
- Все попытки входа будут заблокированы на 4 часа, если в течение 150 секунд будет 90 неудачных попыток.

4. Какие две меры безопасности используются для защиты конечных точек в сети без границ? (Выберите два.)

- denylisting
- Snort IPS
- DLP
- DMZ
- rootkit

5. Какие три типа трафика разрешены, когда была введена команда authentication port-control auto, а клиент еще не прошел аутентификацию? (Выберите три.)

- CDP
- 802.1Q
- IPsec
- TACACS+
- STP
- EAPOL

6. Рассмотрим команду списка доступа, применяемую для исходящего трафика на последовательном интерфейсе маршрутизатора.

access-list 100 deny icmp 192.168.10.0 0.0.0.255 any echo reply

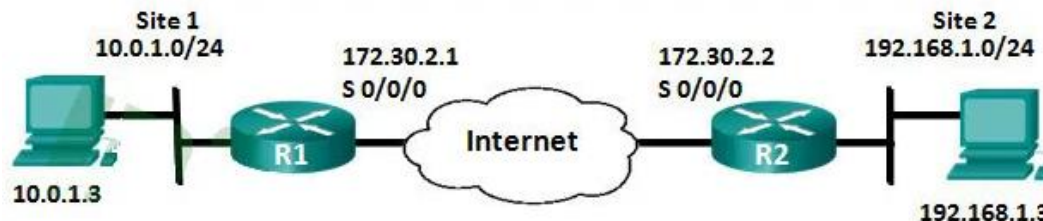
Какой эффект от применения этой команды списка доступа?

- Единственный запрещенный трафик — это эхо-ответы из сети 192.168.10.0/24. Весь остальной трафик разрешен.
- Единственным запрещенным трафиком является трафик на основе ICMP. Весь остальной трафик разрешен.
- Исходящий трафик через последовательный интерфейс запрещен.
- Пользователям в сети 192.168.10.0/24 не разрешается передавать трафик в любое другое место назначения.

7. Какие две функции включены в протоколы TACACS+ и RADIUS? (Выберите два.)

- SIP-поддержка
- шифрование пароля
- поддержка 802.1X
- отдельные процессы аутентификации и авторизации
- использование протоколов транспортного уровня

8. Какой вывод можно сделать из вывода команды `show crypto map`, показанного на маршрутизаторе R1?



```

R1# show crypto map
    Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "R1-R2_MAP" 10 ipsec-isakmp
    Peer = 172.30.2.2
    Extended IP access list 101
        access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
    Current peer: 172.30.2.2
    Security association lifetime: 4608000 kilobytes/900 seconds
    Responder-Only (Y/N): N
    PFS (Y/N): Y
    DH group: group24
    Mixed-mode : Disabled
    Transform sets={
        R1-R2: { esp-aes esp-sha-hmac } ,
    }
    Interfaces using crypto map R1-R2_MAP:
R1#

```

- Криптокарта еще не применена к интерфейсу.
- Текущий IP-адрес однорангового узла должен быть 172.30.2.1.
- Существует несоответствие между наборами преобразования.
- Конфигурация туннеля установлена и может быть протестирована с помощью расширенных эхо-запросов.

Экзаменационная оценка выставляется по итогам теста по правилам:

В случае невыполнения практической работы (часть 1 экзамена) студенту выставляется оценка «неудовлетворительно».

Итоги прохождения теста оцениваются следующим образом:

- задание с 1 вариантом ответа – 1 балл;
- задание с множественным выбором – 2 балла, 1 балл - если только один ответ верный, 0 баллов – если нет правильных ответов или выбрано больше вариантов, чем необходимо;
- задание с сопоставлением – 2 балла.

Полностью неправильно выполненное задание – 0 баллов.

В среднем, максимальное количество баллов по итогам финального теста – 100

Набранное количество баллов интерпретируется в процентное соотношение и оценивается. От 90-100% соответствует оценке «отлично», 80-90% – оценке «хорошо», 70-80% – оценке «удовлетворительно», менее 70% – оценка «неудовлетворительно» (знания и умения на данном этапе освоения дисциплины не сформированы).

Приложение № 2 к рабочей программе дисциплины «Безопасность компьютерных сетей»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Основы построения защищенных компьютерных сетей» являются лекции и практические работы, причем в достаточно большом объеме. Это связано с тем, что в основе курса «Основы построения защищенных компьютерных сетей» лежат самые современные теоретические и практические знания и навыки. По всем темам предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам и отработка навыков работы с сетевым оборудованием.

Для успешного освоения дисциплины очень важно решение достаточно большого количества теоретических и практических работ, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения работ разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения теоретических и практических работ – помочь усвоить фундаментальные понятия и основы компьютерных сетей.

Задания для самостоятельного решения формулируются на лекциях и практических занятиях. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач. Полный список заданий для самостоятельной работы по темам (разделам) дисциплины приведен в ЭУК в LMS Moodle «Основы построения защищенных компьютерных сетей» и ЭУК в LMS NetAcad. Вопросы, возникающие в процессе или по итогам решения этих задач, можно задать на консультациях или в форуме (чате) в ЭУК в LMS Moodle.

Для самостоятельной работы, в том числе и повтора, разобранного на лекциях и практических занятиях материала первого семестра изучения дисциплины, рекомендуется использовать учебно-методическое пособие в LMS NetAcad. Материал каждого раздела включает в себя изложение теоретического материала по заданной теме, который затем иллюстрируется подробным решением типичных задач. В заключение каждого раздела приводятся задания для самостоятельного решения, ответы к этим заданиям и указания по их решению показываются после их выполнения.

В конце изучения дисциплины студенты сдают экзамен.

Экзамен принимается в виде теста и практической работы в программе Cisco Packet Tracer. Проверяются знания, полученные в ходе прохождения курса, навыки и умения, применяемые для построения сети и обеспечения достаточно высокого уровня безопасности ее работы.