

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Проректор по науке

и международным связям

А.В. Толстиков

2 марта 2020 г.



АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

Рабочая программа

для обучающихся по направлению подготовки: 10.06.01 Информационная безопасность

Профиль (направленность):

Методы и системы защиты информации, информационная безопасность
форма обучения (очная)

Захаров А.А. Администрирование компьютерных сетей. Рабочая программа для обучающихся по направлению подготовки 10.06.01 Информационная безопасность, профиль (направленность): методы и системы защиты информации, информационная безопасность, форма обучения (очная). Тюмень, 2020.

Рабочая программа дисциплины (модуля) Администрирование компьютерных сетей опубликована на сайте ТюмГУ: [электронный ресурс] / Режим доступа: <https://www.utmn.ru/sveden/education/#>

1. Пояснительная записка

Целью изучения дисциплины «Администрирование компьютерных сетей» является теоретическая и практическая подготовка специалистов в области разработки и эксплуатации компьютерных сетей с учетом требований по обеспечению информационной безопасности.

В **задачи** дисциплины «Администрирование компьютерных сетей» входит формирование необходимого минимума специальных теоретических знаний и практических навыков по следующим аспектам:

- проектирование компьютерных сетей;
- эксплуатация компьютерных сетей;
- обеспечение информационной безопасности компьютерных сетей.

1.1. Место дисциплины в структуре образовательной программы

Данная дисциплина «Администрирование компьютерных сетей» входит в Б1 Блок 1 «Дисциплины (модули)» вариативной части (дисциплины по выбору) Б1.В.ДВ.1.

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

- «Основы информационной безопасности» – знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации, владение профессиональной терминологией в области информационной безопасности;
- «Администрирование и управление безопасностью в открытых информационных системах» – знание принципов построения современных средств защиты информации, порядок и специфику их применения в информационных системах;
- «Архитектура современных вычислительных систем» – знание методов и средств построения программно-аппаратных технологий и систем передачи информации;
- «Системы и сети передачи информации» – знание технологий передачи данных в сетях общего доступа, владение терминологией компьютерных сетей;

Курс «Администрирование компьютерных сетей» является предшествующей для изучения такой дисциплины как «Методы и системы защиты информации, информационная безопасность».

Знания и практические навыки, полученные в процессе изучения дисциплины «Администрирование компьютерных сетей», используются аспирантами в научно-исследовательской и педагогической работе.

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (модуля)

Код и наименование компетенции	Компонент (знаниевый/функциональный)
ПК-2 - способность к разработке и реализации принципов и решений (технических, математических, организационных и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.	знает - свойства информации, подлежащие закрытию; - этапы развития средств и технологий коммуникаций; - историю развития информационного противоборства в России и мире. умеет - ориентироваться в истории технологий передачи информации, - методах защиты информации в контексте исторического развития.
ПК-7 - способность к анализу рисков нарушения информационной	знает - основные стандарты, используемые при передаче

безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.	цифровой информации; - основные технологии защиты информации. -основные технологии передачи цифровой информации; - назначение основных устройств (маршрутизаторов, коммутаторов) обеспечивающих передачу цифровой информации. умеет - создавать, безопасное подключение LAN к Интернет. - создавать и настраивать LAN сети.
ПК-10 - способность к созданию новых и совершенствованию существующих технологий идентификации и аутентификации пользователей и субъектов информационных процессов.	Знает - основные методы научно-исследовательской деятельности. Умеет - выделять и систематизировать основные идеи в научных текстах; -критически оценивать любую поступающую информацию, вне зависимости от источника; -обходиться без применения стандартных методов при решении задач.

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	Всего часов (академические часы)	Часов в семестре (академические часы)
		3
Общий объем зач. ед. час.	5	5
	180	180
Из них:		
Часы аудиторной работы (всего):	54	54
Лекции	36	36
Практические занятия	18	18
Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	126	126
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		Зачет

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) системы.

Оценка аспиранта в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения аспирантом заданий во время лабораторных работ, индивидуальных домашних заданий, контрольной работы. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных аспирантом в ходе изучения дисциплины. При количестве набранных баллов 61 и более ставится оценка "зачтено", иначе ставится "не зачтено". Аспирант, не получивший зачета, имеет право на пересдачу.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контак тной работы
			Лекции	Практические занятия	Лабораторные/пр актические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Проектирование сетей типа LAN. Сетевое оборудование. Настройка сетевого оборудования	30	6	4	0	0
2.	Построение компьютерной сети	30	6	2	0	0
3.	Внедрение VLAN. Внедрение SpanningTree	30	6	2	0	0
4.	Концепция безопасности компьютерных сетей. Средства обеспечения безопасности компьютерных сетей	30	6	4	0	0
5.	Списки контроля доступа. Удаленный доступ	30	6	4	0	0
6.	Безопасность корпоративных сетей	28	6	2	0	0
7.	Зачет	2	0	0	0	2
	Итого (часов)	180	36	18	0	2

4.2. Содержание дисциплины (модуля) по темам

Тема 1. Проектирование сетей типа LAN. Сетевое оборудование. Настройка сетевого оборудования.

Основные понятия и определения. Типы коммуникаций. Виды информации, подлежащие закрытию, их модели и свойства. Основные этапы становления защищенных коммуникаций. Специальная терминология.

Тема 2. Построение компьютерной сети.

Возникновение LAN. Топологии, архитектуры и технологии. Ethernet. Стандарты. История разработки оборудования для сетевого взаимодействия. Классы IP адресов и маски подсетей по умолчанию. Статический адрес. Динамические адреса. Протокол Dynamic Host Configuration Protocol (DHCP).

Тема 3. Внедрение VLAN. Внедрение SpanningTree.

Коммутация. Режимы потоков трафика. Виртуальные сети. Описание сети. Назначение и принципы работы STP. Достоинства и недостатки протокола.

Тема 4. Концепция безопасности компьютерных сетей. Средства обеспечения безопасности компьютерных сетей.

Наивный подход. Криптография. Кодирование и скрытие информации. Понятие о стеганографии. Аналоговые технологии передачи информации. Цифровая информация. Аппаратное обеспечение – виды сетевых адаптеров. Программное обеспечение. Операционные системы

Тема 5. Списки контроля доступа. Удаленный доступ.

Проектирование поддержки удаленного сотрудника. Формирование списков контроля доступа на маршрутизаторе. Типы списков доступа: стандартные, расширенные, именованные.

Тема 6. Безопасность корпоративных сетей.

Внешние угрозы. Внутренние угрозы. Социотехника. Фишинг. Телефонный фишинг. Вирусы, черви, троянские кони. DoS атаки. Политика безопасности. Антивирусное ПО. Межсетевой экран. Демилитаризованная зона (DMZ).

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Проектирование сетей типа LAN. Сетевое оборудование. Настройка сетевого оборудования	Чтение обязательной литературы, подготовка к практическим занятиям
2.	Построение компьютерной сети	Чтение обязательной литературы, подготовка к практическим занятиям
3.	Внедрение VLAN. Внедрение SpanningTree.	Чтение обязательной литературы, подготовка к практическим занятиям
4.	Концепция безопасности компьютерных сетей. Средства обеспечения безопасности компьютерных сетей	Чтение обязательной литературы, подготовка к практическим занятиям
5.	Списки контроля доступа. Удаленный доступ	Чтение обязательной литературы, подготовка к практическим занятиям
6.	Безопасность корпоративных сетей	Чтение обязательной литературы, подготовка к практическим занятиям

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Разбор примеров контрольных работ.

Контроль за самостоятельной работой осуществляется при выполнении обучающимся теста, контрольной работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет - проводится в виде контрольной работы.

Пример задания: Вариант контрольной работы содержит 2 вопроса из списка примерных вопросов и 1 практическое задание.

Теоретическая часть:

Вопросы к зачету

1. Сферы применения сетевых технологий, основные компоненты сети.
 2. Классификация сетей: размер, архитектура подключения, тип инфраструктуры. Понятие конвергентности.
 3. Cisco IOS: назначение, доступ, режимы.
 4. Базовая настройка устройств. Ограничение доступа к устройствам.
 5. Сетевые протоколы: назначение, виды. Взаимодействие протоколов. Примеры.
 6. Модель TCP/IP.
 7. Эталонная модель OSI. Структура и назначение уровней.
 8. Инкапсуляция данных. Понятие PDU. Примеры.
 9. Физический уровень модели OSI: назначение, характеристики.
 10. Виды сетевых средств подключения.
 11. Канальный уровень модели OSI. PDU 2 уровня.
 12. Физическая и логическая топологии сети, примеры.
 13. Протокол Ethernet. MAC-адрес Ethernet: назначение, представление, виды.
 14. Предотвращение сетевых атак. Примеры.
 15. Коммутатор: назначение, настройка, таблица адресов, принцип работы.
 16. Протокол ARP. Распознавание адресов в сети
 17. Маршрутизатор: назначение, настройка, таблица адресов, принцип работы.
 18. Тестирование сетевых соединений, проверка доступности. Протокол ICMP.
- Команды PING, TRACERT.
19. Сетевой уровень модели OSI. Протокол IP. PDU 3 уровня.
 20. Виды сетевых атак. Примеры.
 21. Понятие маршрутизации. Структура и назначение таблицы маршрутизации.
- Шлюз по умолчанию.
22. Безопасность компонентов сети. Примеры.
 23. Сетевая безопасность. Основные типы угроз. Физическая безопасность.
 24. Сравнение IPv6 с IPv4. Структура и представление адресов. Префикс IPv6.
 25. IPv4. Структура и представление адресов. Виды рассылки. Типы адресов. Маска подсети.
 26. Сегментация сети. Широковещательные домены.
 27. Транспортный уровень модели OSI. Протоколы TCP, UDP. Обмен данных по протоколу TCP.
 28. Планирование адресации. Разбиение сети на подсети на простом примере.
 29. Уровень приложений модели TCP/IP. Примеры и описание протоколов уровня приложений TCP/IP для передачи веб-трафика, почты, файлов.
 30. Топологии небольших сетей. Выбор устройств при построении сети компании.
 31. Поиск и устранение неполадок в сети. Основные подходы. Неполадки в работе кабелей и интерфейсов.
 32. Режимы работы Cisco IOS. Структура команд IOS. Примеры команд.

Примеры практических заданий:

1) Маршрутизатор с двумя интерфейсами LAN, двумя интерфейсами WAN и одним настроенным интерфейсом обратной связи (loopback) работает с протоколом маршрутизации OSPF. Что процесс OSPF маршрутизатора использует для назначения маршрутизатору идентификатора?

- IP-адрес интерфейса, настроенного с приоритетом 0
- идентификатор области OSPF, заданный на интерфейсе с самым высоким IP-адресом
- IP-адрес интерфейса обратной связи
- самый высокий IP-адрес, настроенный на интерфейсах LAN
- самый высокий IP-адрес на интерфейсах WAN

2) Какие меры используются для предотвращения петель маршрутизации в сетях, в которых используются протоколы маршрутизации на базе вектора расстояния? (Выберите два варианта).

- объявления о состоянии канала (LSA)
- протокол связующего дерева
- дерево SPF
- разделение горизонта (split horizon)
- таймеры удержания (hold-down timer)

3) В каком варианте представлено наилучшее описание протоколов маршрутизации на базе вектора расстояния?

- в качестве единственной метрики они используют подсчет переходов (hop).
- они отправляют обновления только при добавлении новой сети.
- они отправляют свои таблицы маршрутизации к напрямую подключенным соседним маршрутизаторам.
- они рассылают обновление маршрутизации по всей сети.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ПК-2 - способность к разработке и реализации принципов и решений (технических, математических, организационных и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.	Знает - свойства информации, подлежащие закрытию; - этапы развития средств и технологий коммуникаций; - историю развития информационного противоборства в России и мире. - основные стандарты, используемые при передаче цифровой информации; - основные технологии защиты информации. - основные технологии передачи цифровой информации;	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-7 - способность к анализу рисков нарушения информационной безопасности и уязвимости	- назначение основных устройств (маршрутизаторов, коммутаторов) обеспечивающих	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и

процессов переработки информации в информационных системах любого вида и области применения.	передачу цифровой информации. Умеет - ориентироваться в истории технологий передачи информации, - методах защиты информации в контексте исторического развития.	открытый, 10 заданий, - Задачи	правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
ПК-10 - способность к созданию новых и совершенствованию существующих технологий идентификации и аутентификации пользователей и субъектов информационных процессов.	- Создавать, безопасное подключение LAN к Интернет. - создавать и настраивать LAN сети.	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Петренко, С. А. Политики безопасности компании при работе в Интернет / Петренко С.А., Курбатов В.А., - 3-е изд., (эл.) - Москва :ДМК Пресс, 2018. - 397 с.: ISBN 978-5-93700-057-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/983161> (дата обращения: 01.03.2020). – Режим доступа: по подписке.

2. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1167736> (дата обращения: 01.03.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

3. Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100346> (дата обращения: 01.03.2020). — Режим доступа: для авториз. пользователей.

4. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 428 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100370> (дата обращения: 01.03.2020). — Режим доступа: для авториз. пользователей.

5. Басыня, Е. А. Сетевая информационная безопасность и анонимизация : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2016. — 76 с. — ISBN 978-5-7782-3107-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/91519.html> (дата обращения: 01.03.2020). — Режим доступа: для авторизир. пользователей

6. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков ; под редакцией Н. И. Синадский. — Екатеринбург : Уральский федеральный университет, ЭБС АСВ, 2014. — 180 с. — ISBN 978-5-7996-1201-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/65983.html> (дата обращения: 01.03.2020). — Режим доступа: для авторизир. пользователей

7.3. Интернет-ресурсы

1. Интернет ресурсы Academy Cisco <http://netacad.com>

7.4. Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) <https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true>
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) <https://icdlib.nspu.ru/>
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА <https://rusneb.ru/>
- Справочная правовая система КонсультантПлюс <http://www.consultant.ru/>

Наименование ПО

- Microsoft Office 365
- "Microsoft Imagine Academy (панель Dreamspark):MS Visual Studio, MS SQL Server, ОС семейства MS Windows, MS Visio, MS Project"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- эмулятор сетей PacketTracer.версия 7.x;
- эмулятор сетей GNS3 2.*
- эмулятор сетей eNSP 1.3.*
- гипервизор Oracle Virtual Box 5.*
- платформа для электронного обучения Microsoft Teams

Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Компьютерный класс с выходом в интернет и стандартное лабораторное и периферийное оборудование классом не ниже чем в приведенной ниже конфигурации.

- 3 маршрутизатора Cisco 2801 с Base IP IOS, 128 Мбайт DRAM, 32 Мбайта флэш-памяти и модулями HWIC-2A/S;
- 3 коммутатора Cisco Catalyst 2960;
- Набор последовательных кабелей и витой пары;
- 2 беспроводных маршрутизатора Linksys (предпочтительно Linksys WRT150N; допустимо использование моделей WRT54G, WRT300N и WRT350N) или аналогичные устройства SOHO;

Для проведения лекционных и практических занятий необходим проектор с разрешением не менее 800x1200 подключенный к компьютеру с выходом в Интернет.