Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Уральский государственный лесотехнический университет»
Социально-экономический институт
Кафедра интеллектуальных систем

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

включая фонд оценочных средств и методические указания
для самостоятельной работы обучающихся

Б1.В.ДЭ.02.01 – ЗАЩИЩЕННЫЕ СЕТЕВЫЕ ПРОТОКОЛЫ

Направление подготовки – 09.03.03 Прикладная информатика
Направленность (профиль) – Администрирование информационных систем
Квалификация – бакалавр
Количество зачётных единиц (часов) – 3 (108)

г. Екатеринбург, 2023

Разработчики:
К.с.-х.н, доцент А.И.Чермных

Рабочая программа утверждена на заседании кафедры интеллектуальных систем (протокол №6 от «01» февраля 2023 г.

Заведующий кафедрой В.В.Побединский

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией социально-экономического института
(протокол №2 от «02» марта 2023 года)

Председатель методической комиссии СЭИ А.В. Чевардин

Рабочая программа утверждена директором социально-экономического института

Директор СЭИ Ю.А. Капустина
«02» марта 2023 г.

Оглавление

1. Общие положения

Дисциплина «Защищенные сетевые протоколы» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, блока Б1 «Дисциплины (модули)» учебного плана, входящего в состав образовательной программы высшего образования 09.03.03 «Прикладная информатика» (профиль «Администрирование информационных систем»).

Нормативно-методической базой для разработки рабочей программы учебной дисциплины «Защищенные сетевые протоколы» являются:

– Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ;

– Приказ Министерства науки и высшего образования Российской Федерации от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;

– Приказ Министерства труда и социальной защиты Российской Федерации от 18.11.2014 г. №896н «Об утверждении профессионального стандарта «Специалист по информационным системам»;

– Федеральный государственный образовательный стандарт высшего образования – бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утвержденный приказом Министерства образования и науки Российской Федерации от 19.09.2017№ 922, с изменениями, внесенными приказами Министерства науки и высшего образования Российской Федерации от 26.11.2020 №1456, от 08.02.2021 №83, от 19.07.2022 №662, от 27.02.2023 №208;

– Учебный план образовательной программы высшего образования направления 09.03.03 «Прикладная информатика» (профиль «Администрирование информационных систем») подготовки бакалавров по очной форме обучения, одобренный Ученым советом УГЛТУ (протокол № 3 от 16.03.2023), с дополнениями и изменениями, утвержденными на заседании Ученого совета УГЛТУ (протокол от 20.04.2023 №4), введенными приказом УГЛТУ от 28.04.2023 №302-А.

Обучение по образовательной программе 09.03.03 «Прикладная информатика» (профиль «Администрирование информационных систем») осуществляется на русском языке.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемыми результатами обучения по дисциплине являются знания, умения, владения и/или опыт деятельности, характеризующие этапы/уровни формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы в целом.

Цели и задачи курса

Цели курса: формирование у студентов профессиональных знаний и умений, связанных с использованием методов построения криптографических протоколов, обеспечивающих защищённую передачу данных между узлами.

Задачи дисциплины:

– изучение основ шифрования и его практического применения в компьютерных сетях;

– формирование умений по обеспечению безопасности в сети Интернет;

– изучение основных методов построения защищенных протоколов передачи данных.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-3 – Способен настраивать оборудование, необходимое для работы ИС.

В результате изучения дисциплины студент должен:

знать:

– сетевые протоколы, иерархию протоколов и режимы их работы, стандарты, соглашения и рекомендации в области компьютерных сетей, методы передачи защищенной информации в сетях;

– основные требования информационной безопасности;

– основы криптографии и алгоритмов шифрования;

уметь:

– настраивать сетевые протоколы в зависимости от прикладных задач;

– устанавливать и настраивать параметры защищенных протоколов;

– обнаруживать и устранять ошибки при передаче данных;

владеть:

– методами построениями защищенной сети передачи данных.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Защищенные сетевые протоколы» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, блока Б1 «Дисциплины (модули)» учебного плана, что означает формирование в процессе обучения у бакалавра компетенций в рамках выбранного профиля подготовки.

Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин ОПОП и написания выпускной квалификационной работы.

Перечень обеспечивающих, сопутствующих и обеспечиваемых дисциплин

Обеспечивающие дисциплины	Сопутствующие дисциплины	Обеспечиваемые дисциплины
Компьютерные сети и телекоммуникации Архитектура вычислительных машин и систем	Сетевое администрирование Проектирование информационно-коммуникационных систем Производственная практика (технологическая (проектно-технологическая практика))	Информационная безопасность Выполнение и защита выпускной квалификационной работы

Указанные связи дисциплины дают обучающемуся системное представление о комплексе изучаемых дисциплин в соответствии с ФГОС ВО, что обеспечивает требуемый теоретический уровень и практическую направленность в системе обучения и будущей деятельности выпускника.

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины

Вид учебной работы	Всего академических часов
Контактная работа с преподавателем*:	**38,25**
лекции (Л)	12
практические занятия (ПЗ)	-
лабораторные работы (ЛР)	26
иные виды контактной работы	0,25
Самостоятельная работа обучающихся:	**69,75**
изучение теоретического курса	44
подготовка к текущему контролю	22
подготовка к промежуточной аттестации	3,75
Вид промежуточной аттестации:	**зачет**
Общая трудоемкость, з.е./ часы	**3/108**

*Контактная работа обучающихся с преподавателем, в том числе с применением дистанционных образовательных технологий, включает занятия лекционного типа, и (или) занятия семинарского типа, лабораторные занятия, и (или) групповые консультации, и (или) индивидуальную работу обучающегося с преподавателем, а также аттестационные испытания промежуточной аттестации. Контактная работа может включать иные виды учебной деятельности, предусматривающие групповую и индивидуальную работу обучающихся с преподавателем. Часы контактной работы определяются Положением об организации и проведении контактной работы при реализации образовательных программ высшего образования, утвержденным Ученым советом УГЛТУ от 25 февраля 2020 года.

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов

5.1. Трудоемкость разделов дисциплины

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
1	Сетевые протоколы	2	-	2	4	10
2	Основы криптографии	2	-	4	6	14
3	Протоколы информационной опасности	2	-	6	8	14
4	Протоколы SSL и TLS	2	-	6	8	14
5	Защищенные протоколы сети Интернет	4	-	8	12	14
Итого по разделам:		**12**	**-**	**26**	**38**	**66**
Промежуточная аттестация		x	x	x	0,25	3,75
Курсовая работа (курсовой проект)		x	x	x	x	-
Всего		**108**				

5.2 Содержание занятий лекционного типа

Тема 1. Сетевые протоколы.

Протоколы: основные понятия и принцип взаимодействия. Принцип работы протоколов. Протоколы сетевого уровня: IP, IPX, RIP, NLSP Характеристика и применение протоколов сетевого уровня. Протоколы транспортного уровня UDP и TCP, их характеристика и применение. Установка протокола TCP/IP в операционных системах.

Протоколы уровня приложений. Различия и особенности распространенных протоколов. Протокол эмуляции удаленного терминала Telnet. Концепция сетевого виртуального терминала. Согласование параметров взаимодействия. Симметрия связи «терминал-процесс». Электронная почта: формат, почтовые клиенты, протоколы. Протоколы SMTP, POP3, IMAP. Их характеристика, назначение и отличие. Настройка программы почтового клиента. Протоколы распределенных файловых систем.

Тема 2. Основы криптографии.

Теоретические основы криптографии. Общие сведения по классической криптографии. Стойкость алгоритмов шифрования. Общая классификация алгоритмов шифрования. Реализация алгоритмов шифрования. Криптография и стеганография. Обзор основных алгоритмов шифрования.

Симметричные криптосистемы. Шифрование с использованием операции XOR. Стандарты блочного шифрования Алгоритм DES. Стандарты блочного шифрования Алгоритм ГОСТ.

Ассиметричные алгоритмы шифрования Стандарт ассиметричного шифрования RSA. Ключевая информация. Генерация ключей. Детерминированные методы. Недетерминированные методы. Генерация сеансовых ключей. Генерация ключей на основе пароля пользователя. Накопление (хранение) ключей. Электронная цифровая подпись. Общие сведения об электронной цифровой подписи. Алгоритмы цифровой подписи.

Тема 3. Протоколы информационной безопасности.

Протокол прикладного уровня PGP. Протокол сетевого уровня IPSec. Защищенный доступ к филиалу организации или к сети другой организации через Internet. Усиление защиты протоколов ИБ прикладного уровня. Заголовки IPSec. Протокол AH. Протокол ESP. Транспортный и туннельный режимы. Защищенные связи. Параметры защищенной связи. Виртуальная частная сеть VPN-IPSec. Протоколы маршрутизации RIP, OSPF и BGP.

Тема 4. Протоколы SSL и TLS.

История SSL. Устройство протокола SSL. Протокол записи. Принцип работы SSL. Цифровые сертификаты. Хэширование. Шифрование. Аутентификация и обмен ключами. Восстановление сессии. Администрирование. Обслуживание сертификатов и ключей.

Протокол транспортного уровня TLS. Передача данных при использовании TLS. Установление защищенной связи (Этап 1. Определение характеристики защиты. Этап 2. Аутентификация и обмен ключами сервера. Этап 3. Аутентификация и обмен ключами клиента. Этап 4. Завершение). Меры безопасности в TLS. Ключевые отличия SSL и TLS. Виды возможных атак.

Тема 5. Защищенные протоколы сети Интернет.

Защищенные протоколы ровня приложений. Протокол HTTPS. Протоколы SMTPS, POP3S, IMAPS. Их характеристика, назначение и отличие. Настройка защищенных протоколов. Протокол SSH - Secure Shell.

5.3 Темы и формы занятий семинарского типа

Учебным планом по дисциплине предусмотрены лабораторные занятия

№	Тема семинарских занятий	Форма проведения занятия	Трудоемкость, час
1.	Сетевые протоколы	лабораторная работа	2
2.	Основы криптографии	лабораторная работа	4
3.	Протоколы информационной безопасности	лабораторная работа	6
4.	Протоколы SSL и TLS	лабораторная работа	6
5.	Защищенные протоколы сети Интернет	лабораторная работа	8
Итого часов:			**26**

5.4 Самостоятельная работа обучающихся

№	Наименование раздела дисциплины (модуля)	Вид самостоятельной работы	Трудоемкость, час
1	Сетевые протоколы	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	10
2	Основы криптографии	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	14
3	Протоколы информационной безопасности	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	14
4	Протоколы SSL и TLS	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	14
5	Защищенные протоколы сети Интернет	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	14
6	Подготовка к промежуточной аттестации	Изучение рекомендованных источников информации, конспектов лекций, подготовка ответов на вопросы зачета	3,75
Итого:			**69,75**

6. Перечень учебно-методического обеспечения по дисциплине

Основная и дополнительная литература

№ п/п	Автор, наименование	Год издания	Количество экземпляров в научной библиотеке
Основная литература			
1	Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. — 120 с. — ISBN 978-5-00137-292-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/257564. — Режим доступа: для авториз. пользователей.	2022	Полнотекстовый доступ при входе по логину и паролю*
2	Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация : учебное пособие / С. С. Гельбух. — Санкт-Петербург : Лань, 2022. — 208 с. — ISBN 978-5-8114-3474-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206585. — Режим доступа: для авториз. пользователей.	2022	Полнотекстовый доступ при входе по логину и паролю*
3	Шилер, А. В. Обеспечение информационной безопасности корпоративных информационных сетей на базе программного комплекса SecureTower : учебно-методическое пособие / А. В. Шилер, А. А. Елизаров, Е. А. Степанова. — Омск : ОмГУПС, 2020. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165730. — Режим доступа: для авториз. пользователей.	2020	Полнотекстовый доступ при входе по логину и паролю*
4	Корниенко, А. А. Криптографические протоколы: учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург: ПГУПС, 2020. — 74 с. — ISBN 978-5-7641-1509-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/191009. — Режим доступа: для авториз. пользователей.	2020	Полнотекстовый доступ при входе по логину и паролю*
Дополнительная литература			
5	Игнатьев, Е. Б. Основы криптографии: учебное пособие / Е. Б. Игнатьев. — Иваново: ИГЭУ, 2020. — 88 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/154559. — Режим доступа: для авториз. пользователей	2020	Полнотекстовый доступ при входе по логину и паролю*
6	Защита компьютерной информации: учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. — Санкт-Петербург: БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 146 с. — ISBN 978-5-907054-82-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/157086. — Режим доступа: для авториз. пользователей.	2019	Полнотекстовый доступ при входе по логину и паролю*
7	Пугин, В. В. Криптографические протоколы: методические указания / В. В. Пугин, С. А. Лабада. — Самара: ПГУТИ, 2018. — 51 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/182303. — Режим доступа: для авториз. пользователей.	2018	Полнотекстовый доступ при входе по логину и паролю*

*- прежде чем пройти по ссылке, необходимо войти в систему

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий.

Электронные библиотечные системы

Каждый обучающийся обеспечен доступом к электронной библиотечной системе УГЛТУ (http://lib.usfeu.ru/), ЭБС Издательства Лань http://e.lanbook.com/, ЭБС Университетская библиотека онлайн http://biblioclub.ru/, содержащих издания по основным изучаемым дисциплинам и сформированных по согласованию с правообладателями учебной и учебно- методической литературы.

Справочные и информационные системы

1. Справочно-правовая система «Консультант Плюс». – Режим доступа: для авториз. пользователей.

2. Информационно-правовой портал Гарант. – URL: http://www.garant.ru/ – Режим доступа: свободный.

Профессиональные базы данных

1. Федеральная служба государственной статистики. Официальная статистика. – URL: http://www.gks.ru/. – Режим доступа: свободный.

2. Научная электронная библиотека elibrary. – URL: http://elibrary.ru/. – Режим доступа: свободный.

3. Национальная электронная библиотека. – URL: https://rusneb.ru/. – Режим доступа: свободный.

Нормативно-правовые акты

1. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ: принят Государственной думой 21 октября 1994 г. (ред. от 09.03.2021) // СПС КонсультантПлюс. — URL: http://www.consultant.ru/document/cons_doc_LAW_5142/. — Режим доступа: свободный. – Текст: непосредственный.

2. Профессиональный стандарт 06.015 «Специалист по информационным системам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 17 сентября 2014 г. №645н. (зарегистрировано в Минюсте России 24.12.2014 N 35361) // СПС КонсультантПлюс. — URL: http://www.consultant.ru/document/cons_doc_LAW_135658/. — Режим доступа: свободный. – Текст: непосредственный.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Формируемые компетенции	Вид и форма контроля
ПК-3 – Способен настраивать оборудование, необходимое для работы ИС	**Промежуточный контроль**: контрольные вопросы **Текущий контроль**: опрос, выполнение практических заданий, тестирование

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Критерии оценивания устного ответа на контрольные вопросы зачета (промежуточный контроль формирования компетенции ПК-3):

«Зачтено» - дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных

связей. Ответ изложен литературным языком в терминах науки, показана способность быстро реагировать на уточняющие вопросы;

«Зачтено» - дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Однако допущены незначительные ошибки или недочеты, исправленные обучающимся с помощью «наводящих» вопросов;

«Зачтено» - дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания обучающимся их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции;

«Не зачтено» – обучающийся демонстрирует незнание теоретических основ предмета, не умеет делать аргументированные выводы и приводить примеры, показывает слабое владение монологической речью, не владеет терминологией, проявляет отсутствие логичности и последовательности изложения, делает ошибки, которые не может исправить, даже при коррекции преподавателем, отказывается отвечать на занятии.

К***ритерии оценивания выполнения заданий в тестовой форме (текущий контроль формирования компетенции ПК-3):***

По итогам выполнения тестовых заданий оценка производится по четырехбалльной шкале. При правильных ответах на:

86-100% заданий – оценка «отлично»;

71-85% заданий – оценка «хорошо»;

51-70% заданий – оценка «удовлетворительно»;

менее 51% - оценка «неудовлетворительно».

Критерии оценивания практических заданий (текущий контроль формирования компетенции ПК-3):

«Зачтено» (отлично) - выполнены все задания, бакалавр четко и без ошибок ответил на все контрольные вопросы.

«Зачтено» (хорошо) - выполнены все задания, бакалавр с небольшими ошибками ответил на все контрольные вопросы.

«Зачтено» (удовлетворительно) - выполнены все задания с замечаниями, бакалавр ответил на все контрольные вопросы с замечаниями.

«Не зачтено» (неудовлетворительно) - обучающийся не выполнил или выполнил неправильно задания, ответил на контрольные вопросы с ошибками или не ответил на конкретные вопросы.

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

7.3.1. Контрольные вопросы к зачету (промежуточный контроль)

1. Протоколы: основные понятия и принцип взаимодействия.
2. Принцип работы протоколов.
3. Протоколы сетевого уровня: IP, IPX, RIP, NLSP Характеристика и применение протоколов сетевого уровня.
4. Протоколы транспортного уровня UDP и TCP, их характеристика и применение.
5. Протоколы уровня приложений.
6. Протокол эмуляции удаленного терминала Telnet.

7. Концепция сетевого виртуального терминала.
8. Согласование параметров взаимодействия.
9. Симметрия связи «терминал-процесс».
10. Электронная почта: формат, почтовые клиенты, протоколы.
11. Протоколы SMTP, POP3, IMAP. Их характеристика, назначение и отличие.
12. Настройка программы почтового клиента.
13. Протоколы распределенных файловых систем.
14. Теоретические основы криптографии.
15. Общие сведения по классической криптографии.
16. Стойкость алгоритмов шифрования.
17. Общая классификация алгоритмов шифрования.
18. Криптография и стеганография.
19. Обзор основных алгоритмов шифрования.
20. Симметричные криптосистемы.
21. Ассиметричные алгоритмы шифрования Стандарт ассиметричного шифрования RSA.
22. Электронная цифровая подпись.
23. Протокол прикладного уровня PGP.
24. Протокол сетевого уровня IPSec.
25. Защищенный доступ к филиалу организации или к сети другой организации через Internet.
26. Заголовки IPSec.
27. Протокол AH.
28. Протокол ESP.
29. Виртуальная частная сеть VPN-IPSec.
30. Протоколы маршрутизации RIP, OSPF и BGP.
31. История SSL. Принцип работы SSL.
32. Цифровые сертификаты.
33. Хэширование.
34. Аутентификация и обмен ключами.
35. Протокол транспортного уровня TLS.
36. Передача данных при использовании TLS.
37. Меры безопасности в TLS.
38. Ключевые отличия SSL и TLS.
39. Защищенные протоколы уровня приложений.
40. Протокол HTTPS.
41. Протоколы SMTPS, POP3S, IMAPS. Их характеристика, назначение и отличие.
42. Протокол SSH - Secure Shell.

7.3.2. Задания в тестовой форме (текущий контроль)

1. Транспортный протокол (TCP) обеспечивает:
1) разбиение файлов на IP-пакеты в процессе передачи и сборку файлов в процессе получения;
2) прием, передачу и выдачу одного сеанса связи;
3) предоставление в распоряжение пользователя уже переработанную информацию;
4) доставку информации от компьютера-отправителя к компьютеру-получателю.

2. Служба FTP в Интернете предназначена:
1) для создания, приема и передачи web-страниц;
2) для обеспечения функционирования электронной почты;
3) для обеспечения работы телеконференций;
4) для приема и передачи файлов любого формата;

3. Преобразование открытого текста сообщения в закрытый называется:
1) процедура шифрования;
2) алгоритм шифрования;
3) обеспечение аутентификации;
4) цифровая запись.

4. Для чего используется TLS:
1) протокол защиты транспортного уровня, криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет;
2) широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.;
3) протокол защиты сеансового уровня, криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет;
4) расширение протокола HTTP для поддержки шифрования в целях повышения безопасности.

5. Как иначе называется симметричное шифрование:
1) шифрование с закрытым ключом;
2) шифрование методом Бейтса;
3) шифрование с открытым ключом;
4) шифрование с переменным ключом.

7.3.3. Практические задания (текущий контроль)

1. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Применение фильтрующего маршрутизатора
2. Защита сетевого трафика с использованием протокола IPSec в Windows NT 5.0. Организация VPN средствами протокола PPTP.
3. Применение специализированных средств организации VPN на примере «VipNet» и «StrongNET».
4. Применение СОА Snort для обнаружения скрытого сканирования, атак, использующих преднамеренное нарушение структуры сетевых пакетов, атак вида «отказ в обслуживании».
5. Применение технологии терминального доступа.
6. Применение программных средств аудита информационной безопасности с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз.

7.4. Соответствие шкалы оценок и уровней сформированных компетенций

Уровень сформированных компетенций	Количество баллов (оценка)	Пояснения
Высокий	«зачтено»	Теоретическое содержание курса освоено полностью, компетенции сформированы, все предусмотренные программой обучения учебные задания выполнены. Обучающийся самостоятельно и на высоком уровне настраивает и обслуживает сетевые элементы и периферийное оборудование инфокоммуникационной системы
Хороший	«зачтено»	Теоретическое содержание курса освоено полностью, компетенции сформированы, все предусмотренные программой обучения учебные задания выполнены с незначительными замечаниями. Обучающийся с незначительными наставлениями настраивает и обслуживает сетевые элементы и периферийное оборудование инфокоммуникационной системы

Средний	«зачтено»	содержание курса освоено частично, компетенции сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, в них имеются ошибки. Обучающийся под руководством настраивает и обслуживает сетевые элементы и периферийное оборудование инфокоммуникационной системы
Низкий	«не зачтено»	Содержание курса не освоено, компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий Обучающийся не способен настраивать и обслуживать сетевые элементы и периферийное оборудование инфокоммуникационной системы

8. Методические указания для самостоятельной работы обучающихся

Самостоятельная работа – планируемая учебная, производственная, технологическая работа обучающихся, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль в контроле за работой студентов и магистрантов).

Самостоятельная работа обучающихся в вузе является важным видом их учебной и производственной деятельности. Самостоятельная работа играет значительную роль в рейтинговой технологии обучения. В связи с этим, обучение в вузе включает в себя две, практически одинаковые по взаимовлиянию части – процесса обучения и процесса самообучения. Поэтому самостоятельная работа должна стать эффективной и целенаправленной работой обучающихся.

Формы самостоятельной работы обучающихся разнообразны. Они включают в себя:

- написание докладов или подготовку рефератов по выполняемому заданию;
- участие в работе конференций, комплексных научных исследованиях;

В процессе изучения дисциплины «Защищенные сетевые протоколы» обучающимся направления 09.03.03 *основными видами самостоятельной работы* являются:

- подготовка к аудиторным занятиям (лекциям и практическим занятиям) и выполнение соответствующих заданий;
- самостоятельная работа над отдельными темами учебной дисциплины в соответствии с учебно-тематическим планом;
- выполнение тестовых заданий;
- подготовка к зачету.

Самостоятельное выполнение *тестовых заданий* по всем разделам дисциплины сформированы в фонде оценочных средств (ФОС)

Данные тесты могут использоваться:

- обучающимися при подготовке к зачету с оценкой в форме самопроверки знаний;
- преподавателями для проверки знаний в качестве формы промежуточного контроля на практических занятиях;
- для проверки остаточных знаний обучающихся, изучивших данный курс.

Тестовые задания рассчитаны на самостоятельную работу без использования вспомогательных материалов. То есть при их выполнении не следует пользоваться учебной и другими видами литературы.

Для выполнения тестового задания, прежде всего, следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступать к прочтению

предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать индекс (цифровое обозначение), соответствующий правильному ответу.

На выполнение теста отводится ограниченное время. Оно может варьироваться в зависимости от уровня тестируемых, сложности и объема теста. Как правило, время выполнения тестового задания определяется из расчета 45-60 секунд на один вопрос.

Содержание тестов по дисциплине ориентировано на подготовку обучающихся по основным вопросам курса. Уровень выполнения теста позволяет преподавателям судить о ходе самостоятельной работы обучающихся в межсессионный период и о степени их подготовки к зачету с оценкой.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Применение цифровых технологий в рамках преподавания дисциплины предоставляет расширенные возможности по организации учебных занятий в условиях цифровизации образования и позволяет сформировать у обучающихся навыки применения цифровых сервисов и инструментов в повседневной жизни и профессиональной деятельности.

Для реализации этой цели в рамках изучения дисциплины могут применяться следующие цифровые инструменты и сервисы:

– для коммуникации с обучающимися:.VK Мессенджер (https://vk.me/app?mt_click_id=mt-v7eix5-1660908314-1651141140) – мессенджер, распространяется по лицензии FreeWare; сервис WEEEK (https://weeek.net/ru) – сервис для коммуникации, распространяется по лицензии trialware;

– для планирования аудиторных и внеаудиторных мероприятий: ВКС Pruffme – система для организации коллективной работы и онлайн-встреч, распространяется по проприетарной лицензии; ВКС Mirapolis – система для организации коллективной работы и онлайн-встреч, распространяется по проприетарной лицензии;

– для совместного использования файлов: Яндекс.Документы (https://docs.yandex.ru/) – инструмент для создания и совместного использования документов, распространяется по лицензии trialware; Яндекс.Диск – сервис для хранения и совместного использования документов, распространяется по лицензии trialware.

Для успешного овладения дисциплиной используются следующие информационные технологии обучения:

– при проведении лекций используются презентации учебного материала, подготовленные в редакторе презентаций, демонстрация работы изучаемых программных продуктов (см. список ниже), выход на профессиональные сайты, использование видеоматериалов различных интернет-ресурсов;

– лабораторные работы по дисциплине проводятся с использованием платформы LMS MOODLE, используются изучаемые программные продукты (см. список ниже).

Для дистанционной поддержки дисциплины используется система управления образовательным контентом Moodle. Для работы в данной системе все обучающиеся на первом курсе получают индивидуальные логин и пароль для входа в систему, в которой размещаются: программа дисциплины, материалы для лекционных и иных видов занятий, задания, контрольные вопросы, дополнительные материалы для изучения дисциплины.

Университет обеспечен необходимым комплектом лицензионного либо свободно распространяемого программного обеспечения:

– операционная система Windows 7, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок действия - бессрочно;

– пакет прикладных программ Office Professional Plus 2010, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок действия – бессрочно;

– операционная система Astra Linux Special Edition. Договор №Pr000013979/0385/22-ЕП-223-06 от 01.07.2022. Срок действия: бессрочно;

– пакет прикладных программ Р7-Офис. Профессиональный. Договор №Pr000013979/0385/22-ЕП-223-06 от 01.07.2022. Срок: бессрочно;

– антивирусная программа Kaspersky Endpoint Security для бизнеса- Стандартный Russian Edition. 250-499 Node 1 year Educational Renewal License. Договор заключается университетом ежегодно;

– система видеоконференсвязи Mirapolis. Договор заключается университетом ежегодно;

– система видеоконференсвязи Pruffme. Договор заключается университетом ежегодно;

– система управления обучением LMS Moodle – программное обеспечение с открытым кодом, распространяется по лицензии GNU Public License (rus);

– браузер Яндекс (https://yandex.ru/) – программное обеспечение на условиях простой (неисключительной) лицензии;

– операционная система Windows Server. Контракт на услуги по предоставлению лицензий на право использовать компьютерное обеспечение № 067/ЭА от 07.12.2020 года. Срок бессрочно;

– операционная система Linux (https://ubuntu.com/) — семейство Unix-подобных операционных систем на базе ядра Linux, свободное программное обеспечение с открытым кодом, распространяется по лицензии GNU Public License (rus);

– гипервизор VMware ESXi(https://my.vmware.com/en/web/vmware/evalcenter?p=free-esxi7) с открытым программным кодом Open Source, распространяется по лицензии GNU Public License;

– Wireshark (https://www.wireshark.org/) — программа-анализатор трафика для компьютерных сетей Ethernet, программа распространяется под свободной лицензией GNU GPL;

– программа для эмуляции работы сети NetEmul (http://netemul.sourceforge.net/ruindex.html) – свободно распространяемое программное обеспечение, распространяется по лицензии GPL;

– электронно-библиотечная система «Лань». Договор №024/23-ЕП–44-03 от 24.03.2023 г. Срок действия: 09.04.2023-09.04.2024; Договор №025/23-ЕП–44-03 от 24.03.2023 г. Срок действия: 09.04.2023-09.04.2024;

– электронно-библиотечная система «Университетская библиотека онлайн». Договор №8505/20220046/22-ЕП-44-06 от 27.05.2022 г. Срок действия: 27.06.2022-26.06.2023;

– электронно-библиотечная система «Образовательная платформа Юрайт». Договор №015/23-ЕП-44-06 от 16.02.2023 г. Срок действия: 16.02.2023-16.02.2024;

– электронные версии периодических изданий. Договор №284-П/0091/22-ЕП-44-06 от 22.12.2022 г. Срок действия: 01.01.2023-31.12.2023;

– программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат. ВУЗ» (URL: https://www.antiplagiat.ru/). Договор № 6414/0107/23-ЕП-223-03 от 27.02.2023 года. Срок с 03.03.2023 г по 03.03.2024 г.;

– справочная правовая система «КонсультантПлюс» (URL: http://www.consultant.ru/). Договор оказания услуг по адаптации и сопровождению экземпляров СПС КонсультантПлюс №0607/ЗК от 25.01.2023. Срок с 01.02.2023 г по 31.01.2024 г.

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Реализация учебного процесса осуществляется в специальных учебных аудиториях университета. Аудитории для проведения занятий лекционного типа укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Помещения для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и

промежуточной аттестации оснащены персональными компьютерами и имеют выход в сеть Интернет. При необходимости обучающимся предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации. Самостоятельная работа обучающихся выполняется в специализированной аудитории, которая оборудована учебной мебелью, компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УГЛТУ. Есть помещение для хранения и профилактического обслуживания учебного оборудования.

Требования к оснащенности аудиторий

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Помещение для лекционных занятий	Переносная мультимедийная установка (проектор, экран). Ноутбук или компьютер. Учебная мебель
Помещение для занятий семинарского типа (лабораторных работ), групповых и индивидуальных консультаций, текущей и промежуточной аттестации	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, электронную информационно-образовательную среду.
Помещения для самостоятельной работы	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, электронную информационно-образовательную среду.
Помещение для хранения и профилактического обслуживания учебного оборудования.	Стеллажи. Раздаточный материал