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.02.02 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ СЕТЯХ

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 «Информационная безопасность в компьютерных сетях» 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 «Информационная безопасность в компьютерных сетях» 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 в области построения защищенных компьютерных сетей с использованием современных программно-аппаратных средств.

Задачи дисциплины:

– формирование знаний о методах и средствах защиты информации в компьютерных сетях, о технологии межсетевого экранирования, построения защищенных виртуальных частных сетей;

– формирование умений по обеспечению безопасности при организации корпоративных сетей и защищенных подключений;

– формирование навыков аудита уровня защищенности информационных систем.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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

В результате изучения дисциплины студент должен:

знать:

– технологии и средства безопасности при передаче данных в компьютерных сетях;

– основные требования информационной безопасности в компьютерных сетях;

– технологии обнаружения компьютерных атак и их возможности;

– основные уязвимости и типовые атаки на современные компьютерные системы;

– возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;

– классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;

– основные принципы администрирования защищенных компьютерных систем;

уметь:

– проектировать топологию сети, обеспечивающих безопасную передачу данных;

– настраивать технологии и средства сетевой фильтрации и безопасности данных;

– обнаруживать и устранять инциденты информационной безопасности при передаче данных;

– выполнять функции администратора безопасности защищенных компьютерных систем;

– выполнять настройку защитных механизмов сетевых программно-аппаратных средств;

– настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;

– применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей;

– организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;

владеть:

– методами построениями защищенной сети передачи данных;

– средствами администрирования сетевых программно-аппаратных комплексов защиты информации;

– средствами администрирования систем обнаружения компьютерных атак;

– средствами и системами аудита информационной безопасности;

– методикой проведения аудита информационной безопасности;

– средствами администрирования систем организации виртуальных частных сетей.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность в компьютерных сетях» 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	Сетевое администрирование Проектирование информационно-коммуникационных систем	Информационная безопасность

Архитектура вычислительных машин и систем	Производственная практика (технологическая (проектно-технологическая практика))	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	Основы обеспечения безопасности в компьютерных сетях	2	-	2	4	10
2	Обнаружение компьютерных атак	2	-	4	6	14
3	Мониторинг компьютерных сетей	2	-	6	8	14
4	Виртуальные частные сети и PROXY-сервера	2	-	6	8	14
5	Технологии защищенной обработки информации	2	-	4	6	6
6	Аудит информационной безопасности в компьютерных сетях	2	-	4	6	8
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. **Основы обеспечения безопасности в компьютерных сетях.**

Основные понятия, концепции и принципы информационной безопасности в компьютерных сетях, уязвимость, угроза, атака, ущерб и риск, управление рисками.

Веб-серверы. Основные угрозы безопасности веб-ресурсов. Межсетевые экраны уровня веб-приложений.

Технологии централизованного файлообмена. Технологии децентрализованного файлообмена.

Программные криптографические механизмы защиты информации в сетях. Локальный подход к обеспечению криптографической защиты информации. Методы и средства обеспечения информационной безопасности удаленного взаимодействия.

Системы обнаружения вторжения и предотвращения вторжений. Архитектура и функции IDS/IPS. Виды IDS/IPS-систем. Подходы к анализу событий безопасности.

Угрозы и уязвимости беспроводных сетей.

Подходы к анализу событий безопасности.

Тема 2. **Обнаружение компьютерных атак**

Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.

Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования.

Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.

Тема 3. **Мониторинг компьютерных сетей.**

Фильтрация, виды фильтрации, стандартные и дополнительные правила фильтрации маршрутизаторов Cisco, файерволы, функциональное назначение файервола, типы файерволов.

Мониторинг трафика. Анализаторы протоколов, анализаторы протоколов, система мониторинга, системы обнаружения вторжений, архитектура сети с защитой периметра и разделением внутренних зон, аудит событий безопасности.

Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования.

Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Службы мониторинга сетевого трафика.

Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации.

Тема 4. **Виртуальные частные сети и PROXY-сервера.**

Прокси-серверы, функции прокси-сервера, Механизмы проксирования. «Проксификация» приложений, файерволы с функцией NAT, традиционная технология NAT, базовая трансляция сетевых адресов, трансляция сетевых адресов и портов, программные файерволы хоста, типовые архитектуры сетей, защищаемых файерволами.

Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.

Защита данных на сетевом уровне. Иерархия технологий защищенного канала, распределение функций между протоколами IPSec, безопасная ассоциация, транспортный и туннельный режимы, протокол прикладного уровня PGP, протокол AH, протокол ESP, базы данных SAD И SPD, VPN на основе шифрования. Транспортный и туннельный режимы. Защищенные связи. Параметры защищенной связи. Протоколы маршрутизации RIP, OSPF и BGP.

Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec.

Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения.

Защита на транспортном уровне. 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. Меры безопасности в TLS. Ключевые отличия SSL и TLS. Виды возможных атак. Организация VPN средствами протокола SSL в операционных системах. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения.

Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.

Тема 5. **Технологии защищенной обработки информации**

Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера. Настройка сервера MSTS. Настройка протокола RDP.

Основы администрирования централизованной работы пользователей. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.

Тема 6. **Аудит информационной безопасности в компьютерных сетях**

Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ.

Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности.

Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации.

Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети.

Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений.

Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратно-программных средств объекта информатизации.

Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков

5.3 Темы и формы занятий семинарского типа

Учебным планом по дисциплине предусмотрены лабораторные занятия

№	Тема семинарских занятий	Форма проведения занятия	Трудоемкость, час
1.	Основы обеспечения безопасности в компьютерных сетях	лабораторная работа	2
2.	Обнаружение компьютерных атак	лабораторная работа	4
3.	Мониторинг компьютерных сетей	лабораторная работа	6
4.	Виртуальные частные сети и PROXY-сервера	лабораторная работа	6
5.	Технологии защищенной обработки информации	лабораторная работа	4
6	Аудит информационной безопасности в компьютерных сетях	лабораторная работа	4
Итого часов:			**26**

5.4 Самостоятельная работа обучающихся

№	Наименование раздела дисциплины (модуля)	Вид самостоятельной работы	Трудоемкость, час
1	Основы обеспечения безопасности в компьютерных сетях	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	10
2	Обнаружение компьютерных атак	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	14
3	Мониторинг компьютерных сетей	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	14
4	Виртуальные частные сети и PROXY-сервера	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	14
5	Технологии защищенной обработки информации	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	6
6	Аудит информационной безопасности в компьютерных сетях	Изучение лекционного материала в соответствии с тематикой. Тест, выполнение практических заданий	8
7	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	Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 284 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/110336. — Режим доступа: для авториз. пользователей.	2015	Полнотекстовый доступ при входе по логину и паролю*
3	Панфилов, И. В. Проблемы защиты информации в компьютерных сетях и системах: учебное пособие / И. В. Панфилов, А. М. Заяц, Е. И. Панфилова. — Санкт-Петербург: СПбГЛТУ, 2008. — 148 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/45554. — Режим доступа: для авториз. пользователей.	2008	Полнотекстовый доступ при входе по логину и паролю*
Дополнительная литература			
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*
5	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*
6	Басыня, Е. А. Системное администрирование и информационная безопасность: учебное пособие: [16+] / Е. А. Басыня. – Новосибирск: Новосибирский государственный технический университет, 2018. – 79 с.: ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575325. – Библиогр. в кн. – ISBN 978-5-7782-3484-0. – Текст: электронный.	2018	Полнотекстовый доступ при входе по логину и паролю*
7	Голиков, А. М. Защита информации от утечки по техническим каналам: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 256 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328. — Режим доступа: для авториз. пользователей.	2015	Полнотекстовый доступ при входе по логину и паролю*
8	Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М. А. Иванов, И. В. Чугунков. — Москва: НИЯУ МИФИ, 2012. — 400 с. — ISBN 978-5-7262-1676-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/75810. — Режим доступа: для авториз. пользователей.	2012	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.

Прочие интернет-ресурсы

1. Лапонина, О. Межсетевое экранирование // Национальный Открытый Университет «Интуит». – URL: https://intuit.ru/studies/courses/20/20/info. — Режим доступа: свободный.
2. Лапонина, О. Протоколы безопасного сетевого взаимодействия // Национальный Открытый Университет «Интуит». – URL: https://intuit.ru/studies/courses/59/59/info. — Режим доступа: свободный.
3. Мэйволд, Э. Безопасность сетей // Национальный Открытый Университет «Интуит». – URL: https://intuit.ru/studies/courses/102/102/info. — Режим доступа: свободный.
4. Новиков, Ю. Основы организации локальных сетей // Национальный Открытый Университет «Интуит». – URL: https://intuit.ru/studies/courses/489/345/info. — Режим доступа: свободный.
5. Семенов, Ю. Процедуры, диагностики и безопасность в Интернет // Национальный Открытый Университет «Интуит». – URL: https://intuit.ru/studies/courses/1124/201/info. — Режим доступа: свободный.

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 и практические задания к зачету **Текущий контроль**: выполнение практических заданий, тестирование

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

Критерии оценивания ответа на 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. Практическое задание выполнено верно, без ошибок выбраны методы и средства для решения поставленной задачи, допускаются небольшие неточности.

«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. Практическое задание выполнено верно, правильно подобраны методы и средства для решения поставленной задачи, допущены незначительные ошибки и неточности, не оказывающие существенного влияния на прогнозируемый результат выполнения задания.

«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. Практическое задание выполнено верно, в целом правильно подобраны методы и средства для решения поставленной задачи, допускается небольшая помощь со стороны преподавателя по подбору методов и средств, допущенные ошибки оказывают влияние на прогнозируемый результат выполнения задания.

«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. Практическое задание выполнено неверно либо не выполнено, методы и средства для решения поставленной задачи подобраны неверно, допущено много ошибок, которые оказывают значимое влияние на прогнозируемый результат выполнения задания.

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)

Теоретические вопросы

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.
2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
4. Создание защищенных сегментов сетей с использованием межсетевых экранов.
5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в операционной системе.
6. Защита рабочих станций с использованием персональных сетевых фильтров.
7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
8. История SSL. Принцип работы SSL.
9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.
10. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.
11. Преимущества технологии терминального доступа. Обеспечение безопасности.
12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.
13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.
14. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
15. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.
16. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем.
17. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности. Методика проведения инструментальных проверок.

18. Протокол прикладного уровня PGP.
19. Назначение и основные функции программных комплексов «Гриф-специалист» и «Кондор-специалист». Построение модели защиты компьютерной системы с использованием комплексной экспертной системы «АванГард».
20.Виды требований безопасности согласно ГОСТ Р ИСО/МЭК 15408-1-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
21. Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort».
21. Протокол сетевого уровня IPSec.
22. Заголовки IPSec.
23. Протокол AH.
24. Протокол ESP.
25. Протоколы маршрутизации RIP, OSPF и BGP.
26. Протокол транспортного уровня TLS.
27. Передача данных при использовании TLS.
28. Меры безопасности в TLS.
29. Ключевые отличия SSL и TLS.
30. Защищенные протоколы уровня приложений.
31. Протокол HTTPS.
32. Протоколы SMTPS, POP3S, IMAPS. Их характеристика, назначение и отличие.
33. Протокол SSH - Secure Shell.

Практические вопросы
1. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами сетевых фильтров.
2. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами сетевых фильтров.
3. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров.
4. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение извне доступа к ресурсам компьютера за исключением двух доверенных узлов. Реализуйте политику средствами сетевых фильтров.
5. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение доступа к Web-ресурсам определенного узла. Реализуйте политику средствами сетевых фильтров.
6. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров.
7. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами сетевых фильтров.
8. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами протокола IPSec.
9. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами протокола IPSec.
10. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec.
11.С использованием программы «Брандмауэр Windows» (Windows Firewall) выполнить настройки, запрещающие использование всех портов защищаемого узла за исключением TCP-порта 3389.

12. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами протокола IPSec.
13.Сгенерируйте и получите в виде файла сертификат открытого ключа с использованием образа ОС Windows Server 2003.
14. Настройте Web-сервер для организации защищенного доступа к Web-странице сиспользованием протокола SSL. Выполнить с использованием образа ОС Windows Server 2003. Файл-сертификат открытого ключа прилагается.
15. Настройте входящее подключение VPN с использованием протокола PPTP. Настроить и установить подключение клиентского узла. Выполнить с использованием образа ОС Windows Server 2003.
16. Осуществите криптографическую защиту сетевого трафика средствами протокола IPSec в ОС Windows XP. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.
17. Осуществите криптографическую защиту сетевого трафика средствами СКЗИ StrongNet. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.
18. Организовать защищенный обмен почтовой информацией между двумя пользователями. Шифрование почтовых сообщений выполнить с помощью алгоритма ГОСТ 28147-89, реализуемого средствами СКЗИ КриптоПро CSP. Выполнить с использованием образов ОС Windows Server 2003 и Windows 2000.
19. Разработайте файл конфигурации и настройте СОА Snort на обнаружение тестирования внутренней структуры сети ICMP-запросами.
20. Разработайте файл конфигурации и настройте СОА Snort на обнаружение ICMP пакетов большой длины.
21. Разработайте файл конфигурации и настройте СОА Snort на обнаружение устанавливаемых из внешней сети TCP-соединений.
22. Установить службу терминального доступа. Выполнить настройки службы MSTS, разрешающие доступ к ресурсам терминального сервера только для учетных записей, зарегистрированных в созданной по умолчанию группе «Remote Desktop Users».
23. Установить службу терминального доступа. Выполнить настройки протокола RDP, запрещающие использование ресурсов рабочей станции, включая буфер обмена, принтеры и накопители.
24.Выявите сетевые узлы в локальном сетевом сегменте с использованием: утилиты fping; утилиты ping и широковещательной ICMP-посылки; утилиты icmpush (тип ICMPпакетов13 и 17); утилиты ping и многоадресной рассылки; утилиты arping; утилиты hping3 и методов TCP- и UDP-разведки; утилиты Ethereal и метода прослушивания сети.
25.С помощью утилиты nmap проведите сканирование портов сетевого узла. Сформируйте списки открытых TCP- и UDP-портов, идентифицируйте версии ОС и запущенных сервисов. По результатам сделайте вывод о возможности обнаружения открытых портов и идентификации типа и версии ОС, а также сетевых сервисов.
26.С помощью программы NetCrunch, постройте карту сети компьютерного класса.

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 операцинной системе сервера. Организация VPN средствами протокола PPTP.
3. Применение специализированных средств организации VPN на примере «VipNet» и «StrongNET».
4. Применение COA 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;
- выполнение практических 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;

– СКЗИ «КриптоПро CSP», договор №z062790537/22/0121/22-ЕП-223-06 от 11.03.2022. Срок действия: до 11.03.2022;

– 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