Подписан цифровой подписью: Платонов Евгений Петрович
Основание: Я подтверждаю этот документ своей удостоверяющей подписью
Дата: 2025.11.19 11:45:53+05'00'

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.15 – ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Направление подготовки – 09.03.02 Информационные системы и технологии
Направленность (профиль) – Информационные системы в управлении организацией
Квалификация – бакалавр
Количество зачётных единиц (часов) – 3 (108)

г. Екатеринбург, 2025

Разработчики: к.п.н., доцент  /Л.Е. Егорова /;

Рабочая программа утверждена на заседании кафедры интеллектуальных систем (протокол № 9 от «05» марта 2025 года).

Зав. кафедрой  / Е.В.Анянова /

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией социально-экономического института
(протокол № 2 от «06» марта 2025 года).

Председатель методической комиссии СЭИ  / А.В. Чевардин /

Рабочая программа утверждена директором социально-экономического института

Директор СЭИ  /Ю.А. Капустина/

«____» _____ 20____ года.

Оглавление

1. Общие положения

Дисциплина «Технологии защиты информации в информационных системах» относится к дисциплинам части, формируемой участниками образовательных отношений, блока Б1 «Дисциплины (модули)» учебного плана, входящего в состав образовательной программы высшего образования 09.03.02 Информационные системы и технологии (профиль «Информационные системы в управлении организацией»).

Нормативно-методической базой для разработки рабочей программы учебной дисциплины «Технологии защиты информации в информационных системах» являются:

- Федеральный закон «Об образовании в Российской Федерации», утвержденный приказом Минобрнауки РФ № 273-ФЗ от 29.12.2012;
- Приказ Минобрнауки России № 245 от 06.04.2021 г. 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 от 13.07.2023 г. №586н «Об утверждении профессионального стандарта «Специалист по информационным системам»;
- Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 09.03.02 «Информационные системы и технологии» (уровень бакалавриата), утвержденный приказом Министерства образования и науки РФ № 926 от 19.09.2017;
- Учебный план образовательной программы высшего образования направления 09.03.02 «Информационные системы и технологии (профиль «Информационные системы в управлении организацией») подготовки бакалавров по очной форме обучения, одобренный Ученым советом УГЛТУ (протокол №3 от 20.03.2025).

Обучение по образовательной программе 09.03.02 «Информационные системы и технологии» (профиль «Информационные системы в управлении организацией») 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 дисциплины

Цель дисциплины – формирование у студентов профессиональных знаний и умений, связанных с использованием методов защиты информации и информационной безопасности при настройке информационных систем под задачи автоматизации бизнес-процессов.

Задачи дисциплины:

– формирование знаний теории и методологии защиты информации, правовой базы и законодательства Российской Федерации в области информационной безопасности, основ инженерно-технической защиты информации и криптографических методов;

– формирование умений по организационному обеспечению информационной безопасности и оценке качества процессов и услуг;

– формирование навыков использования нормативно-правовых документов, международных и отечественных стандартов в области информационной безопасности, решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-4 – Способен развертывать информационные системы у заказчика в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению информационных систем.

В результате изучения дисциплины обучающийся должен:

знать:

– теорию информационной безопасности, методологию защиты информации;

– правовое обеспечение информационной безопасности, законодательную базу, систему государственного контроля и управления в области информационной безопасности;

– организационное обеспечение информационной безопасности;

– основные программные средства защиты информации;

– криптографические методы и средства обеспечения информационной безопасности;

уметь:

– оценивать состояние организационной защиты информации на объекте;

– определять рациональные меры по обеспечению организационной защите на объекте;

– организовать работу с персоналом с секретной (конфиденциальной) информацией;

владеть:

– методами выявления угроз информационной безопасности объекта;

– способами обеспечения режима и секретности на объекте.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Технологии защиты информации в информационных системах» относится к дисциплинам части, формируемой участниками образовательных отношений, блока Б1 «Дисциплины (модули)» учебного плана, что означает формирование в процессе обучения у бакалавра профессиональных 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	Сопутствующие	Обеспечиваемые
Сетевые и интернет-технологии Администрирование информационных 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
	очная форма
Контактная работа с преподавателем*:	**30,25**
лекции (Л)	12
практические занятия (ПЗ)	-
лабораторные работы (ЛР)	18
промежуточная аттестация (ПА)	0,25
Самостоятельная работа обучающихся:	**77,75**
изучение теоретического курса	50

подготовка к текущему контролю	22
подготовка к промежуточной аттестации	5,75
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	Самостоя-тельная работа
1	Введение в информационную безопасность	2	-	2	4	10
2	Угрозы информационной безопасности на предприятии	2	-	2	4	13
3	Основные программные средства защиты информации	4	-	8	12	20
4	Организационное обеспечение информационной безопасности	2	-	3	5	11
5	Правовые аспекты информационной безопасности	2	-	3	5	18
Итого по разделам:		**12**	**х**	**18**	**30**	**72**
Промежуточная аттестация		х	х	х	0,25	5,75
Всего		**108**				

5.2 *Содержание занятий лекционного типа*

1. Введение в информационную безопасность

Актуальность информационной безопасности. Основные цели и задачи системы защиты. Источники угроз и атак. Основные классификации атак. Системы критериев оценки защищенности среды.

2. Угрозы информационной безопасности на предприятии

Виды угроз информационной безопасности и их характеристика. Модели нарушителей информационной безопасности на предприятии. Формы преступного посягательства. Оценка ущерба вследствие организационных нарушений информационной безопасности на предприятии.

3. Основные программные средства защиты информации

Программные средства защиты информации. Задачи обеспечения конфиденциальности, целостности и задачи обеспечения наблюдаемости, решаемые программными средствами защиты информации. Изучение основных технологий в области аутентификации данных, криптографии и обеспечении целостности данных. Управление доступом к ресурсам автоматизированной системы.

Технические мероприятия, призванные обеспечить физическую и информационную безопасность. Технические средства для реализации мероприятий данной группы.

Обеспечение безопасности электронного документооборота. Электронная подпись. Методы и средства защиты информации при работе с удаленными базами данных. Стеганография. Компьютерные вирусы и программы типа «Троянский конь». Средства обнаружения и уничтожения компьютерных вирусов.

4. Организационное обеспечение информационной безопасности

Корпоративная политика норм и требований, предъявляемых к сотрудникам на

предприятии в отношении защиты корпоративной информации. Подходы к реализации мероприятий по обеспечению информационной безопасности. Построение модели защищенной системы. Обеспечение целостности и конфиденциальности. Триада CIA. Примеры реализации политик безопасности информации на различных предприятиях.

5. Правовые аспекты информационной безопасности

Требования к защите информации, изложенные в соответствующих Законах РФ, стандартах и нормативных документах. Сравнение с нормативными документами о защите информации и мер наказания нарушителей законов о защите информации в развитых странах.

5.3 Темы и формы практических занятий

Учебным планом по дисциплине предусмотрены лабораторные работы

№	Наименование раздела дисциплины (модуля)	Форма проведения занятия	Трудоёмкость, час
1	Введение в информационную безопасность	лабораторная работа	2
2	Угрозы информационной безопасности на предприятии	лабораторная работа	2
3	Основные программные средства защиты информации	лабораторная работа	8
4	Организационное обеспечение информационной безопасности	лабораторная работа	3
5	Правовые аспекты информационной безопасности	лабораторная работа	3
Итого:			**18**

5.4 Самостоятельная работа обучающихся

№	Наименование раздела дисциплины (модуля)	Вид самостоятельной работы	Трудоемкость, час
1	Введение в информационную безопасность	выполнение практических заданий, подготовка к тестовым заданиям	10
2	Угрозы информационной безопасности на предприятии	выполнение практических заданий, подготовка к тестовым заданиям	13
3	Основные программные средства защиты информации	выполнение практических заданий, подготовка к тестовым заданиям	20
4	Организационное обеспечение информационной безопасности	выполнение практических заданий, подготовка к тестовым заданиям	11
5	Правовые аспекты информационной безопасности	выполнение практических заданий, подготовка к тестовым заданиям	18
6	Подготовка к промежуточной аттестации	изучение лекционного материала и дополнительной литературы в соответствии с тематикой	5,75
Итого:			**77,75**

6. Перечень учебно-методического обеспечения по дисциплине

Основная и дополнительная литература

№ п/п	Автор, наименование	Год издания	Примечание
Основная учебная литература			
1	Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 6-е изд., стер. — Санкт-Петербург : Лань, 2025. — 124 с. — ISBN 978-5-507-52899-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/462293. — Режим доступа: для авториз. пользователей.	2025	Полнотекстовый доступ при входе по логину и паролю*
2	Басаргин, А. А. Информационная безопасность и защита информации : практикум : учебное пособие / А. А. Басаргин. — Новосибирск : СГУГиТ, 2024. — 80 с. — ISBN 978-5-907711-75-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/484910. — Режим доступа: для авториз. пользователей.	2024	Полнотекстовый доступ при входе по логину и паролю*

Дополнительная учебная литература			
3	Информационная безопасность и защита информации: учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна: Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/154490. — Режим доступа: для авториз. пользователей.	2020	Полнотекстовый доступ при входе по логину и паролю*
4	Моргунов, А. В. Информационная безопасность: учебно-методическое пособие / А. В. Моргунов. — Новосибирск: НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227.— Режим доступа: для авториз. пользователей.	2019	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.
3. База данных Scopus компании ElsevierB.V. – URL: https://www.scopus.com/. – Режим доступа: для авториз. пользователей.

Профессиональные базы данных

1. Научная электронная библиотека elibrary. – URL: http://elibrary.ru/. – Режим доступа: свободный.
2. Национальная электронная библиотека. – URL: https://rusneb.ru/. – Режим доступа свободный.
3. Электронный фонд правовых и нормативно-технических документов // Акционерное общество «Информационная компания «Кодекс». – URL: https://docs.cntd.ru/. — Режим доступа: свободный.

Нормативно-правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Электронный фонд правовых и нормативно-технических документов. Акционерное общество «Информационная компания «Кодекс». – URL: https://docs.cntd.ru/document/9004937. – Режим доступа: свободный.
2. Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Электронный фонд правовых и нормативно-технических документов. Акционерное общество «Информационная компания «Кодекс». – URL: https://docs.cntd.ru/document/420384668. – Режим доступа: свободный.
3. Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации» // Электронный фонд правовых и нормативно-технических документов. Акционерное общество «Информационная компания

«Кодекс». – URL: https://docs.cntd.ru/document/901990051. – Режим доступа: свободный.

4. Федеральный закон от 27.07.2006 №152-ФЗ (ред. от 02.07.2021) «О персональных данных» // Электронный фонд правовых и нормативно-технических документов. Акционерное общество «Информационная компания «Кодекс». – URL: https://docs.cntd.ru/document/901990046. – Режим доступа: свободный.

5. Федеральный закон от 06.04.2011 №63-ФЗ (ред. от 11.06.2021) «Об электронной подписи» // Электронный фонд правовых и нормативно-технических документов. Акционерное общество «Информационная компания «Кодекс». – URL: https://docs.cntd.ru/document/902271495. – Режим доступа: свободный.

6. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Электронный фонд правовых и нормативно-технических документов. Акционерное общество «Информационная компания «Кодекс». – URL: https://docs.cntd.ru/document/902377706. – Режим доступа: свободный.

7. ГОСТ Р ИСО/МЭК 27018-2020 Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки: Information technology. Security techniques and tools. Code of practice for protection of personally identifiable information (Pll) in public clouds acting as Pll processors: национальный стандарт Российской Федерации: введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 10 ноября 2020 г. №1042-ст: введен впервые: дата введения 2021-06-01 / подготовлен Федеральным государственным учреждением "Федеральный исследовательский центр "Информатика и управление" Российской академии наук" (ФИЦ ИУ РАН) и Обществом с ограниченной ответственностью "Информационно-аналитический вычислительный центр" (ООО ИАВЦ) // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/573116016. – 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-4 - Способен развертывать информационные системы у заказчика в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению информационных систем	**Промежуточный контроль:** контрольные вопросы зачета **Текущий контроль:** тестовые задания, проверка практических заданий

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 компетенций ПК-4)

51-100 баллов (зачтено) – обучающийся для получения зачета должен успешно дать полный, развернутый ответ на поставленный вопрос, продемонстрировать умение работы в электронных системах, показать совокупность осознанных знаний об объекте изучения. Ответ должен быть изложен литературным языком, в логической последовательности, показана способность быстро реагировать на уточняющие вопросы;

Менее 51 балла (не зачтено) – студент демонстрирует незнание теоретических основ предмета, не умеет делать аргументированные выводы и приводить примеры работы в системе, проявляет отсутствие логичности и последовательности изложения, делает ошибки, которые не может исправить, даже при коррекции преподавателем, отказывается отвечать на занятии.

Критерии оценивания выполнения заданий в тестовой форме (текущий контроль формирования компетенций ПК-4)

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

51-100% заданий – оценка *«Зачтено»;*

менее 51% – оценка *«Не зачтено».*

Критерии оценивания практических заданий (текущий контроль формирования компетенции ПК-4):

«отлично»: выполнены все задания, студент четко и без ошибок ответил на все контрольные вопросы;

«хорошо»: выполнены все задания, студент без с небольшими ошибками ответил на все контрольные вопросы;

«удовлетворительно»: выполнены все задания с замечаниями, студент ответил на все контрольные вопросы с замечаниями;

«неудовлетворительно»: студент 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

Контрольные вопросы к зачету (промежуточный контроль)

1. Основные понятия информационной безопасности. Задачи. Объекты защиты информации.
2. Вирусная атака. Классификация вирусов. Антивирусная защита. Виды антивирусных программ.
3. Фильтрация трафика. Обзор персональных программных межсетевых экранов
4. Технология виртуальных частных сетей.
5. Шифрование с несимметричными ключами, обзор.
6. Шифрование с симметричным ключом, обзор.
7. Защита баз данных.
8. Организационные меры по обеспечению безопасности на предприятии.
9. Защита от форс-мажор факторов.
10. Законодательство РФ в области информационной безопасности
11. Средства аутентификации: программные, физические и биологические.
12. Защита информации в операционных системах
13. Электронная цифровая подпись, принципы и примеры использования
14. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
16. Программные средства защиты.
17. Оценка качества безопасности продукции и услуг.
18. Стандарты в области информационной безопасности.

Задания в тестовой форме (текущий контроль)

1. Дополните

_____ – это защищенность информации, информационных ресурсов и систем от случайных или преднамеренных воздействий, которые могут нанести ущерб субъектам информационных отношений

2. Выберите номера правильных ответов

Укажите основные задачи информационной безопасности

1. Обеспечение подлинности и сохранности информации
2. Обеспечение разграничения доступа к информации и ресурсам системы
3. Обеспечение функционирования системы
4. Обеспечение централизованного сбора информации

3. Выберите номер правильного варианта ответа.
….– вид атаки по цели воздействия

1. Активная атака
2. Безусловная атака
3. Атака с обратной связью
4. Атака на нарушение целостности информации

4. Выберите номер правильного варианта ответа
Основная функция брандмауэра

1. Деление сети на подсети
2. Увеличение количества хостов в каждой подключенной подсети
3. Контроль трафика
4. Контроль учетных записей

5. Выберите номер правильного варианта ответа
Определите отличие идентификации от аутентификации

1. Идентификация задает права доступа к объекту, аутентификация – проверку подлинности объекта прав доступа
2. Процедура идентификации описывает объект; аутентификация обеспечивает подлинность объекта
3. Идентификация – успешная попытка представить объект не тем, чем он является; аутентификация – неуспешная попытка
4. Аутентификация – процедура обмена шифрованными ключами для опознания объекта; идентификация – процедура проверки подлинности ключей

6. Выберите номера правильных ответов
К внутренним источникам угроз безопасности относятся

1. Программное обеспечение, в том числе и разработанное на предприятии
2. Каналы связи: Internet, модемная связь, телефонные линии, факс
3. Оборудование, коммуникации, системы водоснабжения
4. Форс-мажор факторы
5. Персонал предприятия, в том числе временные и бывшие работники
6. Всё выше перечисленное

7. Дополните
_____ – это набор факторов, приводящих к сбоям или неработоспособности системы, а также наносящих урон целостности информации

8. Дополните
_____ – это специально написанная программа, способная создавать свои копии и внедрять их в файлы, системные области компьютера, вычислительные с целью

выполнения несанкционированных действий на несущем компьютере или сети

9. Выберите номер правильного варианта ответа

Определите возможности Пользователя, являющегося членом группы с правом чтения папки и имеющего личное разрешение на запись для той же папки

1. Читать и записывать в эту папку
2. Читать содержимое папки
3. Только входить в папку без возможности получения списка содержимого
4. Осуществлять полный доступ к папке и ее содержимому

10. Выберите номер правильного варианта ответа

Укажите меры, необходимые для защиты от троянских программ

1. Проверять наличие цифровой подписи
2. Никогда не устанавливать на сетевых служебных компьютерах непроверенное программное обеспечение
3. Запрашивать разрешение на прием того или иного активного объекта.
4. Использовать протокол SSL

11. Выберите номер правильного варианта ответа

ШИФРОВАНИЕ, использующее один и тот же ключ как для зашифровки, так и для расшифровки данных, называется

1. Однонаправленным шифрованием
2. Шифрованием на симметричном ключе
3. «Закрытым» шифрованием
4. Шифрованием на ассиметричном ключе

12. Выберите номера правильных ответов

Мониторинг трафика включает в себя

1. Проверку интенсивности трафика
2. Фильтрацию трафика
3. Проверку направленности трафика
4. Проверку целостности журналов трафика
5. Проверку содержания трафика
6. Проверку действий пользователя

13. Дополните

_____ подтверждает правильность и подлинность информации о фирме или индивидуальном программисте

14. Выберите номера правильных ответов

В области создания средств защиты информации действуют следующие нормативные акты:

1. Документы ФСБ о информационной безопасности
2. Документы ФАПСИ о разработке и сертификации средств криптографической защиты информации
3. Документы Гостехкомиссии о лицензировании и сертификации деятельности и средств в области защиты информации

4. ГОСТы

15. Выберите номера правильных ответов

По назначению выделяют следующие виды антивирусных программ:

1. Ревизоры
2. Иммунизаторы
3. Резидентные мониторы
4. Цензоры
5. Сканеры

16. Выберите номер правильного варианта ответа

Политики паролей не позволяют

1. Задавать минимальную длину пароля
2. Устанавливать алгоритм шифрования пароля
3. Требовать неповторяемости паролей
4. Задавать срок действия пароля

17. Выберите номера правильных ответов

Укажите государственные органы, обеспечивающие информационную безопасность в России

1. Межведомственная комиссия по государственной тайне
2. Федеральное агентство правительственной связи и информации при Президенте РФ
3. Государственная техническая комиссия при президенте РФ
4. Министерство внутренних дел
5. Федеральная служба безопасности
6. Служба внешней разведки

Типовые варианты практических заданий (текущий контроль)

Проанализировать и спроектировать план сети предприятия с учетом требований информационной безопасности и расстановкой программной средств защиты информации.

7.4. Соответствие шкалы оценок и уровней сформированных компетенций

Уровень сформированных компетенций	Количество баллов (оценка)	Пояснения
Высокий	90-100 баллов «зачтено»	Теоретическое содержание курса освоено полностью, все предусмотренные программой обучения учебные задания выполнены. Обучающийся способен на высоком уровне администрировать сетевую инфраструктуру и программное обеспечение инфокоммуникационной среды организации требований информационной безопасности
Хороший	70-89 баллов «зачтено»	Теоретическое содержание курса освоено полностью, все предусмотренные программой обучения учебные задания выполнены, однако в знаниях и умениях обучающегося наблюдаются некоторые пробелы и (или) неполное понимание вопросов. Обучающийся способен при небольшой коррекции действий со стороны администрировать сетевую инфраструктуру и программное обеспечение инфокоммуникационной среды организации требований информационной безопасности.
Средний	51-69 баллов	Теоретическое содержание курса освоено в объеме, достаточном для дальнейшего освоения основной образовательной программы,

	«зачтено»	выполнения профессиональной деятельности под руководством. Обучающийся способен под руководством администрировать сетевую инфраструктуру и программное обеспечение инфокоммуникационной среды организации требований информационной безопасности.
Низкий	Менее 51 балла «не зачтено»	Теоретическое содержание курса не освоено либо освоено в объеме, недостаточном для дальнейшего освоения основной образовательной программы, выполнения профессиональной деятельности, предусмотренные программой обучения учебные задания не выполнены либо выполнены с большим количеством грубых ошибок. Обучающийся не способен администрировать сетевую инфраструктуру и программное обеспечение инфокоммуникационной среды организации требований информационной безопасности.

8. Методические указания для самостоятельной работы обучающихся

Самостоятельная работа обучающихся – особый вид познавательной деятельности, в процессе которой происходит формирование оптимального для данного индивида стиля получения, обработки и усвоения учебной информации на основе интеграции его субъективного опыта с культурными образцами.

Формы самостоятельной работы студентов разнообразны. Они включают в себя:

- изучение и систематизацию официальных государственных документов: законов, постановлений, указов, нормативно-инструкционных и справочных материалов с использованием информационно-поисковых систем «Консультант Плюс», «Гарант», глобальной сети «Интернет»;
- изучение учебной, научной и методической литературы, материалов периодических изданий с привлечением электронных средств официальной, статистической, периодической и научной информации;
- выполнение практических заданий;
- подготовка к тестовым заданиям.

В процессе изучения дисциплины «Информационная безопасность» *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;
- подготовка к зачету.

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 студентов по основным вопросам курса. Уровень выполнения теста позволяет преподавателям судить о ходе самостоятельной работы студентов в межсессионный период и о степени их подготовки к экзамену.

Для выполнения *практического задания* необходимо внимательно прочитать задание, повторить лекционный материал по соответствующей теме, изучить рекомендуемую литературу, в т.ч. дополнительную, в которой предлагаются решения практических ситуаций и приводятся аргументы в пользу того или иного решения. На основании полученных на лекциях и лабораторных работах знаний и умений обучающиеся самостоятельно выбирают решение практического задания и реализуют его. В ходе демонстрации (защиты) полученного решения преподавателю необходимо не только сформулировать решение какой-либо задачи, но и объективно оценить свою работу, оптимальность и эффективность предлагаемого решения.

При *подготовке к промежуточной аттестации* обучающиеся должны:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

–подготовить ответы на вопросы к зачету.

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; Яндекс.Телемост (https://telemost.yandex.ru/) – инструмент для организации и проведения видеовстреч, распространяется по лицензии Shareware;

- для планирования аудиторных и внеаудиторных мероприятий: Яндекс.Календарь (https://calendar.yandex.ru/) – онлайн календарь-планер, распространяется по лицензии ShareWare;

- для совместного использования файлов: Яндекс.Документы (https://docs.yandex.ru/) – инструмент для создания и совместного использования документов, распространяется по лицензии Shareware; Yandex Forms (https://cloud.yandex.ru/services/forms) – бесплатный сервис для создания форм для опроса, регистрации и т.д., распространяется по лицензии Shareware; @Облако (https://cloud.mail.ru/) – сервис для создания, хранения и совместного использования файлов, распространяется по лицензии Shareware; Яндекс.Диск – сервис для хранения и совместного использования документов, распространяется по лицензии Shareware.

Для успешного овладения дисциплиной используются следующие информационные технологии обучения: при проведении практических занятий используются презентации материала в программе Microsoft Office (PowerPoint), выход на профессиональные сайты, использование аудиоматериалов и видеоматериалов различных интернет-ресурсов.

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.

Университет обеспечен необходимым комплектом лицензионного 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;

– антивирусная программа Kaspersky Endpoint Security для бизнеса- Стандартный Russian Edition. 250-499 Node 2 year Educational Renewal License. Лицензионный сертификат: № лицензии 1B08-201001-083025-257-1457. PN: KL4863RATFQ. Срок действия: обновляется 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;

– платформа 1С: Предприятие 8. Договор №0164/ЗК от 31.05.2021 г. Срок действия: бессрочно.

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

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

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 практических занятий, групповых и индивидуальных консультаций, текущей и промежуточной аттестации	Доска. Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, электронную информационную образовательную среду университета
Помещения для самостоятельной работы	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, электронную информационную образовательную среду университета
Помещение для хранения и профилактического обслуживания учебного оборудования.	Стеллажи. Раздаточный материал