Министерство науки и высшего образования РФ

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.12 Информационная безопасность

Направление подготовки 27.03.05 «Инноватика»
Направленность (профиль) «Управление инновационной деятельностью»
Квалификация – бакалавр
Количество зачётных единиц (часов) – 4 (144)

Екатеринбург 2025

Разработчики: к.с.-х.н., доцент  Е.В. Анянова

Рабочая программа утверждена на заседании кафедры интеллектуальных систем

(протокол № 3 от «26» ноября 2025 года)

Заведующий кафедрой  Е.В. Анянова

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией социально-экономического института
(протокол № 2 от « 04» декабря 2025 года)

Председатель методической комиссии СЭИ  А.В. Чевардин

Рабочая программа утверждена директором социально-экономического института

Директор СЭИ  Ю.А. Капустина

«04» декабря 2025 года

Оглавление

1. Общие положения 4
2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4
3. Место дисциплины в структуре образовательной программы 5
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 6
5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов 6
5.1. Трудоемкость разделов дисциплины 6
5.2. Содержание занятий лекционного типа 7
5.3. Темы и формы занятий семинарского типа (практических занятий) 7
5.4. Детализация самостоятельной работы 8
6. Перечень учебно-методического обеспечения по дисциплине 8
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине 10
7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы 10
7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания 10
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 12
7.4. Соответствие шкалы оценок и уровней сформированности компетенций 15
8. Методические указания для самостоятельной работы обучающихся 16
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине 17
10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине 19

1. Общие положения

Дисциплина «Информационная безопасность» относится к блоку Б1 учебного плана, входящего в состав основной профессиональной образовательной программы высшего образования (ОПОП ВО) 27.03.05 «Инноватика» направленность (профиль) «Управление инновационной деятельностью».

Нормативно-методической базой для разработки рабочей программы учебной дисциплины «Информационная безопасность» являются:

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

–Приказ Минобрнауки России «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» от 06.04.2021 г. № 245;

–Приказ Минобрнауки России «О внесении изменений в федеральные государственные образовательные стандарты высшего образования» от 19.07.2022 г. № 662;

–Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) направления подготовки 27.03.05 «Инноватика» (уровень бакалавриата), утвержденный приказом Министерства образования и науки РФ от 31.07.2020 г. № 870;

–Положение о практической подготовке обучающихся, утвержденное приказом Министерства науки и высшего образования Российской Федерации от 05.08.2020 г. № 885 и приказом Министерства просвещения Российской Федерации от 05.08.2020 г. № 390;

–Профессиональный стандарт 06.016 «Руководитель проектов в области информационных технологий», утвержденный Приказом Министерства труда и социальной защиты РФ от 18.11.2014 № 893н;

- Учебный план ОПОП ВО 27.03.05 «Инноватика» направленность (профиль) «Управление инновационной деятельностью» по очной форме обучения, одобренный Ученым советом УГЛТУ (протокол № 12 от 18.12.2025) и утвержденный ректором УГЛТУ (18.12.2025).

Обучение по образовательной программе 27.03.05 «Инноватика» направленность (профиль) «Управление инновационной деятельностью» 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.

Цель освоения дисциплины – формирование у студентов профессиональных знаний и умений, связанных с использованием методов защиты информации и способов управления качества продукции, процессов, услуг с учетом аспектов информационной безопасности; приобретении студентами актуальных знаний и умений, позволяющих проявить себя в будущей профессиональной деятельности, реализовать свой творческий потенциал путем использования существующего программного обеспечения, а так же поиска новых, более эффективных и функциональных средств защиты информации.

Задачи дисциплины:

- овладение теорией и методологией защиты информации;
- приобретение знаний и умений по организационному обеспечению информационной безопасности и оценке качества процессов и услуг;
- формирование знаний и умений, необходимых для использования нормативно-правовых документов, международных и отечественных стандартов в области информа-

ционной безопасности, решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности;

• освоение основ инженерно-технической защиты информации и криптографических методов;

• ознакомление с правовой базой и законодательством Российской Федерации в области информационной безопасности.

Процесс изучения дисциплины направлен на формирование следующей профессиональной компетенции:

ПК-5. Способен принимать участие в управлении рисками инновационного проекта.

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 секретности на объекте.

3. Место дисциплины в структуре образовательной программы

Данная учебная дисциплина относится к обязательным дисциплинам базовой части, что означает формирование в процессе обучения у студента основных профессиональных знаний и компетенций в рамках выбранной специальности. Освоение дисциплины «Информационная безопасность» опирается на знания, умения и компетенции, приобретённые в процессе изучения обеспечивающих дисциплин. В свою очередь, изучение дисциплины «Информационная безопасность» позволяет обучающимся быть подготовленными к изучению обеспечиваемых дисциплин (см. табл.).

Перечень обеспечивающих, сопутствующих и обеспечиваемых дисциплин

Обеспечивающие	Сопутствующие	Обеспечиваемые
Информационные технологии в профессиональной деятельности	Управление рисками в инновационной деятельности Производственная практика (преддипломная практика)	Выполнение, подготовка к процедуре защиты 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 4 зачетных единицы (144 академических часа).

Вид учебной работы	Академические часы
Контактная работа с преподавателем*:	54,25
в том числе:	18

- занятия лекционного типа (ЛЗ)	
- занятия семинарского типа (практические занятия) (ПЗ)	36
- промежуточная аттестация (ПА)	0,25
Самостоятельная работа студентов (СР)	89,75
в том числе: - изучение теоретического курса (ТО)	64
- подготовка к текущему контролю (ТК)	14
- промежуточная аттестация (ПА)	11,75
Вид промежуточной аттестации	Зачет
Общая трудоемкость	144

* 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

Очная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	ЛЗ	ПЗ	Всего контактной работы	Самостоятельная работа
1	Основные цели и задачи курса	2	4	6	8
2	Угрозы информационной безопасности на предприятии	2	6	8	14
3	Основные программные средства защиты информации	6	12	18	22
4	Организационное обеспечение информационной безопасности	4	6	10	18
5	Правовые аспекты информационной безопасности	4	8	12	16
Итого по разделам		18	36	54	78
Промежуточная аттестация		x	x	0,25	11,75
Всего часов 144					

5.2. Содержание занятий лекционного типа

Тема 1. Основные цели и задачи курса

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

Тема 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.

Тема 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.

Тема 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. Примеры реализации политик безопасности информации на различных предприятиях.

Тема 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 занятий семинарского типа (практических занятий)

Учебным планом по дисциплине предусмотрены практические занятия.

№	Наименование темы практического занятия	Форма проведения занятия	Трудоёмкость, час.
1	Основные цели и задачи курса	Семинар	4
2	Угрозы информационной безопасности на предприятии	Решение практических заданий	6
3	Основные программные средства защиты информации	Решение практических заданий	12
4	Организационное обеспечение информационной безопасности	Решение практических заданий	6
5	Правовые аспекты информационной безопасности	Решение практических заданий	8
Всего часов			36

5.4. Детализация самостоятельной работы

№	Наименование раздела (темы) дисциплины	Вид самостоятельной работы	Трудоемкость, час.
1	Основные цели и задачи курса	Изучение теоретического курса	6
		Подготовка к текущему контролю	2
2	Угрозы информационной безопасности на предприятии	Изучение теоретического курса	12
		Подготовка к текущему контролю	2
3	Основные программные средства защиты информации	Изучение теоретического курса	16
		Подготовка к текущему контролю	6

№	Наименование раздела (темы) дисциплины	Вид самостоятельной работы	Трудоемкость, час.
4	Организационное обеспечение информационной безопасности	Изучение теоретического курса	16
		Подготовка к текущему контролю	2
5	Правовые аспекты информационной безопасности	Изучение теоретического курса	14
		Подготовка к текущему контролю	2
Итого по разделу			78
Промежуточная аттестация		Подготовка к зачету	11,75
Всего часов			89,75

6. Перечень учебно-методического обеспечения по дисциплине

Основная и дополнительная учебная литература

№ п/п	Реквизиты источника	Год издания	Примечание
Основная учебная литература			
1	Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации: учебное пособие: [16+] / А. А. Сидак, В. В. Василенко, С. В. Рыженко; Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694670	2022	Полнотекстовый доступ при входе по логину и паролю*
2	Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с.– Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст: электронный	2020	Полнотекстовый доступ при входе по логину и паролю*
3	Аверченков, В. И. Аудит информационной безопасности: учебное пособие: [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с.: ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245	2021	Полнотекстовый доступ при входе по логину и паролю*
Дополнительная учебная литература			
4	Ковалев, Д. В. Информационная безопасность: учебное пособие / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. – Ростов-на-Дону: Южный федеральный университет, 2016. – 74 с.– Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493175 –	2016	Полнотекстовый доступ при входе по логину и паролю*
5	Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с.– Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348	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. Срок действия договоров продлевается ежегодно.

Справочные и информационные системы

1. Справочно-правовая система «Консультант Плюс». – URL: http://www.consultant.ru/ - Режим доступа: для авториз. пользователей.
2. Информационно-правовой портал Гарант. – URL: http://www.garant.ru/ – Режим доступа: свободный.
3. Информационная система 1С: ИТС. – URL: http://its.1c.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. Экономический портал. – URL: https://institutiones.com/. Режим доступа: свободный.
4. Информационная система РБК– URL: https://ekb.rbc.ru/. Режим доступа: свободный.
5. Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru/. Режим доступа: свободный.
6. База полнотекстовых и библиографических описаний книг и периодических изданий. – URL: (http://www.ivis.ru/products/udbs.htm). Режим доступа: свободный.
7. Сайт Центрального банка РФ: официальный сайт Центрального банка Российской Федерации. – URL: https://cbr.ru. Режим доступа: свободный.
8. ГлавбухСтуденты: Образование и карьера. – URL: http://student.1gl.ru/. Режим доступа: свободный.
9. Министерство экономического развития РФ – официальный сайт: – URL: http://economy.gov.ru/. Режим доступа: свободный.
10. Министерство промышленности и торговли РФ – официальный сайт. – URL: http://minpromtorg.gov.ru/. Режим доступа: свободный.
11. Министерство финансов РФ. Официальная статистика. – URL: http://www.minfin.ru/ru/statistics/accounts/. Режим доступа: свободный.

Нормативно-правовые акты

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
2. Федеральный закон «О государственной тайне» от 21.09.1993 № 182
3. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. N 683
4. Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. Утверждена Указом Президента Российской Федерации от 09.05.2017 № 203

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

Компетенции	Вид и форма контроля
ПК-5. Способен принимать участие в управлении рисками инновационного проекта	**Текущий контроль:** тестирование, выполнение практических заданий **Промежуточный контроль:** контрольные вопросы к зачету

Этапы формирования компетенции:

ПК-5 – первый (проведение занятий лекционного типа, второй (проведение занятий семинарского типа, самостоятельная работа обучающихся, третий (подготовка и сдача зачета).

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

Показатели и критерии оценивания устного ответа на контрольные вопросы зачета (промежуточная аттестация - зачет, формирование компетенции ПК-5)

Показатель: совокупность проявленных знаний, умений, навыков. *Критерии* оценивания:

- знание актуальности информационной безопасности, источников угроз и атак, систем критериев оценки защищенности среды.
- умение оценивать ущерб вследствие организационных нарушений информационной безопасности на предприятии, определять формы преступного посягательства;
- владеет корпоративной политикой норм и требований, предъявляемых к сотрудникам на предприятии в отношении защиты корпоративной информации.
- владение подходами к реализации мероприятий по обеспечению информационной безопасности.

«Зачтено»: обучающийся демонстрирует системные теоретические знания, владеет терминологией, делает аргументированные выводы и обобщения, приводит примеры, показывает свободное владение монологической речью и способность быстро реагировать на уточняющие вопросы. Обучающийся, применяя знания, умения и навыки, полученные при изучении дисциплины:

- *на высоком уровне* способен принимать участие в управлении рисками инновационного проекта (ПК-5).

«Зачтено»: обучающийся демонстрирует системные теоретические знания, владеет терминологией, делает аргументированные выводы и обобщения, приводит примеры, показывает свободное владение монологической речью, но при этом делает несущественные ошибки, которые быстро исправляет самостоятельно или при незначительной коррекции преподавателем. Обучающийся, применяя знания, умения и навыки, полученные при изучении дисциплины:

- *на базовом уровне* способен принимать участие в управлении рисками инновационного проекта (ПК-5).

«Зачтено»: обучающийся демонстрирует неглубокие теоретические знания, проявляет слабо сформированные навыки анализа явлений и процессов, недостаточное умение делать аргументированные выводы и приводить примеры, показывает не достаточно свободное владение монологической речью, терминологией, логичностью и последовательностью изложения, делает ошибки, которые может исправить только при коррекции преподавателем. Обучающийся, применяя знания, умения и навыки, полученные при изу-

чении дисциплины:

- *на пороговом уровне* способен принимать участие в управлении рисками инновационного проекта (ПК-5).

«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 последовательностью изложения, делает ошибки, которые не может исправить, даже при коррекции преподавателем, отказывается отвечать на занятии. Обучающийся:

- *на низком уровне* способен или не способен принимать участие в управлении рисками инновационного проекта (ПК-5).

Критерии оценивания выполнения заданий в тестовой форме (текущий контроль, формирование компетенции ПК-5)

Показатель: количество правильных ответов. *Критерии оценивания*:

- знание актуальности информационной безопасности, источников угроз и атак, систем критериев оценки защищенности среды;
- знание нормативной документами о защите информации и мер наказания нарушителей законов о защите информации;
- умение оценивать мероприятия по обеспечению информационной безопасности;
- умение оценивать ущерб вследствие организационных нарушений информационной безопасности;
- владение основными технологиями в области аутентификации данных, криптографии и обеспечении целостности данных.

По итогам выполнения тестовых заданий оценка производится по четырех балльной шкале при правильных ответах на:

86-100% заданий – «Зачтено» оценка «5» (отлично);

71-85% заданий – «Зачтено» оценка «4» (хорошо);

51-70% заданий – «Зачтено» оценка «3» (удовлетворительно);

менее 50% - «Не зачтено» оценка «2» (неудовлетворительно).

Критерии оценивания выполнения практических заданий (текущий контроль, формирование компетенции ПК-5)

Показатели: выполнение всех практических заданий; уровень ответа на контрольные вопросы при защите заданий. *Критерии оценивания*:

- знание программных средств защиты информации;
- умение обеспечения конфиденциальности, целостности задач обеспечения наблюдаемости, решаемых программными средствами защиты информации;
- умение строить модели защищенной системы;
- владение техническими мероприятиями, призванные обеспечить физическую и информационную безопасность.
- владение техническими средствами для реализации мероприятий данной группы.

«5» (отлично): выполнены все задания практических работ, обучающийся четко и без ошибок ответил на все контрольные вопросы. Обучающийся, применяя знания, умения и навыки, полученные при изучении дисциплины:

- *на высоком уровне* способен принимать участие в управлении рисками инновационного проекта (**ПК-5**).

«4» (хорошо): выполнены все задания практических работ, обучающийся ответил на все контрольные вопросы с замечаниями. Обучающийся, применяя знания, умения и навыки, полученные при изучении дисциплины:

- *на базовом уровне* способен принимать участие в управлении рисками инновационного проекта (**ПК-5**).

«3» (удовлетворительно): выполнены все задания практических работ с замечаниями, обучающийся ответил на все контрольные вопросы с замечаниями. Обучающийся, применяя знания, умения и навыки, полученные при изучении дисциплины:

- *на пороговом уровне* способен принимать участие в управлении рисками инновационного проекта (**ПК-5**).

«2» (неудовлетворительно): обучающийся не выполнил или выполнил неправильно задания практических работ, обучающийся ответил на контрольные вопросы с ошибками или не ответил на конкретные вопросы. Обучающийся:

- *на низком уровне* способен или не способен принимать участие в управлении рисками инновационного проекта (ПК-5).

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 (фрагмент) (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

Практическая работа (фрагмент) (текущий контроль)

Тема. Исследование основных методов криптографической зашиты информации

Цель: исследование основных методов криптографической зашиты информации.

Задание: на языке VBA или C++ написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем. Описание. По мере

развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ.

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

7.4. Соответствие шкалы оценок и уровней сформированности компетенций

По компетенции в зависимости от уровня освоения преподаватель выставляет следующие оценки: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соответствие шкалы оценок и уровней сформированности компетенции

Уровень сформированности компетенции	Оценка	Пояснения
Высокий	Отлично	Теоретическое содержание дисциплины освоено полностью, компетенции сформированы, все предусмотренные программой обучения учебные задания выполнены. Обучающийся демонстрирует отличную способность самостоятельного поиска, анализа и синтеза полученной информации. Отлично ориентируется в информационном пространстве и способен использовать информационные системы для решения прикладных задач. Обучающийся на высоком уровне способен принимать участие в управлении рисками инновационного проекта.
Базовый	Хорошо	Теоретическое содержание дисциплины освоено полностью, компетенции сформированы, все предусмотренные программой обучения учебные задания выполнены с незначительными замечаниями. Обучающийся демонстрирует способность самостоятельного поиска, анализа и синтеза полученной информации. Хорошо ориентируется в информационном пространстве и способен использовать информационные системы для решения прикладных задач. Обучающийся на базовом уровне способен принимать участие в управлении рисками инновационного проекта.
Пороговый	удовлетворительно	Теоретическое содержание дисциплины освоено частично, компетенции сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, в них имеются ошибки. Обучающийся демонстрирует способность поиска, анализа и синтеза полученной информации только под руководством преподавателя. Слабо ориентируется в информационном пространстве и способен использовать информационные системы для решения прикладных задач. Обучающийся на пороговом уровне способен принимать участие в управлении рисками инновационного проекта.
Низкий	неудовлетворительно	Теоретическое содержание дисциплины 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.

Уровень сформированности компетенции	Оценка	Пояснения
		Обучающийся не обладает знаниями по имеющимся системам, не способен производить поиск информации, информацию предоставляет не в структурируемом виде. Обучающийся на низком уровне способен либо не способен принимать участие в управлении рисками инновационного проекта.

8. Методические указания для самостоятельной работы обучающихся

Вид учебных занятий	Организация деятельности обучающегося
Занятия лекционного типа	В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на выполнение самостоятельной работы. В ходе лекций обучающимся рекомендуется: - вести конспектирование учебного материала; - обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению; - задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. В рабочих конспектах желательно оставлять поля, на которых во внеаудиторное время можно сделать пометки из учебно-методического обеспечения для самостоятельной работы обучающихся, дополняющего материал прослушанной лекции, а также пометки, подчеркивающие особую важность тех или иных теоретических положений. Для успешного овладения курсом необходимо посещать все лекции, так как тематический материал взаимосвязан между собой. В случаях пропуска занятия обучающемуся необходимо самостоятельно изучить материал и ответить на контрольные вопросы по пропущенной теме во время индивидуальных консультаций.
Занятия семинарского типа (практические занятия)	Практические занятия – это активная форма учебного процесса. При подготовке к праутическим занятиям обучающемуся необходимо изучить основную литературу, ознакомится с дополнительной литературой, учесть рекомендации преподавателя. Темы теоретического содержания предполагают дискуссионный характер обсуждения. Большая часть тем дисциплины носит практический характер, т.е. предполагает выполнение заданий и решение задач, анализ практических ситуаций
Самостоятельная работа (изучение теоретического курса, подготовка к практическим занятиям)	Важной частью самостоятельной работы является чтение учебной и научной литературы. Основная функция учебников – ориентировать студента в системе знаний, умений и навыков, которые должны быть усвоены будущими специалистами по данной дисциплине.
Подготовка к зачету	Подготовка к зачету предполагает: - изучение основной и дополнительной литературы - изучение конспектов лекций - участие в проводимых контрольных опросах - тестирование по темам Оценка за зачет выставляется по критериям, представленным в пункте 7.2.

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

Применение цифровых технологий в рамках преподавания дисциплины предостав-

ляет 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;

- 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 trialware;

Yandex Forms (https://cloud.yandex.ru/services/forms) – бесплатный сервис для создания форм для опроса, регистрации и т.д., распространяется по лицензии trialware.

Для успешного овладения дисциплиной используются следующие информационные технологии обучения при проведении лекций используются презентации материала в программе Microsoft Office (PowerPoint), выход на профессиональные сайты, использование 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.

Для достижения цели задач дисциплины используются в основном традиционные информативно-развивающие технологии обучения с учетом различного сочетания пассивных форм (лекция, практическое занятие, консультация, самостоятельная работа) и репродуктивных методов обучения (повествовательное изложение учебной информации, объяснительно-иллюстративное изложение) и практических методов обучения (выполнение расчетных работ).

Университет обеспечен необходимым комплектом лицензионного программного обеспечения:

- операционная система Windows 7, 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 Office Professional Plus 2010, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. 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;

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

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

– браузер Yandex (https://yandex.ru/project/browser/) – программное обеспечение распространяется по простой (неисключительной) лицензии;

– кроссплатформенное программное обеспечение для управления проектами OpenProj (https://openproj.ru.uptodown.com/windows), распространяется на условиях лицензии Common Public Attribution License Version 1.0;

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

– система управления данными Microsoft SQL Server. Контракт на услуги по предоставлению лицензий на право использовать компьютерное обеспечение № 067/ЭА от 07.12.2020 года. Срок действия: бессрочно;

– интегрированная среда для разработки Visual Studio. Контракт на услуги по предоставлению лицензий на право использовать компьютерное обеспечение № 067/ЭА от 07.12.2020 года. Срок действия: бессрочно;

– система управления реляционными базами данных MySQL (https://www.mysql.com/) – программное обеспечение с открытым кодом, распространяется по лицензии GNU GPL 2 и проприетарной лицензии;

– Apache HTTP-сервер (httpd.apache.org) – программное обеспечение с открытым кодом, распространяется по лицензии Apache License;

– скриптовый язык общего назначения PHP (php.net) – программное обеспечение с открытым исходным кодом, распространяется по лицензии PHP License;

– система управления контентом WordPress (wordpress.org) – свободно распространяемая система с открытым исходным кодом, распространяется под лицензией GNU GPL.

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, занятий семинарского типа, 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.

Оснащенность аудиторий и помещений

Наименование аудиторий и специальных помещений	Оснащенность аудиторий и специальных помещений
Помещение для занятий лекционного типа	Мультимедийное оборудование (проектор, экран или интерактивная доска, ноутбук или компьютер). Учебная мебель
Помещение для практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Столы компьютерные, стулья. Рабочие места, оборудованные компьютерами с выходом в сеть Интернет и электронную информационно-образовательную среду УГЛТУ, интерактивная доска, проектор
Помещения для самостоятельной работы обучающихся	Столы компьютерные, стулья. Рабочие места, оборудованные компьютерами с выходом в сеть Интернет и электронную информационно-образовательную среду УГЛТУ