Рабочая программа дисциплины (модуля)*
Информационная безопасность и защита информации

Направление подготовки (специальность)

02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль)

Прикладное программирование и системы искусственного интеллекта

Присваиваемая квалификация (степень)

бакалавр

Форма обучения

очная

Год набора 2026

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2026 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является теоретическая и практическая подготовка обучающихся к деятельности, связанной с комплексным анализом возможных угроз и с постановкой конкретных задач заданной степени сложности в рамках обеспечения информационной безопасности, а также содействие развитию системного мышления.

Задачи дисциплины:

– изучение основных аспектов обеспечения информационной безопасности государства;

– изучение методологии создания систем защиты информации;

– изучение основных элементов теории компьютерной безопасности;

– изучение математических основ моделей безопасности;

– изучение вопросов оценки защищенности и обеспечения безопасности компьютерных систем.

Результаты обучения по дисциплине направлены на достижение индикаторов:

УК-2.1. Демонстрирует знание теоретических основ принятия решений в сфере управления проектами.

УК-2.2. Выявляет и анализирует различные способы решения задач в рамках цели проекта и аргументирует их выбор.

УК-2.3. Демонстрирует способность проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений.

УК-10.1. Имеет представление о содержании понятий «экстремизм», «терроризм», основных формах их проявления и последствиях.

УК-10.2. Имеет представление о содержании понятия «коррупционное поведение», разграничивает коррупционные и схожие некоррупционные явления в различных сферах жизни общества.

УК-10.3. Организует профессиональную среду, опираясь на этические и правовые нормы поведения, препятствующие проявлениям экстремизма, терроризма, формированию коррупционного поведения.

ОПК-5.1. Обладает базовыми знаниями основ установки и администрирования информационных систем и баз данных с учетом информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.21

2.1 Требования к предварительной подготовке обучающегося:

Современные технологии поиска и обработки информации

Информатика

Правоведение

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Моделирование информационных процессов

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Знать:

– действующие правовые нормы и ограничения в области информационной безопасности;
– имеющиеся в организации ресурсы, влияющие на выбор способов защиты информации.

Уметь:

– формулировать задачи обеспечения информационной безопасности в рамках поставленной цели;
– выбирать оптимальные способы защиты информации с учетом правовых норм, ресурсов и ограничений.

Владеть:

– навыками применения правовых норм при выборе и обосновании способов защиты информации;

– навыками анализа ресурсных ограничений и учета их при планировании мероприятий по защите информации.

ОПК-5: Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности

Знать:

– архитектуру современных информационных систем и их типовые уязвимости;
– стандарты и модели обеспечения информационной безопасности в ИТ- системах;
– методы контроля доступа, аутентификации и регистрации событий безопасности.

Уметь:

– проектировать элементы подсистемы информационной безопасности в составе ИТ- систем;
– настраивать средства контроля доступа, регистрации и анализа событий безопасности;
– применять современные средства защиты информации при разработке и эксплуатации программных систем.

Владеть:

– навыками интеграции средств защиты информации в прикладные программные системы и сервисы;
– методами анализа и интерпретации журналов событий безопасности.

УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности

Знать:

– этические и правовые нормы поведения;
– содержание понятий «экстремизм», «терроризм», «коррупционное поведение»; основные формы их проявления и последствия;
– понятие и виды террористической деятельности;
– основы государственной политики Российской Федерации по противодействию терроризму в информационной сфере;
– нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности значимых объектов критической информационной инфраструктуры;
– способы выявления угроз информационной безопасности значимых объектов критической информационной инфраструктуры;
– основные термины и понятия гражданского права, используемые в антикоррупционном законодательстве;
– практику применения действующего антикоррупционного законодательства.

Уметь:

– правильно толковать гражданско-правовые термины, используемые в антикоррупционном законодательстве;
– разграничивать коррупционные и схожие некоррупционные явления в различных сферах жизни общества.

Владеть:

– навыками применения на практике антикоррупционного законодательства;
– навыками пресечения коррупционного поведения;
– навыками организации профессиональной среды, опираясь на этические и правовые нормы поведения, препятствующие проявлениям экстремизма, терроризма, формированию коррупционного поведения.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
3.1.2	– основы государственной информационной политики и стратегию развития информационного общества в России;
3.1.3	– основные нормативные правовые акты в области защиты информации;
3.1.4	– основные угрозы и уязвимости, характерные для распределенных и сетевых ИТ- систем;
3.1.5	– принципы построения систем криптографической защиты информации;
3.1.6	– основные международные и отечественные стандарты в области информационной безопасности.
3.2	**Уметь:**
3.2.1	– выявлять и анализировать угрозы информационной безопасности в прикладных программных и вычислительных системах;
3.2.2	– применять математические методы и алгоритмы для решения задач защиты информации;

3.2.3	– разрабатывать и обосновывать меры по повышению защищенности прикладных информационных систем;
3.2.4	– анализировать архитектуру ИТ- систем на предмет угроз информационной безопасности;
3.2.5	– выбирать и применять механизмы контроля доступа, аутентификации и шифрования;
3.2.6	– разрабатывать предложения по повышению защищенности программных и информационных систем.
3.3	**Владеть:**
3.3.1	– навыками использования программных средств защиты информации в прикладных задачах;
3.3.2	– методами документирования и представления результатов анализа и обеспечения информационной безопасности;
3.3.3	– навыками работы в междисциплинарной команде при решении задач обеспечения информационной безопасности;
3.3.4	– навыками настройки и эксплуатации программных средств защиты информации;
3.3.5	– методами документирования требований и решений в области информационной безопасности для ИТ- проектов;
3.3.6	– навыками проведения базового аудита информационной безопасности ИТ- систем.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**3 ЗЕТ**
Часов по учебному плану : 108 в том числе : аудиторные занятия : 34 самостоятельная работа : 73,8 : контактная работа: 34,2 ИКР: 0,2	Виды контроля в семестрах: зачеты 7

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Введение в информационную безопасность			
1.1	Понятие информации и информационной безопасности, конфиденциальность, целостность, доступность. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.2	Информационная безопасность в системе национальной безопасности РФ, стратегия развития информационного общества. /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.3	Нормативно- правовая база РФ в сфере ИБ (Конституция РФ, законы об информации, персональных данных, КИИ, связи и др.). /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
	Раздел 2. Методы и средства защиты информации			
2.1	Модели угроз и нарушителя, типовые уязвимости ИС, ИСПД, КИИ. /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
2.2	Криптографические методы защиты (основы шифрования, ЭП, хэш- функции, протоколы). /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3

2.3	Некриптографические методы: разграничение доступа, идентификация и аутентификация, аудит и журналирование, резервное копирование, антивирусная защита, межсетевые экраны. /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
2.4	Организационные меры защиты: политика безопасности, регламенты, служба ИБ, обязанности пользователей. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
	Раздел 3. Практика обеспечения информационной безопасности в информационных системах			
3.1	Оценка угроз и рисков, выбор мер защиты для ИС, ИСПД, объектов КИИ. /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
3.2	Основы построения СУИБ, роль ФСТЭК России, ФСБ России и др. уполномоченных органов. /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
3.3	Примеры инцидентов, анализ журналов безопасности, базовый аудит ИБ. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
3.4	Информационная безопасность в профессиональной деятельности. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
3.5	Самостоятельная проработка изученного лекционного материала, рекомендованной литературы. Закрепление практического материала. Подготовка к промежуточной аттестации. /Ср/	7	73,8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
	Раздел 4. Иная контактная работа			
4.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	7	0,2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

База тестовых вопросов закрытого типа (тестирование по основным темам онлайн/аудиторное).
База тестовых вопросов открытого типа (проверочные работы по нормативным актам и базовым понятиям).
База тестовых вопросов открытого типа для зачета (теоретический вопрос и практическое задание).

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Учебный план предусматривает для данной дисциплины лекционные занятия и самостоятельную работу обучающихся.
Промежуточная аттестация проводится в форме зачета по билетам с теоретическими вопросами и практическим заданием.

1. Тестовые задания закрытого типа
о Задания с выбором одного или нескольких правильных вариантов ответа по основным темам дисциплины: базовые понятия информации и информационной безопасности, конфиденциальность, целостность и доступность информации, виды угроз и уязвимостей, классификация нарушителей, общие требования нормативных правовых актов в области защиты информации.
о Задания на установление соответствия между понятиями и их определениями, между видами угроз и соответствующими им мерами защиты.
о Задания на выбор правильной последовательности этапов обеспечения информационной безопасности (идентификация активов, анализ угроз и уязвимостей, оценка рисков, выбор мер защиты, контроль эффективности).
Примеры:

1. Файл с персональными данными пациента был отправлен по нешифрованной электронной почте. Какое свойство информационной безопасности в первую очередь нарушается?
а) Целостность
б) Доступность
в) Конфиденциальность
г) Аутентичность
2. К какому типу угроз относится установка сотрудником несанкционированного программного обеспечения на рабочий компьютер?
а) Внешняя преднамеренная угроза
б) Внутренняя преднамеренная угроза
в) Внешняя непреднамеренная угроза
г) Внутренняя непреднамеренная угроза
3. Какой из перечисленных нормативных актов напрямую регулирует обработку персональных данных в Российской Федерации?
а) Гражданский кодекс РФ
б) Федеральный закон «Об информации, информационных технологиях и о защите информации»
в) Федеральный закон «О персональных данных»
г) Трудовой кодекс РФ

2. Тестовые задания открытого типа (проверочные работы)
о Краткие развернутые ответы по вопросам нормативного регулирования в области информационной безопасности (основные положения законодательных и подзаконных актов, регулирующих защиту информации, в том числе персональных данных и критической информационной инфраструктуры).
о Задания на раскрытие содержания ключевых терминов и категорий (информация, информационная безопасность, информационная угроза, инцидент информационной безопасности, конфиденциальная информация, персональные данные и др.).
о Ситуационные задания, требующие анализа описанной ситуации (кейс) и формулирования возможных последствий нарушения информационной безопасности, а также общих предложений по их предотвращению.
Примеры:
1. Дайте определение понятиям:
а) «информационная безопасность»;
б) «угроза информационной безопасности»;
в) «инцидент информационной безопасности».
Укажите, чем инцидент отличается от угрозы.
2.Организация обрабатывает персональные данные клиентов в информационной системе. В ходе внутренней проверки выявлено отсутствие журналирования действий пользователей и политики смены паролей.
Необходимо:
а) указать, какие свойства информационной безопасности потенциально нарушаются;
б) предложить не менее трех организационных и технических мер для снижения рисков.
3.Приведите пример ситуации нарушения конфиденциальности информации в вашей профессиональной области (или в типовой ИС) и опишите:
а) какие последствия может повлечь такое нарушение;
б) какие меры могли бы предотвратить данное нарушение.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Примеры типовых билетов:
Билет 1.
1. Теоретический вопрос:
Дайте определение понятиям «информационная безопасность», «конфиденциальность», «целостность», «доступность информации». Объясните взаимосвязь этих свойств.
2. Практическое задание:
Описана ситуация: сотрудник организации копирует служебные документы на личную USB- флешку для работы дома.
Необходимо:
а) указать, какие свойства информационной безопасности нарушаются;
б) предложить не менее трёх мер (организационных и технических), позволяющих снизить риск таких нарушений.

Билет 2.
1. Теоретический вопрос:

Перечислите основные классы угроз информационной безопасности и виды нарушителей. Приведите примеры для каждого класса.
2. Практическое задание:
В локальной сети организации используется общее файловое хранилище, к которому всем пользователям выданы права «полный доступ».
Необходимо:
а) указать возможные угрозы и последствия для информационной безопасности;
б) предложить варианты разграничения доступа и другие меры защиты.

Билет 3.
1. Теоретический вопрос:
Основные положения нормативно- правовой базы Российской Федерации в области защиты информации: назовите ключевые законы и укажите, какие виды информации они регулируют.
2. Практическое задание:
В информационной системе обрабатываются персональные данные клиентов. Пароли пользователей хранятся в открытом виде в базе данных.
Необходимо:
а) указать, какие требования информационной безопасности нарушены;
б) предложить меры по обеспечению защиты аутентификационных данных.

Билет 4.
1. Теоретический вопрос:
Криптографические методы защиты информации: основные понятия (симметричное и асимметричное шифрование, электронная подпись, хэш- функции), их назначение и области применения.
2. Практическое задание:
Организация планирует передавать конфиденциальные документы по открытым каналам связи (электронная почта, интернет- мессенджеры).
Необходимо:
а) предложить схему защиты передаваемой информации с использованием криптографических средств;
б) обосновать выбор предложенных средств и мер.

Билет 5.
1. Теоретический вопрос:
Организационные меры обеспечения информационной безопасности: политика безопасности, регламенты, распределение ролей и ответственности, обучение персонала.
2. Практическое задание:
На предприятии произошла утечка информации из- за отправки файла не тому адресату по электронной почте.
Необходимо:
а) указать возможные причины произошедшего инцидента;
б) предложить комплекс организационных и технических мер, направленных на предотвращение аналогичных инцидентов в будущем.

6.4. Критерии оценивания

В рамках промежуточной аттестации (зачёта по билетам) используются типовые контрольные вопросы и задания открытого типа, включающие:
• один теоретический вопрос, проверяющий знание основных понятий, нормативно-правовой базы и принципов обеспечения информационной безопасности;
• одно практическое задание, направленное на оценку умения анализировать угрозы и уязвимости, выбирать и обосновывать меры защиты информации.

Критерии оценивания теста
Оцениваемые результаты: знание основных понятий, классификаций, нормативной базы и базовых методов защиты информации; понимание связей между угрозами и мерами защиты.
86–100% верных ответов — оценка «зачтено».
Обучающийся демонстрирует полное и системное усвоение теоретического материала, правильно использует терминологию, допускает единичные несущественные ошибки.
71–85% верных ответов — оценка «зачтено».
Материал в целом усвоен, допущены отдельные ошибки и неточности, не искажающие основных понятий и взаимосвязей.
51–70% верных ответов — оценка «зачтено».

Знания фрагментарны, есть пропуски в понимании отдельных тем, допущено значительное количество ошибок, однако базовые представления по дисциплине сохранены.
0–50% верных ответов — оценка «не зачтено».
Отсутствует целостное представление о ключевых понятиях и закономерностях, допущено большое количество ошибок, затрудняется интерпретация результатов.

Критерии оценивания проверочной работы
Оцениваемые результаты: умение раскрывать теоретические вопросы в развернутой форме, оперировать нормативным материалом, давать определение понятиям, приводить примеры, выполнять элементарный анализ ситуаций.
«зачтено»
• Ответ полный, логичный, структурированный; корректно раскрыты все элементы вопроса; приведены необходимые определения, классификации, ссылки на нормативные акты; даны обоснованные примеры или пояснения; стилистических и логических ошибок, искажающих смысл, нет.
• Ответ в целом полный, но отдельные аспекты раскрыты менее подробно; возможны несущественные неточности в терминологии или ссылках на нормативный материал; примеры приведены, но не всегда достаточно глубоко проанализированы.
• Ответ фрагментарен, часть существенных элементов вопроса отсутствует или раскрыта поверхностно; допущены терминологические ошибки; связь с нормативной базой и практикой прослеживается слабо; однако основной смысл вопроса отражён.
«не зачтено»
• Основные элементы вопроса не раскрыты или раскрыты неверно; допущены грубые ошибки в определениях и выводах; отсутствует понимание базовых понятий и нормативных требований; ответ носит бессистемный характер или отсутствует.

Критерии оценивания зачета (по билетам)
Оцениваемые результаты: комплексно — знание теории, умение анализировать ситуации и обосновывать выбор мер защиты, владение профессиональной терминологией.
Оценка выставляется по совокупности выполнения теоретического и практического задания в билете.
«зачтено»
• Теоретический вопрос раскрыт полно и последовательно, продемонстрировано глубокое понимание понятий, классификаций, нормативной базы; используются корректные термины. Практическое задание выполнено полностью: корректно выделены угрозы и уязвимости, предложен адекватный комплекс организационных и технических мер, есть обоснование выбора. Существенных ошибок нет.
• Теоретический вопрос раскрыт в основном полно, но отдельные аспекты рассмотрены менее подробно; присутствуют единичные неточности, не влияющие на общую правильность ответа. Практическое задание решено правильно по сути, предложены разумные меры защиты, но обоснование менее детализировано, возможны отдельные упущения.
• Теоретический ответ неполный, важные элементы темы раскрыты поверхностно или пропущены; допущены терминологические ошибки. В практическом задании угрозы и меры защиты определены частично, комплекс мер неполон или слабо обоснован, но основная идея решения прослеживается.
«не зачтено»
• Теоретический вопрос не раскрыт или раскрыт неверно; продемонстрировано отсутствие понимания ключевых понятий и нормативной базы. Практическое задание не выполнено либо выполнено с грубыми ошибками (неверная идентификация угроз, предложенные меры защиты неадекватны или отсутствуют).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Партыка Т. Л., Попов И.И.	Информационная безопасность: учебное пособие (https://znanium.com/catalog/document?id=364624)	Москва : Издательство "ФОРУМ", 2021	ЭБС
Л1.2	Фомичев В. М.	Криптографические методы защиты информации: (курс лекций) : учебное пособие для академического бакалавриата: учебное пособие (https://biblioclub.ru/index.php?page=book&id=720954)	Москва : Прометей, 2023	ЭБС

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.3	Запечников С. В., Казарин О. В., Тарасов А. А.	Криптографические методы защиты информации: учебник для вузов (https://urait.ru/bcode/536453)	Москва : Юрайт, 2024	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Катаржнов А. Д.	Организационно-распорядительные документы органов власти, муниципальных образований и предприятий по защите персональных данных (https://e.lanbook.com/book/91424)	Санкт- Петербург : НИУ ИТМО, 2016	ЭБС
Л2.2	Чекулаева Е. Н., Кубашева Е. С.	Управление информационной безопасностью: учебное пособие (https://biblioclub.ru/index.php?page=book&id=612591)	Йошкар-Ола : Поволжский государственный технологический университет, 2020	ЭБС
Л2.3	Вострецова Е. В.	Основы информационной безопасности: учебное пособие (https://biblioclub.ru/index.php?page=book&id=697636)	Екатеринбург : Издательство Уральского университета, 2019	ЭБС

7.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л3.1	Кармановский Н. С., Михайличенко О. В., Прохожев Н. Н.	Организационно-правовое и методическое обеспечение информационной безопасности (https://e.lanbook.com/book/91449)	Санкт- Петербург : НИУ ИТМО, 2016	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Официальный интернет-портал правовой информации. Государственная система правовой информации http://pravo.gov.ru Раздел «Официальное опубликование правовых актов» в электронном виде» http://publication.pravo.gov.ru/
Э2	Официальный интернет-портал правовой информации. Государственная система правовой информации http://pravo.gov.ru БД «Информационно-правовая система «Законодательство России» http://pravo.gov.ru/proxy/ips/?start_search&fattrib=1
Э3	Кодексы и законы РФ - правовая справочно-консультационная система http://kodeks.systecs.ru

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

LMS Moodle

LibreOffice

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении данной дисциплины используются лекционные и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.
Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).
При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом

нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ с помощью специальных технических и программных средств к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.

Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и особенностям восприятия информации.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.

При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Направление подготовки (специальность) 02.03.02 Фундаментальная информатика и информационные технологии
Направленность (профиль) Прикладное программирование и системы искусственного интеллекта
Рабочая программа дисциплины «Информационная безопасность и защита информации»
2026 год набора, очная форма обучения

Рабочая программа дисциплины (модуля) одобрена и рекомендована:

Проректор по учебной работе	утверждено 27.02.26	А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 8 от 19.02.2026

Председатель Ученого совета математического факультета	согласовано	А. С. Скорынин

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 08 от 14.02.2026

Заведующий кафедрой	согласовано	А. Н. Ручай
Автор (составитель)		А. Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 274-1