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

Направление подготовки (специальность)

01.03.02 Прикладная математика и информатика

Направленность (профиль)

Прикладная математика и искусственный интеллект

Присваиваемая квалификация (степень)

бакалавр

Форма обучения

очная

Год(ы) набора 2025

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

Челябинск 2025 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-4.1. Имеет представление об основных существующих информационных технологиях, используемых при решении профессиональных задач.

ОПК-4.2. Демонстрирует умения использовать существующие информационные технологии при решении задач профессиональной деятельности.

ОПК-4.3. Имеет практический опыт использования существующих информационных технологий для решения задач профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.13

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;
- имеющиеся в организации ресурсы для решения поставленных задач.

Уметь:

- грамотно формулировать цель проекта;
- исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели;
- использовать организационно-правовые методы обеспечения информационной безопасности;
- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.

Владеть:

- навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели;
- навыками использования профессиональной терминологии в области информационной безопасности;
- профессиональной терминологией в области информационной безопасности;
- навыками математического моделирования угроз безопасности автоматизированных информационных систем.

ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Знать:

– пакеты современных компьютерных программ, принципы работы современных информационных технологий.

Уметь:

– воспринимать информацию, самостоятельно искать, извлекать, систематизировать, анализировать необходимую для решения задач информацию.

Владеть:

– методами сбора, обработки, интерпретаций полученной информации, используя современные информационные технологии и аппаратно-программные средства, методы хранения, защиты и подачи информации.

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;
3.1.3	– стратегию развития информационного общества в России;

3.1.4	– содержание понятий «экстремизм», «терроризм», «коррупционное поведение»; основные формы их проявления и последствия.
3.2	**Уметь:**
3.2.1	– пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;
3.2.2	– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.
3.3	**Владеть:**
3.3.1	– использования профессиональной терминологии в области информационной безопасности;
3.3.2	– построения систем защиты информации;
3.3.3	– навыками противодействия экстремизму, терроризму, коррупционному поведению в профессиональной деятельности.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**2 ЗЕТ**
Часов по учебному плану : 72 в том числе : аудиторные занятия : 34 самостоятельная работа : 34,5 : контактная работа: 37,5 ИКР: 3,5	Виды контроля в семестрах: зачеты 5

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Информационная безопасность и защита информации			
1.1	Информационная безопасность в системе национальной безопасности Российской Федерации. Понятие национальной безопасности Российской Федерации. Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.2	Основы государственной политики Российской Федерации в области информационной безопасности. Национальные интересы Российской Федерации в информационной сфере. Виды и источники угроз информационной безопасности. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.3	Понятие, виды, условия возникновения и современное состояние терроризма. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.4	Информационная безопасность в системе национальной безопасности Российской Федерации Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.5	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.6	Организационная система обеспечения информационной безопасности Российской Федерации. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3

1.7	Структура законодательства Российской Федерации в сфере обеспечения информационной безопасности. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.8	Уголовная и административная ответственность за правонарушения в информационной сфере. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.9	Основы государственной политики Российской Федерации в области информационной безопасности. Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	7,5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.10	Информационное противоборство, методы и средства его осуществления. Понятие информационного противоборства. Информационные войны, методы и средства их ведения. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.11	Информационное оружие, его классификация и возможности. Понятие кибертерроризма, виды компьютерных атак. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.12	Информационное противоборство, методы и средства его осуществления. Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.13	Виды защищаемой информации ограниченного доступа. Государственная тайна. Коммерческая тайна. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.14	Виды защищаемой информации ограниченного доступа. Персональные данные. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.15	Виды защищаемой информации ограниченного доступа. Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	7	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.16	Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры. Принципы и основные направления обеспечения информационной безопасности. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.17	Автоматизированная информационная система как объект защиты. Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.18	Общая характеристика методов и средств защиты информации в автоматизированных информационных системах. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.19	Понятие комплексного обеспечения информационной безопасности. Политика обеспечения информационной безопасности предприятия (организации). /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.20	Задачи и организационная структура подразделения обеспечения информационной безопасности предприятия (организации). /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3

1.21	Государственная система обнаружения , предотвращения и ликвидации последствий компьютерных атак (ГосСОПКА) Российской Федерации. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
1.22	Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	8	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3
	Раздел 2. Иная контактная работа			
2.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	5	3,5	

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Перечень вопросов к зачету.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Учебный план предусматривает для данной дисциплины лекционные занятия и самостоятельную работу обучающихся. Текущая аттестация предполагает проверку предоставленных рефератов по одной из предложенных тем.

Примерный перечень тем реферативных работ

1. Понятие национальной безопасности РФ. Роль и место информационной безо-пасности в системе национальной безопасности РФ.
2. Организационно-правовой режим защиты государственной тайны.
3. Организационно-правовой режим защиты коммерческой тайны.
4. Компьютерные преступления.
5. Законодательство о персональных данных.
6. Требования к защите ПД при их обработке в ИСПД.
7. Виды угроз безопасности ПД при их обработке в ИСПД.
8. Критическая информационная инфраструктура РФ.
9. Информационные войны и информационное оружие.
10. Этапы создания подразделения информационной безопасности, функциональные обязанности сотрудников.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Перечень вопросов к зачету
1. Понятие национальной безопасности. Основные угрозы и критерии оценки со-стояния национальной безопасности России.
2. Категории персональных данных. Уровни защищенности информационной сис-темы персональных данных (ИСПД).
3. Понятие информационной безопасности. Интересы личности, общества и госу-дарства в информационной сфере.
4. Обязанности обладателя конфиденциальной информации по ее защите.
5. Основные положения государственной политики и организационная основа обеспечения информационной безопасности РФ.
6. Требования к обеспечению безопасности ИСПД в зависимости от уровня защи-щенности ИСПД.
7. Угрозы информационной безопасности Российской Федерации.
8. Понятие информационной войны, цели и средства её ведения.
9. Контроль и надзор в сфере обеспечения информационной безопасности.
10. Понятие и основные свойства информации. Виды защищаемой информации.
11. Конституция РФ о правах и обязанностях граждан в информационной сфере.
12. Общие принципы и методы обеспечения информационной безопасности РФ.
13. Основные направления обеспечения информационной безопасности объектов критической информационной инфраструктуры (КИИ). Порядок категорирования объектов КИИ.
14. Состав преступления, предусмотренный статьей 274 УК РФ.
15. Задачи единой государственной системы обнаружения и предупреждения компь-ютерных атак на критически важную информационную инфраструктуру (Гос-СОПКА)..
16. Должностные обязанности руководителя подразделения информационной безо-пасности.

17. Правовой режим защиты государственной тайны. Порядок допуска к сведениям, составляющим гостайну.
18. Состав и содержание организационных и технических мер по защите ИСПД.
19. Правовой режим защиты коммерческой тайны.
20. Процедура оценки обстановки на объекте защиты.
21. Состав преступления, предусмотренный статьей 272 УК РФ.
22. Типовые и частные модели угроз безопасности ИСПД.
23. Состав преступления, предусмотренный статьей 273 УК РФ.
24. Состав и содержание организационных и технических мер по защите значимого объекта КИИ.
25. Состав преступления, предусмотренный статьей 274.1 УК РФ.
26. Этапы создания и структура службы безопасности предприятия.
27. Понятие и виды административной ответственности за нарушение требований информационной безопасности.
28. Задачи подразделения информационной безопасности предприятия.
29. Комплексная защита информации – сущность и задачи.
30. Должностные обязанности администратора безопасности АИС.
31. Компетенция ФСБ России в сфере обеспечения информационной безопасности.
32. Обязанности пользователя АИС по обеспечению информационной безопасности.
33. Понятие объекта КИИ. Порядок категорирования объектов КИИ.
34. Компетенция ФСТЭК России в сфере обеспечения информационной безопасно-сти.
35. Обязанности оператора по защите персональных данных.
36. Классификация информационного оружия.

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
Допуском к зачету является сделанный доклад по подготовленному реферату на выбранную тему.
Зачет проходит в виде теста в системе электронного обучения MOODLE.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Зачет	100
Итого		100

Критерии оценивания теста на зачете
Тест формируется в системе электронного обучения MOODLE.
Максимальный балл за тест – 100 баллов.
Отлично/зачтено/91-100 баллов.
Хорошо/зачтено/70-90 баллов.
Удовлетворительно/зачтено/51-69 баллов.
Неудовлетворительно/не зачтено/0-50 баллов.

При подведении итогов учитываются результаты текущей аттестации:
0-60 баллов – не зачтено;
61-100 баллов – зачтено.

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	Рытенкова О.	Информационная безопасность: журнал (https://biblioclub.ru/index.php?page=book&id=238446)	Москва : ГРОТЕК, 2014	ЭБС
Л1.2	Белоус А.И., Солодуха В.А.	Кибероружие и кибербезопасность. О сложных вещах простыми словами: монография (https://znanium.com/catalog/document?id=361651)	Вологда : Инфра-Инженерия, 2020	ЭБС
Л1.3	Партыка Т. Л., Попов И.И.	Информационная безопасность: учебное пособие (https://znanium.com/catalog/document?id=364624)	Москва : Издательство "ФОРУМ", 2021	ЭБС

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.4	Мельников В.П., Куприянов А.И., Мельников В.П.	Информационная безопасность: учебник (https://book.ru/book/944143)	Москва : КноРус, 2022	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Загинайлов Ю. Н.	Основы информационной безопасности: курс визуальных лекций: учебное пособие (https://biblioclub.ru/index.php?page=book&id=362895)	Москва, Берлин : Директ-Медиа, 2015	ЭБС
Л2.2		Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: практикум (https://biblioclub.ru/index.php?page=book&id=458012)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016	ЭБС
Л2.3	Диогенес Ю., Озкайя Э.	Кибербезопасность. стратегия атак и обороны (https://e.lanbook.com/book/131717)	Москва : ДМК Пресс, 2020	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

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) 01.03.02 Прикладная математика и информатика
Направленность (профиль) Прикладная математика и искусственный интеллект
Рабочая программа дисциплины «Информационная безопасность и защита информации»
2025 год набора, очная форма обучения

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 от 01.02.2025

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. № 247-1