Рабочая программа дисциплины (модуля)*

Информационная безопасность и защита информации

Направление подготовки (специальность)

02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль)

Математические и алгоритмические основы интеллектуальных систем

Присваиваемая квалификация (степень)

бакалавр

Форма обучения

очная

Год(ы) набора

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

Челябинск 2025 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Основная цель это вооружение конкретными знаниями и умениями, дающими возможность квалифицированно осуществлять профессиональную деятельность.

Результаты обучения по дисциплине направлены на достижение следующих 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

ПК-3.1. Демонстрирует методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

ПК-3.2. Умеет разрабатывать требования к программному продукту, применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

ПК-3.3. владеет навыками проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

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.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.В.1.07

2.1 Требования к предварительной подготовке обучающегося:

Правоведение

Архитектура вычислительных систем

Интернет-технологии

Операционные системы

Информатика

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

Программная инженерия

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:

Для достижения УК 2.1: основы информационной безопасности и защиты информации в сфере управления проектами

Уметь:

Для достижения УК 2.2: выявлять и анализировать различные способы решения задач информационной безопасности и защиты информации в рамках цели проекта и обосновывать их выбор.

Владеть:

Для достижения УК 2.3: навыками обеспечения информационной безопасности при решении задач проекта, выбирая оптимальный способ защиты информации, исходя из действующих правовых норм и имеющихся ресурсов.

ПК-3: Способность к разработке требований и проектированию программного обеспечения на основе применения базовых математических знаний и информационных технологий при решении проектно-технических и прикладных задач

Знать:

Для достижения ПК-3.1: методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

Уметь:

Для достижения ПК-3.2: разрабатывать требования к программному продукту, применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

Владеть:

Для достижения ПК-3.3: навыками проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

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

Знать:

Для достижения УК-10.1: методы информационной безопасности в сфере противодействия экстремизму и терроризму

Уметь:

Для достижения УК-10.2: противодействовать экстремизму и терроризму в информационной среде

Владеть:

Для достижения УК-10.3: навыками защиты информации от проявлений экстремизма и терроризма

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	теоретические основы принятия решений в информационной безопасности и защите информации.
3.2	**Уметь:**
3.2.1	выявлять и анализировать различные способы решения задач информационной безопасности и защиты информации в рамках цели проекта и обосновывать их выбор.
3.3	**Владеть:**
3.3.1	навыками обеспечения информационной безопасности при решении задач проекта, выбирая оптимальный способ защиты информации, исходя из действующих правовых норм и имеющихся ресурсов.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость			**2 ЗЕТ**
Часов по учебному плану	:	72	Виды контроля в семестрах:
в том числе	:		
аудиторные занятия	:	44	зачеты 6
самостоятельная работа	:	23,5	
контактная работа: 48,5			
ИКР: 4,5			

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код заняти	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Правовая основа информационной безопасности информационных систем			

1.1	Предмет, цели и задачи дисциплины “Информационная безопасность и защита информации”. Основные определения и понятия. Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ. Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации. Тенденции развития информационной политики государств и ведомств. Государственная тайна. Правовое обеспечение защиты информации. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
1.2	Правовая основа информационной безопасности информационных систем. /Ср/	6	8	Л1.1 Л1.2 Л1.3Л2.1 Э1
	Раздел 2. Технологические основы информационной безопасности. Основные понятия и определения.			
2.1	Понятие информации, информатизации, информационных систем и смежных с ними: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера. Понятие автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы определения, сопоставление. /Лек/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Э1
2.2	Технологические основы информационной безопасности. Основные понятия и определения. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
2.3	Технологические основы информационной безопасности. /Лаб/	6	2	Л1.1Л2.1 Э1
	Раздел 3. Общеметодологические принципы теории информационной безопасности			
3.1	Этапы развития информационной безопасности. Этап комплексной защиты. Требования к системе защиты информации. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Комплексность: целевая, инструментальная, структурная, функциональная, временная. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
3.2	Общеметодологические принципы теории информационной безопасности. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
3.3	Общеметодологические принципы теории информационной безопасности. /Лаб/	6	4	Л1.1Л2.1 Э1
	Раздел 4. Классификация и анализ угроз информационной безопасности			
4.1	Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: Подверженность физическому искажению или уничтожению. Возможность несанкционированной (случайной или злоумышленной) модификации. Опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные. /Лек/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Э1
4.2	Классификация и анализ угроз информационной безопасности. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
4.3	Классификация и анализ угроз информационной безопасности. /Лаб/	6	4	Л1.1Л2.1 Э1

	Раздел 5. Причины, виды, каналы утечки и искажения информации			
5.1	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты - модель системы с полным перекрытием. Последовательность решения задач защиты информации. Фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
5.2	Причины, виды, каналы утечки и искажения информации. /Лаб/	6	4	Л1.1 Л1.2Л2.1 Э1
	Раздел 6. Функции и задачи защиты информации			
6.1	Методы формирования функций защиты. Сокрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
6.2	Функции и задачи защиты информации. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
6.3	Функции и задачи защиты информации. /Лаб/	6	4	Л1.1 Л1.3Л2.1 Э1
	Раздел 7. Криптографические методы защиты информации			
7.1	Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89. Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами. Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
7.2	Причины, виды, каналы утечки и искажения информации. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
7.3	Криптографические методы защиты информации. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
7.4	Криптографические методы защиты информации. /Лаб/	6	4	Л1.1Л2.1 Э1
	Раздел 8. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей			

8.1	Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети. Применение паролей и биометрических средств аутентификации пользователей. Протоколы взаимной проверки подлинности объектов сети. Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI. Обеспечение целостности информации. Аутентификация информации и ЭЦП сообщений. Однонаправленные хэш-функции. Коды проверки подлинности информации. Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов. /Лек/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Э1
8.2	Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей. /Ср/	6	1,5	Л1.1 Л1.2 Л1.3Л2.1 Э1
8.3	Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей. /Лаб/	6	4	Л1.1Л2.1 Э1
	Раздел 9. Архитектура и методы организации систем защиты информации			
9.1	Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. Специализированные программно-аппаратные средства защиты информации. Средства и механизмы обеспечения безопасности сетевого оборудования Cisco systems. Серверы доступа (брандмауэры) Cisco ASA5500. Средства обнаружения вторжений IDS 4200. /Лек/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Э1
9.2	Архитектура и методы организации систем защиты информации. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Э1
9.3	Архитектура и методы организации систем защиты информации. /Лаб/	6	4	Л1.1Л2.1 Э1
	Раздел 10. Иная контактная работа			
10.1	Индивидуальные консультации, текущий контроль. /ИКР/	6	4,5	Л1.1 Л1.2Л2.1 Э1

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

1. Самостоятельная работа в форме домашних работ
2. Проверка понятийного аппарата (опрос)
3. Участие в конференции
4. Компьютерное тестирование

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

1. Какие мероприятия с использованием пассивных технических средств позволяют закрывать каналы утечки информации?
А) Локализация излучений;
Б) Пространственное зашумление;
В) Развязывание информационных сигналов;
Г) Линейное зашумление;
Д) Уничтожение закладных устройств.

2. Какие из технических каналов утечки информации относятся к речевой информации?

А) Электромагнитные;
Б) Вибрационные;
В) Оптико-электронный;
Г) Электрический.

3. Основные угрозы доступности информации:
А) непреднамеренные ошибки пользователей;
Б) хакерская атака;
В) отказ программного и аппаратно обеспечения;
Г) перехват данных.

4. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ):
А) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения;
Б) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты;
В) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом.

5. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
А) несанкционированного управления удаленным компьютером;
Б) внедрения агрессивного программного кода в рамках активных объектов Web-страниц;
В) перехвата или подмены данных на путях транспортировки
вмешательства в личную жизнь;
Г) поставки неприемлемого содержания.

6. Наиболее эффективное средство для защиты от сетевых атак?
А) Использование сетевых экранов или «firewall»;
Б) Использование антивирусных программ;
В) Посещение только «надёжных» Интернет-узлов;
Г) Использование только сертифицированных программ-браузеров при доступе к сети Интернет.

7. Информация, составляющая государственную тайну не может иметь гриф…
А) «для служебного пользования»;
Б) «секретно»;
В) «совершенно секретно»;
Г) «особой важности».

8. Разделы современной криптографии:
А) Симметричные криптосистемы;
Б) Криптосистемы с открытым ключом;
В) Криптосистемы с дублированием защиты;
Г) Системы электронной подписи;
Д) Управление паролями;
Е) Управление передачей данных;
Ё) Управление ключами.

9. Суть компрометации информации?
А) Внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации;
Б) Несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений;
В) Внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений.

10. К формам защиты информации не относится…
А) аналитическая;
Б) правовая;
В) организационно-техническая;
Г) страховая.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

1. Общая проблема информационной безопасности информационных систем. Доктрина информационной

безопасности РФ
2. Приоритетные направления в области защиты информации. Тенденции развития информационной политики государств и ведомств.
3. Защита информации, тайна, средства защиты информации, угрозы и определения, сопоставление.
4. Этапы развития информационной безопасности.
5. Требования к системе защиты информации.
6. Показатели информации.
7. Понятие угрозы. Виды угроз.
8. Последовательность решения задач защиты информации.
9. Фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации.
10. Методы формирования функций защиты.
11. Управление системой защиты информации.
12. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности.
13. Классификация криптографических методов.
14. Стойкость криптосистем.
15. Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA..
16. Криптосистема Эль Гамаля.
17. Криптосистемы без передачи ключей.
18. Управление ключами. Методы генерации, хранения и распределения ключей.
19. Протоколы управления ключами.
20. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП).
21. Идентификация и аутентификация объектов сети.
22. Идентификация и подтверждение подлинности пользователей сети. Применение паролей и биометрических средств аутентификации пользователей.
23. Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ.
24. Особенности межсетевого экранирования на различных уровнях модели OSI.
25. Обеспечение целостности информации. Аутентификация информации и ЭЦП сообщений. Однонаправленные хэш-функции. Коды проверки подлинности информации.
26. Средства антивирусной защиты.
27. Архитектура системы защиты информации (СЗИ).
28. Средства и механизмы обеспечения безопасности сетевого оборудования Cisco systems.
29. Средства обнаружения вторжений IDS 4200.

6.4. Критерии оценивания

1. Самостоятельная работа в форме домашних работ - 0-5 баллов
2. Проверка понятийного аппарата (опрос) - 0-10 баллов
3. Участие в конференции - 0-10 баллов
4. Компьютерное тестирование - 0-20 баллов

Для допуска на зачет по дисциплине студент должен набрать 40 баллов. Зачет проводится в два этапа. На первом этапе студент выполняет компьютерный тест из 10 вопросов. Продолжительность – до 25 минут. На втором этапе студенту выдаётся теоретический вопрос по одному из разделов дисциплины из базы контрольных вопросов к зачету. Время выполнения – до 20 минут. Максимальное количество зарабатываемых баллов – 25.
«Зачтено» (не ниже 60 баллов) – выставляется студенту, если: он твердо знает программный материал, грамотно и по существу его излагает; владеет основными методами; не допускает существенных ошибок; умеет применять основные положения на практике, выполняет тест не менее чем на 60 %.
«Не зачтено» (ниже 60 баллов) – выставляется студенту в том случае, если он: не знает основополагающих вопросов изучаемого курса или значительной части программного материала; допускает ошибки, обнаруживает неумение их исправлять; не может увязать теорию с практикой, выполняет тест менее чем на 60 %.
Студенты, не набравшие достаточного количества баллов в течение семестра и не выполнившие практические работы сдают зачет повторно в форме беседы совместно с решением задачи.

Эти критерии доводятся до сведения студентов в ходе учебного процесса и проведении консультаций.
При оценке знаний студента учитываются также:
- результаты текущего контроля;
- посещаемость учебных занятий;

- активность во время занятий;
- участие в научной работе;
- наличие навыков самостоятельной и исследовательской работы.

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачете.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства.
Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:
для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа,
для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,
При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:
а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме);
б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются ассистентом);
в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, с использованием услуг ассистента, устно).
При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

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

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Ресурс
Л1.1	Спицын В. Г.	Информационная безопасность вычислительной техники: учебное пособие (https://biblioclub.ru/index.php?page=book&id=208694)	Томск : Эль Контент, 2011	ЭБС
Л1.2	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
Л1.3	Аверченков В. И.	Аудит информационной безопасности: учебное пособие (https://biblioclub.ru/index.php?page=book&id=93245)	Москва : ФЛИНТА, 2021	ЭБС

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Ресурс
Л2.1	Голиков А. М.	Основы проектирования защищенных телекоммуникационных систем: учебное пособие для специалитетета: 10.05.02 информационная безопасность телекоммуникационных систем. курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу (https://e.lanbook.com/book/110273)	Москва : ТУСУР, 2016	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг http://biblioclub.ru/

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

LMS Moodle

Adobe Reader

Microsoft Office Professional Plus 2010 (Лицензия Троицкого филиала)

Microsoft Office Professional Plus 2013 (Лицензия Троицкого филиала)

Айрен (IREN)

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. ИНФОРМИО [Электронный ресурс] : электронный справочник [обеспечение всех типов образовательных учреждений нормативными, методическими, научно-практическими материалами]. – URL: http://www.informio.ru/.

2. Национальная электронная библиотека (НЭБ) [Электронный ресурс]: объединенный электронный каталог фондов российских библиотек: сайт. – URL: http://нэб.рф.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Материально-техническое обеспечение реализации рабочей программы дисциплины «Информационная безопасность и защита информации» включает:

- основную и дополнительную литературу;
- любые учебные аудитории (посадочные места не менее 15) с проекторами мультимедиа-оборудованием (проектор, ноутбук или стационарный компьютер) для проведения лекционных занятий в зависимости от занятости аудиторного фонда филиала;
- учебная аудитория для проведения самостоятельной работы студентов;
- наличие помещений для самостоятельной работы с компьютерной техникой и с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации;
- сайт tfmoodle.csu.ru, на котором расположены материалы для организации самостоятельной работы студентов.
- Обучение инвалидов и лиц с ограниченными возможностями здоровья осуществляется с применением следующего специального оборудования:

а) для лиц с нарушением слуха (колонки, мультимедийный проектор);

б) для лиц с нарушением зрения (мультимедийный проектор (использование презентаций с укрупненным текстом));

в) для лиц с нарушением опорно-двигательного аппарата (персональные мобильные компьютеры).

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

1. Общие методические указания по изучению дисциплины

Обучение дисциплине «Информационная безопасность и защита информации» включает в себя следующие основные положения:
– изучение базовых методов и технологий защиты информации;
– изучение технологий работы со сложно структурированной информацией;
– формирование умения находить правильный метод для решения поставленных задач.
При изучении дисциплины студент должен овладеть базовыми методами и новыми методами работы с системами защиты информации, уяснить понятийный аппарат СЗИ, научиться проектировать СЗИ, анализировать полученные результаты. Для достижения этой цели студент должен:
– Осуществлять фиксацию информации в интеллект-картах, чтобы иметь в наличии ответы на вопросы программы изучаемой дисциплины.
– Творчески применять изученные методы работы в проектах.
– В процессе обучения осуществлять тщательную проработку информации, полученной в ходе лекционных занятий и чтения учебника, предусматривающую запоминание основных положений, формулировок, определений, принципов, методов.
– В процессе обучения творчески и самостоятельно работать с заданиями.
– Выполнять поиск информации различными способами, для чего требуется интуиция, творческий

потенциал, которые, в свою очередь, вырабатывается при реализации творческих проектов. Это приводит к необходимости реализовывать задания самостоятельно, в неаудиторных условиях.
В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (Microsoft Teams, форумы, электронная почта, сотовая связь) и отложенного времени (системы дистанционного обучения Moodle, электронная почта, форумы).
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 системы дистанционного обучения Moodle, электронной почты, сотовой связи, форумов.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

2. Методические указания студентам по выполнению самостоятельной работы

1. Для выполнения самостоятельной работы, нужно проработать материалы лекционных занятий, а также материалы учебника по данной теме, изучить интернет-ресурсы, освоить работу с соответствующим программным обеспечением.
2. Самостоятельная работа выполняется с использованием по следующей схеме:
– изучить теоретический материал по методам работы с информацией различного вида;
– подобрать варианты выполнения задания;
– разработать план работы;
– выполнить задание с подробным объяснением;
– предоставить результат в виде прикладного решения.
3. Проверка в течение семестра результатов самостоятельной работы проводится преподавателем с последующим выставлением баллов.
4. Если студент не может справиться с самостоятельной работой, то ему необходимо приходить на дополнительные занятия.

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.

02.03.02 Фундаментальная информатика и информационные технологии. Математические и алгоритмические основы интеллектуальных систем. Информационная безопасность и защита информации, 2025 год набора, очная

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом Троицкого филиала ФГБОУ ВО «ЧелГУ»

Протокол заседания № 6 от 21.02.2025

Председатель Ученого совета
Троицкого филиала ФГБОУ ВО
«ЧелГУ» согласовано Л.А. Захарова

Заседанием кафедры гуманитарных и естественно-научных дисциплин

Протокол заседания № 6 от 20.02.2025

Заведующий кафедрой согласовано И.В. Черетских

Автор (составитель) С.М. Серебрянский

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1