Рабочая программа дисциплины (модуля)*

Информационная безопасность

Направление подготовки (специальность)

38.05.01 Экономическая безопасность

Направленность (профиль)

Экономико-правовое обеспечение экономической безопасности

Присваиваемая квалификация (степень)

экономист (специалист)

Форма обучения

заочная

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

формирование профессиональных компетенций обучающихся при работе с современными системами информационной безопасности, технологическими способами защиты информации, организационными мерами по информационной защите, экономическими и правовыми принципами их функционирования, а также возможностями использования защиты в работе с информационными ресурсами в различных областях экономики и бизнеса.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.18

2.1 Требования к предварительной подготовке обучающегося:

Информационная культура

Информационная культура

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

Экономическая безопасность

Экономическая безопасность

Национальная и региональная экономическая безопасность

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

ОПК-6: Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.

Знать:

современные информационные технологии и программные средства для решения профессиональных задач

Уметь:

использовать современные информационные технологии и программные средства при решении профессиональных задач

Владеть:

навыками использования современных информационных технологий и программных средств при решении профессиональных задач

ОПК-7: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Знать:

принципы работы современных информационных технологий и использования их для решения задач профессиональной деятельности

Уметь:

понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Владеть:

навыками понимания принципов работы современных информационных технологий и использования их для решения задач профессиональной деятельности

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	современные информационные технологии и программные средства для решения профессиональных задач
3.1.2	принципы работы современных информационных технологий и использования их для решения задач профессиональной деятельности
3.2	**Уметь:**

3.2.1	использовать современные информационные технологии и программные средства при решении профессиональных задач
3.2.2	понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
3.3	**Владеть:**
3.3.1	использования современных информационных технологий и программных средств при решении профессиональных задач
3.3.2	понимания принципов работы современных информационных технологий и использования их для решения задач профессиональной деятельности

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**3 ЗЕТ**
Часов по учебному плану : 108 в том числе : аудиторные занятия : 8 самостоятельная работа : 94,55 часов на контроль : 4 контактная работа: 9,45 ИКР: 1,45	Виды контроля на курсах: зачеты 3

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации			
1.1	Информационная безопасность в системе национальной безопасности Российской Федерации /Лек/	3	0,5	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
1.2	Лабораторная работа №1. Законодательный уровень информационной безопасности /Лаб/	3	0,5	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
1.3	Информационная безопасность в системе национальной безопасности Российской Федерации /Ср/	3	16	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
	Раздел 2. Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности			
2.1	Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности /Ср/	3	18	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
2.2	Лабораторная работа №2. Стандарты и спецификации в области информационной безопасности Лабораторная работа №3. Создание и управление учетными записями пользователей /Лаб/	3	1	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
2.3	Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности /Лек/	3	1	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
	Раздел 3. Методы и средства обеспечения информационной безопасности. Защита информации криптографическими методами			
3.1	Методы и средства обеспечения информационной безопасности. Защита информации криптографическими методами /Лек/	3	1	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3

3.2	Лабораторная работа №4. Защита информации криптографическими методами. Шифры замены. /Лаб/	3	1	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
3.3	Методы и средства обеспечения информационной безопасности. Защита информации криптографическими методами /Ср/	3	12,55	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
	Раздел 4. Основы комплексного обеспечения информационной безопасности. Модели, стратегии (политики) и системы обеспечения информационной безопасности			
4.1	Основы комплексного обеспечения информационной безопасности. Модели, стратегии (политики) и системы обеспечения информационной безопасности /Ср/	3	16	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
4.2	Лабораторная работа № 5. Аудит информационных процессов Лабораторная работа № 6. Аудит реестра в операционной системе /Лаб/	3	0,5	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
4.3	Основы комплексного обеспечения информационной безопасности. Модели, стратегии (политики) и системы обеспечения информационной безопасности /Лек/	3	0,5	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
	Раздел 5. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей			
5.1	Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей /Лек/	3	0,5	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
5.2	Лабораторная работа № 7. «Контур-Экстерн» - система электронного защищенного документооборота /Лаб/	3	0,5	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
5.3	Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей /Ср/	3	16	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
	Раздел 6. Методология построения и анализа систем обеспечения информационной безопасности			
6.1	Методология построения и анализа систем обеспечения информационной безопасности /Ср/	3	16	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
6.2	Лабораторная работа №6. Изучить работу шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации. /Лаб/	3	0,5	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
6.3	Методология построения и анализа систем обеспечения информационной безопасности /Лек/	3	0,5	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
	Раздел 7. Зачет			
7.1	зачет по информационной безопасности /Зачёт/	3	0	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3
	Раздел 8. Иная контактная работа			
8.1	Индивидуальные консультации, текущий контроль /ИКР/	3	1,45	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Тест
Собеседование

Защита лабораторной работы
Ситуационная задача

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

1. Вопросы для собеседования при защите лабораторной работы
Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации
1. Информация как объект правового регулирования.
2. Структура информационной сферы и характеристика ее элементов.
3. Виды информации.
4. Конституционные гарантии прав на информацию и механизм их реализации.
5. Законодательство РФ в области информационной безопасности.
6. Субъекты и объекты правоотношений в области информационной безопасности. Понятия и виды защищаемой информации по российскому законодательству.
7. Отрасли законодательства, регламентирующие деятельность по защите информации.

Тема 2. Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности
1. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
2. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
3. Органы защиты государственной тайны и их компетенция.
4. Порядок допуска и доступа к государственной тайне.
5. Перечень и содержание организационных мер, направленных на защиту государственной тайны.
6. Ответственность за нарушение правового режима защиты государственной тайны.

Тема 3. Методы и средства обеспечения информационной безопасности. Защита информации криптографическими методами
1. Виды угроз информационной безопасности на объекте защиты.
2. Цели и задачи организационной защиты информации.
3. Виды угроз информационной безопасности.
4. Модели нарушителей.
5. Основные направления организационной защиты на объекте.
6. Структура сил и средств организационной защиты информации.
7. Служба безопасности объекта.
8. Принципы организации службы безопасности объекта.
9. Типовая структура службы безопасности.
10. Основные документы, регламентирующие деятельность службы безопасности. Действия сотрудников службы безопасности в чрезвычайных условиях.

Тема 4. Основы комплексного обеспечения информационной безопасности. Модели, стратегии (политики) и системы обеспечения информационной безопасности
1. Организация и обеспечение секретного делопроизводства.
2. Требования режима секретности при работе с секретными документами. Назначение и задачи секретного делопроизводства.
3. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов.
4. Допуск к секретной (конфиденциальной) информации.
5. Обеспечение режима секретности при проведении НИОКР по секретной(конфиденциальной) тематике.
6. Организация обеспечения режима секретности при проведении служебного совещания.
7. Организация работ по защите информации при опубликовании открытых материалов.
8. Экспертные комиссии.

Тема 5. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей
1. Основные понятия, используемые при описании моделей разграничения доступа: объект, субъект, метод, право, привилегия, владелец, суперпользователь.
2. Избирательное разграничения доступа.
3. Понятие матрицы доступа. Два подхода к кодированию матрицы доступа: векторы и списки.
4. Изолированная программная среда. Полномочное разграничение доступа.
5. Средства динамического изменения полномочий пользователя: необходимость, различные подходы к реализации.

6. Особенности разграничения доступа в системах управления базами данных.
7. Разграничение доступа в Unix- системах.
8. Формат, атрибутов защиты файла.
9. Разграничения доступа в Windows. Права, привилегии.
10. Формат атрибутов защиты объекта. Концепция олицетворения.

Тема 6. Методология построения и анализа систем обеспечения информационной безопасности
1. Основные типы компьютерных вирусов: файловые, сетевые, почтовые, макровирусы.
2. Основные модели программных закладок: наблюдатель, перехват, искажение. Типичные признаки присутствия в системе компьютерных вирусов и программных закладок.
3. Основные средства и методы противодействия компьютерным вирусам и программным закладкам: сигнатурное и эвристическое сканирование, контроль целостности, антивирусный мониторинг.
4. Факторы, ограничивающие эффективность антивирусных средств.
5. Задача защиты от несанкционированного копирования.
6. Методы привязки к программно-аппаратной среде.
7. Применение специальных аппаратных устройств (электронных ключей и т.п.) для защиты от несанкционированного копирования информации.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

1. Вопросы для собеседования после написания теста
1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности
4. Место информационной безопасности в системе национальной безопасности
5. Интересы личности в информационной сфере
6. Интересы общества в информационной сфере
7. Интересы государства в информационной сфере
8. Угрозы информационному обеспечению государственной политики Российской Федерации
9. Виды угроз информационной безопасности
10. Внешние источники угроз информационной безопасности
11. Внутренние источники угроз информационной безопасности государства.
12. Информационное оружие, его классификация и возможности.
13. Доктрина информационной войны
14. Методы и средства ведения информационной войны
15. Понятие информационного противоборства
16. Причины искажения информации,
17. Виды искажения информации
18. Каналы утечки информации
19. Естественные и искусственные каналы утечки информации
20. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств ВТ
22. Компьютерная система как объект информационной безопасности.
23. Информационные процессы как объект информационной безопасности
24. Влияние человеческого фактора на обеспечение информационной безопасности
25. Программно-аппаратные средства обеспечения информационной безопасности.
26. Классификация программно-аппаратных средств обеспечения информационной безопасности
27. Защита от несанкционированного доступа
28. Антивирусная защита
29. Межсетевые экраны
30. VPN-технологии
31. Криптографические методы защиты информации

2. Примеры тестовых заданий
1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Сотрудники
Хакеры
Атакующие

Контрагенты (лица, работающие по договору)

2. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
Улучшить контроль за безопасностью этой информации
Снизить уровень классификации этой информации

3. Что самое главное должно продумать руководство при классификации данных?
Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
Необходимый уровень доступности, целостности и конфиденциальности
Оценить уровень риска и отменить контрмеры
Управление доступом, которое должно защищать данные

4. Что такое процедура?
Правила использования программного и аппаратного обеспечения в компании
Пошаговая инструкция по выполнению задачи
Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
Обязательные действия

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
Владельцы данных
Пользователи
Администраторы
Руководство

6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
Поддержка высшего руководства
Эффективные защитные меры и методы их внедрения
Актуальные и адекватные политики и процедуры безопасности
Проведение тренингов по безопасности для всех сотрудников

7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
Когда риски не могут быть приняты во внимание по политическим соображениям
Когда необходимые защитные меры слишком сложны
Когда стоимость контрмер превышает ценность актива и потенциальные потери

8. Что такое политики безопасности?
Пошаговые инструкции по выполнению задач безопасности
Общие руководящие требования по достижению определенного уровня безопасности
Широкие, высокоуровневые заявления руководства
Детализированные документы по обработке инцидентов безопасности

9. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
Анализ рисков
Анализ затрат / выгоды
Результаты ALE
Выявление уязвимостей и угроз, являющихся причиной риска

10. Что лучше всего описывает цель расчета ALE?
Количественно оценить уровень безопасности среды
Оценить возможные потери для каждой контрмеры
Количественно оценить затраты / выгоды
Оценить потенциальные потери от угрозы в год

11. Тактическое планирование – это:
Среднесрочное планирование

Долгосрочное планирование
Ежедневное планирование
Планирование на 6 месяцев

12. Что является определением воздействия (exposure) на безопасность?
Нечто, приводящее к ущербу от угрозы
Любая потенциальная опасность для информации или систем
Любой недостаток или отсутствие информационной безопасности
Потенциальные потери от угрозы

13. Эффективная программа безопасности требует сбалансированного применения:
Технических и нетехнических методов
Контрмер и защитных механизмов
Физической безопасности и технических средств защиты
Процедур безопасности и шифрования

14. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
Внедрение управления механизмами безопасности
Классификацию данных после внедрения механизмов безопасности
Уровень доверия, обеспечиваемый механизмом безопасности
Соотношение затрат / выгод

15. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
Только военные имеют настоящую безопасность
Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
Военным требуется больший уровень безопасности, т.к. их риски существенно выше
Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

16. Как рассчитать остаточный риск?
Угрозы х Риски х Ценность актива
(Угрозы х Ценность актива х Уязвимости) х Риски
SLE х Частоту = ALE
(Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

17. Что из перечисленного не является целью проведения анализа рисков?
Делегирование полномочий
Количественная оценка воздействия потенциальных угроз
Выявление рисков
Определение баланса между воздействием риска и стоимостью необходимых контрмер

18. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
Поддержка
Выполнение анализа рисков
Определение цели и границ
Делегирование полномочий

3. Пример ситуационной задачи

Вы – сотрудник лечебного учреждения. Ежедневно в базе данных происходит накопление большого количества информации.

1. Перечислите возможные способы обеспечения целостности и предотвращения уничтожения данных.

2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему.

Ответ к задаче №1

1. Резервное копирование, архивирование.

2. В случае резервного копирования речь идет о кратко- или среднесрочном дополнительном хранении данных, которые еще могут понадобиться пользователям в их работе. Если, например, в результате повреждения жесткого диска или по иным причинам текущие данные теряются, их удастся быстро восстановить. Так можно эффективно защитить данные от разного рода случайностей. Время хранения резервных копий массива данных устанавливается не слишком продолжительное — несколько недель или месяцев.

Архивированию, напротив, подвергаются данные, которые из категории активно используемых перешли в «статичное» состояние, поэтому к ним обращаются сравнительно редко. Их можно уже извлечь из резервной копии и сохранить в архиве. Оба подхода различаются и уровнем затрат на приобретение необходимых технических средств: для архивирования большого объема данных применяются, как правило, недорогие носители с высокой емкостью хранения, например, оптические носители.

В описанной выше ситуации необходимо осуществлять резервное копирование данных.

6.4. Критерии оценивания

1. Критерии оценки собеседования - зачтено ставится при оценке выше удовлетворительно

Оценка - отлично.
Критерии оценки:
1) обучающийся логично и последовательно излагает материал;
2) обучающийся умеет выявлять и анализировать проблемы и предлагает способы их решения;
3) обучающийся знает основные принципы принятия и реализации решений;
4) содержание выступления подтверждает знание и свободное владение фактическим материалом обучающегося по теме.

Оценка - хорошо.
Критерии оценки:
1) обучающийся испытывает отдельные затруднения в логичности и последовательности изложения материала;
2) обучающийся допускает отдельные неточности и затруднения в выявлении и анализе проблемы;
3) обучающийся допускает незначительные ошибки при определении принципов принятия решений;
4) в содержании выступления присутствуют незначительные неточности при изложении фактического материала.

Оценка - удовлетворительно.
Критерии оценки:
1) обучающийся частично отражает содержание заявленной темы; материал в значительной степени излагается бессистемно и с нарушением логических связей;
2) обучающийся испытывает значительные трудности при анализе фактического материала и формировании решения проблем;
3) обучающийся испытывает затруднения в изложении фактического материала;
4) обучающимся допускаются ошибки в основном содержания понятий.

Оценка - неудовлетворительно.
Критерии оценки:
1) обучающийся не отражает содержание заявленной темы, не владеет фактическим материалом;
2) обучающийся не умеет анализировать и выявлять проблемы в конкретных ситуациях;
3) обучающийся не приводит конкретных примеров, подтверждающих те или иные факты из предметной области вопроса, он не может изложить фактический материал;
4) выступление не отражает основные понятия предмета.

2. Критерии оценки теста - зачтено ставится при оценке выше удовлетворительно

Оценка - отлично. Критерии оценки: набрано 90 баллов и более.

Оценка - хорошо. Критерии оценки: набрано от 75 до 89 баллов.
Оценка - удовлетворительно. Критерии оценки: набрано от 50 до 74 баллов.
Оценка - неудовлетворительно. Критерии оценки: набрано 49 баллов и менее.

3. Критерии оценки ситуационной задачи

Оценка - отлично.
Критерии оценки:
Задание выполнено полностью, обучающийся демонстрирует сформированность как знаний, так и деятельностной составляющей компетенций, сформированы предметные и межпредметные знания и умения, демонстрируются умения применять знания в разных ситуациях.

Оценка - хорошо.
Критерии оценки:
обучающийся четко определяет проблему, пути ее решения, у него частично сформированы предметные и межпредметные знания и умения, частично демонстрируются умения применять знания в разных ситуациях, однако отсутствуют умения аргументировать сделанный выбор, продемонстрировать предлагаемые способы решения проблемы.

Оценка - удовлетворительно.
Критерии оценки:
обучающийся формулирует проблему, содержащуюся в задании, определяет пути ее решения, однако сформированы изолированные знания и умения, отсутствуют умения устанавливать внутри- и межпредметные связи в содержании, нет опыта решения подобных заданий, в результате предложенные варианты решения неверны.

Оценка - неудовлетворительно.
Критерии оценки:
обучающийся не может сформулировать проблему, представленную в задании, не знает способов ее решения, в силу недостаточной теоретической подготовки.

Требования (критериальные показатели) к уровням освоения программы
Критерии оценивания уровня освоения дисциплины (модуля):

Зачтено – обучающийся глубоко и полно владеет содержанием учебного материала; умеет связывать теорию с практикой, решает задачи, теоретические выводы подтверждает примерами, фактами, данными научных исследований; осуществляет межпредметные связи, предложения. Делает выводы логично, четко. Ясно и кратко излагает ответы на поставленные вопросы; умеет обосновывать свои суждения и профессионально-личностную позицию по излагаемому вопросу. Ответ носит самостоятельный характер, но содержание ответа имеет отдельные неточности (несущественные ошибки) в изложении теоретического и практического материала, отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой; допущенные ошибки исправляются студентом после дополнительных вопросов экзаменатора. Допустимо, что обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности и существенные ошибки в определении понятий, формулировке положений, не привлекает для аргументации ответа основные положения исследовательских, концептуальных и нормативных документов, не умеет обосновать свои суждения; наблюдается нарушение логики изложения. Допустимо, что ответ отличается низким уровнем самостоятельности, не содержит собственной профессионально-личностной позиции.

Не зачтено – обучающийся имеет разрозненные, бессистемные знания: не умеет выделять главное и второстепенное; допускает ошибки в определении понятий, формулировке теоретических положений, искажает их смысл; не ориентируется в нормативно-концептуальных, программно-методических, исследовательских материалах, беспорядочно и неуверенно излагает материал; не умеет соединять теоретические положения с практикой; не умеет применять знания для обоснования и объяснения фактов, не устанавливает межпредметные связи.
При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания.

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,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.
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,
- в форме аудиофайла.
Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

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, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);
б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);
в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно на языке Брайля, 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.
Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

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	Прохорова О. В.	Информационная безопасность и защита информации (https://e.lanbook.com/book/169817)	Санкт- Петербург : Лань, 2021	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Исмагилова А. С., Салов И. В., Шагапов И. А., Корнилова А. А.	Информационная безопасность в цифровом обществе: учебное пособие (https://biblioclub.ru/index.php?page=book&id=611084)	Уфа : Башкирский государственный университет, 2019	ЭБС
Л2.2	Арзамаскин Ю. Н., Бирюков А. В., Булва В. И., Зиновьева Е. С., Алборова М. Б.	Международная информационная безопасность: новая геополитическая реальность	Москва : Аспект Пресс, 2021	

7.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л3.1	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие (https://biblioclub.ru/index.php?page=book&id=571485)	Москва, Берлин : Директ-Медиа, 2020	ЭБС
Л3.2	Глинская Е.В., Чичварин Н.В.	Информационная безопасность конструкций ЭВМ и систем: учебное пособие (https://znanium.com/catalog/document?id=362430)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2021	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Лань [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Лань. – URL: http://e.lanbook.com/ информационная безопасность
Э2	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. – URL: http://biblioclub.ru/
Э3	Юрайт [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Юрайт. – URL: https://biblio-online.ru

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

LMS Moodle

Adobe Reader

VirtualBox

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Российское образование [Электронный ресурс] : федеральный портал / ФГАУ ГНИИ ИТТ «Информика». – [Москва, 2002 -]. – Режим доступа : http://www.edu.ru/, свободный (02.09.2018).

2. * Электронная библиотека диссертаций [Электронный ресурс] : официальный сайт / Российская государственная библиотека. – Москва : Рос. гос. б-ка, 2003 - . – Доступ к полным текстам из читальных залов библиотеки ЧелГУ : http://diss.rsl.ru/ (02.09.2018).

3. Электронная библиотека экономической и деловой литературы [Электронный ресурс] : // AUP.Ru : административно-управленческий портал / АУП-Консалтинг. – [Б. м., 1999-]. – Режим доступа : http://www.aup.ru/, свободный (02.09.2018).

4. Дело и сервис [Электронный ресурс] : сайт / Издательская группа «Дело и сервис». – [Б. м., 2000 –]. – Режим доступа: http://www.dis.ru/, свободный (02.09.2018).

5. * eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. – Москва, [1999-]. – Доступ к полным текстам из сети ЧелГУ. – Режим доступа : http://elibrary.ru/defaultx.asp (02.09.2018).

6. Консультант Плюс [Электронный ресурс] : официальный сайт компании Консультант Плюс. – Режим доступа : http://consultant.ru/, свободный (02.09.2018).

7. ГАРАНТ [Электронный ресурс] : информационно-правовой портал [сайт]. – Режим доступа : http://garant.ru/, свободный (02.09.2018).

8. Информационно-правовой консорциум «КОДЕКС». – [Москва, 1991–]. – Режим доступа : http://kodeks.ru/, свободный (02.09.2018.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Стандартные средства обеспечения безопасности операционной системы Windows.

2. - На сайте экономического факультета http://moodle.econ.csu.ru/: контент по дисциплине «Информационная безопасность», в котором организован форум для общения как обучающихся с преподавателем, так и между собой при обсуждении тем курса. Проводятся онлайн занятия.

3. База тестовых вопросов в системе Moodle, структурированная по разделам и уровням сложности на сайте экономического факультета ЧелГУ http:\moodle.econ.cgu.chel.su .Вход по паролям.

В процессе осуществления лекционных и лабораторных занятий возможно использование слайд-презентаций (по некоторым темам), видео-, аудио- материалов (по некоторым темам), компьютерного тестирования, информационных (справочных) систем, подготовка проектов с использованием электронного офиса и др.

Освоение дисциплины осуществляется с использованием средств обучения общего назначения:

- аудитории для проведения лекционных и практических занятий 2-го, 4-го и лабораторного корпусов ЧелГУ с возможностью использования переносного мультимедийного оборудования (экран, ноутбук, проектор, колонки);

- компьютерные классы 2-го, 4-го и лабораторного корпусов ЧелГУ для проведения лабораторных работ и самостоятельной работы обучающихся.

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения:

– лекционная аудитория – мультимедийное оборудование, мобильный радиокласс (для обучающихся с нарушениями слуха); источники питания для индивидуальных технических средств;

– учебная аудитория для самостоятельной работы – стандартные рабочие места с персональными компьютерами; рабочее место с персональным компьютером, с программой экранного доступа, программой экранного увеличения и брайлевским дисплеем для обучающихся с нарушениями зрения.

Для обеспечения тематической иллюстрации занятий лекционного типа в образовательном процессе используются цифровые образовательные ресурсы (мультимедийные презентации), различные формы наглядности (рисунки, таблицы, схемы и т.д.). Для проведения занятий лекционного типа используется переносное и / или стационарное мультимедийное оборудование (экран, ноутбук, проектор, колонки) в аудиториях 2-го, 4-го и лабораторного корпусов ЧелГУ.

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

Обучение по дисциплине «Информационная безопасность» предполагает изучение курса на аудиторных занятиях (лекции, лабораторные занятия) и самостоятельной работы обучающихся. Лабораторные работы предполагают их проведение в компьютерном классе в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:
 знакомит с новым учебным материалом;
 разъясняет учебные элементы, трудные для понимания;
 систематизирует учебный материал;
 ориентирует в учебном процессе.
Подготовка к лекции заключается в следующем:
 внимательно прочитайте материал предыдущей лекции;
 узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
 ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
 постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
 запишите возможные вопросы, которые вы зададите лектору на лекции.
Подготовка к лабораторным работам:
 внимательно прочитайте материал лекций, относящихся к данной лабораторной работе, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
 выпишите основные термины;
 ответьте на контрольные вопросы по занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;
 уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до занятия) во время текущих консультаций преподавателя;
 готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;
 рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.
Подготовка к зачету. К зачету необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:
 программой дисциплины;
 перечнем знаний и умений, которыми обучающийся должен владеть;
 контрольными мероприятиями;

 учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
 перечнем вопросов.

После этого у вас должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

На самостоятельной работе обучающимся прививается практика работы с нормативной, специальной литературой, а также навыки самостоятельного научного поиска и исследовательской работы. Такие занятия помогают осуществлять обратную связь и оказать практическую помощь обучающимся при подготовке к лабораторным занятиям, написанию контрольных, курсовых и других видов научных работ.

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.

38.05.01, Экономико-правовое обеспечение экономической безопасности, Экономическая безопасность, Информационная безопасность, 2025, заочная

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом факультета экономики и управления

Протокол заседания № 1 от 11.02.2025

Председатель Ученого совета факультета экономики и управления согласовано А. А. Егорова

Заседанием кафедры прикладной экономики и маркетинга

Протокол заседания № 5 от 04.02.2025

Заведующий кафедрой согласовано С. А. Головихин

Автор (составитель) О.Л. Голубева

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