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

Форма обучения

очная

Год(ы) набора 2026

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

Миасс 2026 г.

38.05.01 Экономико-правовое обеспечение экономической безопасности, специальность "Экономическая безопасность", рабочая программа дисциплины "Информационная безопасность", год набора - 2026, очная форма обучения:

Утверждена:
Проректор по учебной работе утверждено 25.02.26 А.А. Саламатов

Согласована:
Ученым советом Миасского филиала ФГБОУ ВО "ЧелГУ"

Протокол заседания № 8 от 24.02.2026

Председатель Ученого совета
Миасского филиала ФГБОУ ВО
"ЧелГУ" согласовано Т. В. Малькова

Заседанием кафедры прикладной математики

Протокол заседания № 6 от 30.01.2026

Заведующий кафедрой согласовано Е.В. Дутикова

Автор (составитель) Е.В. Дутикова

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

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели изучения 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.

Основные задачи изучения дисциплины:

- познакомить обучающихся с определением, классификацией и характеристиками информационной безопасности; с организационными и экономическими аспектами работы с информационными ресурсами и методами оценки эффективности их безопасности;

- дать представление об особенностях информационной безопасности, сегментах и участниках информационного рынка, особенностях формирования безопасности информации;

- рассмотреть основные технологические принципы безопасности мировых информационных ресурсов на основе глобальной сети INTERNET.

Изучение дисциплины направлено на достижение индикаторов:

ОПК-6.1. Знает основные программные средства и сферу их применения в области профессиональных задач

ОПК-6.2. Владеет основными информационными технологиями для решения профессиональных задач

ОПК-6.3. Применяет современные информационные технологии и программные средства для решения профессиональных задач

ОПК-7.1. Знает принципы работы современных информационных технологий

ОПК-7.2. Понимает принципы работы современных информационных технологий

ОПК-7.3. Использует принципы работы современных информационных технологий для решения задач профессиональной деятельности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.07

2.1 Требования к предварительной подготовке обучающегося:

Современные технологии поиска и обработки информации

Информационные технологии

Математика

Делопроизводство и режим секретности

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

Экономическая безопасность

Экономическая безопасность в системе национальной безопасности

Экономическая безопасность интернет-предпринимательства

Подготовка к процедуре защиты и защита выпускной квалификационной работы

Производственная практика (практика по профилю профессиональной деятельности)

Производственная практика (преддипломная практика)

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

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

Знать:

организационно-правовое обеспечение информационной безопасности;

Уметь:

применять методы защиты информации для решения задач обеспечения информационной безопасности,

анализировать риски политики информационной безопасности;

Владеть:

навыками применения различных методов защиты информации, работы с сертификатами, подписи документов и защиты почты, средствами защиты от несанкционированного доступа;

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

Знать:

основные понятия и определения информационной безопасности, основы криптографии, основные методы и приемы защиты от несанкционированного доступа

Уметь:

зашифровывать и дешифровывать сообщения различными способами, составлять матрицу доступа к информационным ресурсам, использовать криптографические методы

Владеть:

навыками настройки подсистемы защиты информации ОС Windows, MS Office, Internet Explorer, оценки уровня конфиденциальности и расчета затрат на обеспечение защиты информации.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	организационно-правовое обеспечение информационной безопасности;
3.1.2	основные понятия и определения информационной безопасности, основы криптографии, основные методы и приемы защиты от несанкционированного доступа
3.2	**Уметь:**
3.2.1	применять методы защиты информации для решения задач обеспечения информационной безопасности, анализировать риски политики информационной безопасности;
3.2.2	зашифровывать и дешифровывать сообщения различными способами, составлять матрицу доступа к информационным ресурсам, использовать криптографические методы
3.3	**Владеть:**
3.3.1	навыками применения различных методов защиты информации, работы с сертификатами, подписи документов и защиты почты, средствами защиты от несанкционированного доступа;
3.3.2	навыками настройки подсистемы защиты информации ОС Windows, MS Office, Internet Explorer, оценки уровня конфиденциальности и расчета затрат на обеспечение защиты информации.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость			**4 ЗЕТ**
Часов по учебному плану	:	144	Виды контроля в семестрах:
в том числе	:		
аудиторные занятия	:	50	экзамены 2
самостоятельная работа	:	63,7	
часов на контроль	:	27	
контактная работа: 53,3			
ИКР: 3,3			

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код заняти	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Основные понятия и определения информационной безопасности. Законодательный уровень информационной безопасности. Правовая защита информации.			
1.1	Основные понятия и определения информационной безопасности. Законодательный уровень информационной безопасности. Правовая защита информации. /Лек/	2	2	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2

1.2	Законодательный уровень информационной безопасности. Правовая защита информации. /Пр/	2	4	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
1.3	Основные понятия и определения информационной безопасности. Законодательный уровень информационной безопасности. Правовая защита информации. /Ср/	2	15	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
	Раздел 2. Угрозы информационной безопасности.			
2.1	Угрозы информационной безопасности. /Лек/	2	2	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
2.2	Мониторинг факторов, вызывающих угрозы экономической безопасности предприятия с использованием приложения MS Exel. /Пр/	2	6	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
2.3	Угрозы информационной безопасности. /Ср/	2	10	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
	Раздел 3. Политика безопасности в компьютерных системах.			
3.1	Политика безопасности в компьютерных системах. /Лек/	2	2	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
3.2	Политика безопасности. Матрица доступа к информационным ресурсам /Пр/	2	4	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
3.3	Анализ рисков политики информационной безопасности на предприятии методом экспертных оценок. /Пр/	2	4	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
3.4	Оценка уровня конфиденциальности и расчет затрат на обеспечение защиты информации на предприятии. /Пр/	2	4	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
3.5	Политика безопасности в компьютерных системах. /Ср/	2	10	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
	Раздел 4. Уровни информационной безопасности			
4.1	Административный уровень информационной безопасности. Процедурный уровень информационной безопасности. Программно-технический уровень информационной безопасности. /Лек/	2	6	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
4.2	Уровни информационной безопасности /Ср/	2	7	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
	Раздел 5. Криптографические методы защиты информации.			
5.1	Криптографические методы защиты информации. /Лек/	2	2	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
5.2	Криптографические средства защиты информации. Шифры замены. Шифры перестановки /Пр/	2	4	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
5.3	Обеспечение информационной безопасности при работе с приложениями Microsoft Office. Шифрованная файловая система Windows /Пр/	2	2	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
5.4	Работа с криптопровайдерами. /Пр/	2	2	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2

5.5	Криптографические методы защиты информации. /Ср/	2	11,7	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
	Раздел 6. Вредоносные программы. Межсетевое экранирование. Виртуальные частные сети.			
6.1	Вредоносные программы. Межсетевое экранирование. Виртуальные частные сети. /Лек/	2	2	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
6.2	Профилактика заражения вирусами компьютерных систем. /Пр/	2	4	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
6.3	Вредоносные программы. Межсетевое экранирование. Виртуальные частные сети. /Ср/	2	10	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2
	Раздел 7. Иная контактная работа			
7.1	Индивидуальные консультации, текущий контроль /ИКР/	2	3,3	Л1.1 Л1.2 Л1.3Л2.1

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Тестирование
Собеседование
Практические работы
Экзамен

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Практические работы:
- “Законодательный уровень информационной безопасности”.
- “Политика безопасности. Матрица доступа к информационным ресурсам”.
- “Профилактика заражения вирусами компьютерных систем”.
- “Криптографические средства защиты информации. Шифры замены. Шифры перестановки”.
- “Обеспечение информационной безопасности при работе с приложениями Microsoft Office”.
- “Шифрованная файловая система Windows”.
- “Работа с криптопровайдерами”
- "Мониторинг факторов, вызывающих угрозы экономической безопасности предприятия с использованием приложения MS Exel".
- "Анализ рисков политики информационной безопасности на предприятии методом экспертных оценок".
- "Оценка уровня конфиденциальности и расчет затрат на обеспечение защиты информации на предприятии".

Пример вопросов для собеседования
Опрос № 1.
1) Защищаемая информация и Информационная безопасность.
2) Классификация информационных ресурсов.
3) Основные составляющие информационной безопасности.
4) Направления защиты информации.
5) Правовая защита информации.
6) Техническая защита информации.
7) Криптографическая защита информации.
8) Физическая защита информации.

Опрос № 2.
1) Угроза информации.
2) Классификация угроз безопасности. Основные виды угроз безопасности.
3) Угроза конфиденциальности.
4) Угроза целостности.
5) Угроза доступности.
6) Уязвимость компьютерной системы.

7) Атака на компьютерную систему.
8) Взаимосвязь основных субъектов и объектов обеспечения безопасности, как это предлагается в международном стандарте ISO/IEC-15408.

Опрос № 3
1) Политика безопасности.
2) Что составляет основу политики безопасности.
3) Понятие конфиденциальной информации.
4) Что понимается под доступом к информации. Санкционированный и не санкционированный доступ к информации.
5) Организация доступа к ресурсам предполагает...
6) Избирательная политика безопасности. Матрица доступа к информационным ресурсам.
7) Полномочное управление доступом. Модель Белла-Лападула.
8) Механизмы аутентификации.

Опрос № 4
1) Административный уровень информационной безопасности.
2) Главная цель мер административного уровня.
3) Административные меры включают в себя...
4) Три уровня политики безопасности.
5) Программа безопасности.
6) Синхронизации программы безопасности с жизненным циклом систем.
7) Понятие об управлении рисками.
8) Этапы процесса управления рисками.

Опрос № 5
1) Процедурный уровень информационной безопасности.
2) Основные классы мер процедурного уровня безопасности.
3) Управление персоналом. Общие принципы.
4) Физическая защита.
5) Направления деятельности направленных на поддержание работоспособности.
6) Реагирования на нарушения программы безопасности. Главные цели.
7) Процесс планирование восстановительных работ, основные этапы.

Опрос № 6
1) Программно-технические меры информационной безопасности.
2) Основные сервисы обеспечения безопасности.
3) Классификация сервисов безопасности.
4) Особенности современных информационных систем.
5) Архитектура системы безопасности.
6) Стандарты повышения надежности информационных систем.

Опрос № 7
1) Шифрование информации.
2) Шифротекст, Криптопргорамма, Шифр.
3) Основные виды шифров.
4) Криптография. Обобщенная схема криптографической системы.
5) Основные классы криптосистем.
6) Методы шифрации. Симметричные и ассиметричные криптосистемы.
7) Криптоанализ. Фундаментальное правило криптоанализа.
8) Электронный документ. Электронная подпись. Классификация электронных подписей.
9) Хэширование.
10) Основные группы аппаратно - программных криптографических средств защиты информации.

Опрос № 8
1) Вредоносная программа.
2) Назвать критерии, по которым программные продукты (модули) могут быть отнесены к категории вредоносных программ.
3) Способы распространения вредоносных программ.
4) Классификация вредоносных программ.

5) Последствия заражения вредоносной программой.
6) Антивирусное программное обеспечение.

Опрос № 9
1) Межсетевой экран или брандмауэр.
2) Основные задачи и функции сетевого экрана.
3) Концепцию межсетевого экранирования.
4) Классификация межсетевых экранов.
5) Виртуальные частные сети.
6) Технология виртуальных частных сетей.
7) Особенности использования VPN.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Экзамен в форме тестирования.

1. Вставьте пропущенное слово.
«Под информационной безопасностью будем понимать защищенность информации и …….. от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры»
а) поддерживающей инфраструктуры
б) человека
в) конфиденциальных данных

2. Защита информации – это …
а) комплекс мероприятий, направленных на обеспечение информационной безопасности
б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов
в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям
г) все определения корректны

3. Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:
а) обнаружение угроз
б) пресечения и локализация угроз
в) ликвидация угроз

4. Возможность за приемлемое время получить требуемую информационную услугу называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации

5. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации
г) конфиденциальностью информации

6. Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации
а) доступность информации
б) целостность информации
в) предоставление информации
г) конфиденциальность информации

7. Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:

а) законодательного уровня
б) административного уровня
в) процедурного уровня
г) программно-технического уровня
д) программно-аппаратного уровня

8. Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:
а) Федеральная служба по техническому и экспортному контролю при Президенте РФ
б) Федеральная служба безопасности Российской Федерации
в) Служба внешней разведки Российской Федерации

9. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:
а) политикой безопасности
б) методами защиты информации
в) ограничением доступа к информации
учетными записями пользователей

10. Потенциальная возможность определенным образом нарушить информационную безопасность – это ….
а) угроза
б) атака
в) взлом

11. Источниками угрозы называют …
а) потенциальных злоумышленников
б) компьютерные вирусы
в) глобальную сеть Интернет

12. Ошибки программного обеспечения с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы

13. Ошибки администрирования системы с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы

14. Ошибка в программе, вызвавшая крах системы с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы

15. Некоторая уникальная информация, позволяющая различать пользователей называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ

16. Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ

17. Совокупность идентификатора и пароля пользователя называется:
а) логин пользователя
б) учетная запись пользователя
в) ключ пользователя

18. Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) опознанием пользователя
г) созданием учетной записи пользователя

19. Проверка принадлежности пользователю предъявленного им идентификатора является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) регистрацией пользователя
г) созданием учетной записи пользователя

20. Факт получения охраняемых сведений злоумышленниками или конкурентами называется:
а) утечкой
б) разглашением
в) взломом

21. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называется:
а) утечкой
б) разглашением
в) взломом

22. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена, называется:
а) утечкой
б) разглашением
в) взломом

23. Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) перехват передаваемой по сети информации (Sniffing)
д) спуфинг
е) сканирование портов

24. Атака, целью которой является трафик локальной сети, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

25. Атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг

е) сканирование портов

26. Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

27. К внутренним нарушителям информационной безопасности относятся:
а) сотрудники отделов разработки и сопровождения ПО данного предприятия
б) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации
в) посетители
г) руководители предприятия различных уровней
д) клиенты

28. Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях) относится к …
а) активным угрозам
б) непреднамеренным искусственным угрозам
в) преднамеренным искусственным угрозам
г) естественным угрозам

29. Естественные угрозы безопасности информации вызваны:
а) ошибками при действиях персонала
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
в) воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека
г) корыстными устремлениями злоумышленников

30. Целостность - это …
а) защита от несанкционированного доступа к информации, свойство информации быть известной и доступной, только прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам)
б) актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
в) возможность за приемлемое время получить требуемую информационную услугу

31. Потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации:
а) атака
б) угроза
в) уязвимость

32. Собственник как субъект доступа к информации - это:
а) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов
б) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами
в) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации

33. Что такое вредоносная программа?
а) программы, наносящие вред человеку
б) программы, наносящие вред данным, хранящимся на компьютере
в) программы, наносящие вред данным и программам, хранящимся на компьютере
г) все вышеперечисленное

34. Основными типами вредоносных программ являются:
а) вирусы, черви, троянские и хакерские программы
б) шпионское, рекламное программное обеспечение
в) потенциально опасное программное обеспечение
г) все вышеперечисленное

6.4. Критерии оценивания

Критерии оценивания тестирования

Отметка «отлично» ставится в том случае, если набранная сумма баллов (% выполненных заданий) (мах – 100) 96-100
Отметка «хорошо» – если 76-95 баллов.
Отметка «удовлетворительно» – если 60-75 баллов.
Отметка «неудовлетворительно» – если менее 60 баллов

Критерии оценивания собеседования:
Отметка «отлично» ставится в том случае, если:
В ответе качественно раскрыто содержание темы. Ответ хорошо структурирован. Прекрасно освоен понятийный аппарат. Продемонстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать дискуссионные положения.
Отметка «хорошо» ставится в том случае, если:
Основные вопросы темы раскрыты. Структура ответа в целом адекватна теме. Хорошо освоен понятийный аппарат. Продемонстрирован хороший уровень понимания материала. Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.
Отметка «удовлетворительно» ставится в том случае, если:
Тема частично раскрыта. Ответ слабо структурирован. Понятийный аппарат освоен частично. Понимание отдельных положений из материала по теме. Удовлетворительное умение формулировать свои мысли, обсуждать дискуссионные положения.
Отметка «неудовлетворительно» ставится в том случае, если:
Тема не раскрыта. Понятийный аппарат освоен неудовлетворительно. Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.

Критерии оценивания практической работы
Оценка «зачтено» ставится, если:
1) Контрольная работа представлена в установленный срок и оформлена в соответствии с установленными требованиями.
2) Работа написана самостоятельно и в ней в полной мере раскрыты вопросы контрольных заданий.
3) В освещении вопросов заданий не содержится грубых ошибок.
4) При решений заданий сделаны правильные и аргументированные выводы.
Оценка «не зачтено» ставится, если:
1) Студент не справился с заданиями.
2) В работе не раскрыто основное содержание вопросов, имеются грубые ошибки.
3) Имеются явные признаки плагиата.
4) Оформление работы не соответствует требованиям.
Работа, по результатам проверки которой выставлена оценка «не зачтено», возвращается студенту на доработку. Студент не может быть допущен до сдачи экзамена до тех пор, пока не представит исправленную работу.

Критерии оценивания экзамена
На экзамене студенту будет предложен билет, состоящий из 3-х вопросов по разным разделам курса, при ответе на которые экзаменуемый должен продемонстрировать знание теоретических понятий темы вопроса и проиллюстрировать их разбором практического примера. Возможные оценки:
«отлично» (5) – владеет в полной мере;
«хорошо» (4) – владеет достаточно;
«удовлетворительно» (3) – владеет недостаточно;
«неудовлетворительно» (2) – не владеет.
«Отлично» («5») – студент глубоко и полно владеет содержанием учебного материала и понятийным аппаратом; умеет связывать теорию с практикой, иллюстрировать примерами, фактами, данными научных исследований; обозначает межпредметные связи. 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.

«Хорошо» («4») – ответ студента соответствует указанным выше критериям, но содержание ответа имеет отдельные неточности (несущественные ошибки) в изложении теоретического и практического материала, отличается меньшей обстоятельностью, глубиной и полнотой; допущенные ошибки исправляются студентом после дополнительных вопросов экзаменатора.
«Удовлетворительно» («3») – студент 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. Ответ отличается низким уровнем самостоятельности, не содержит собственной профессионально-личностной позиции.
«Неудовлетворительно» («2») – студент имеет разрозненные, бессистемные знания: не умеет выделять главное и второстепенное; допускает ошибки в определении понятий, формулировке теоретических положений, искажающие их смысл; не ориентируется в нормативно-концептуальных, программно-методических, исследовательских материалах, беспорядочно и неуверенно излагает материал; не умеет соединять теоретические положения с педагогической практикой; не умеет применять знания для обоснования и объяснения фактов.

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

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Ресурс
Л1.1	Прохорова О. В.	Информационная безопасность и защита информации: учебник для вузов (https://e.lanbook.com/book/462293)	Санкт-Петербург : Лань, 2025	ЭБС
Л1.2	Баланов А. Н.	Комплексная информационная безопасность: учебное пособие для вузов (https://e.lanbook.com/book/460715)	Санкт-Петербург : Лань, 2025	ЭБС
Л1.3	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: учебное пособие (https://znanium.ru/catalog/document?id=465001)	Москва : Издательский Центр РИОР, 2025	ЭБС

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Ресурс
Л2.1	Баланов А.Н.	Комплексная информационная безопасность: полный справочник специалиста: практическое пособие (https://znanium.ru/catalog/document?id=451735)	Вологда : Инфра-Инженерия, 2024	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. – URL: http://biblioclub.ru/. http://biblioclub.ru
Э2	Юрайт [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Юрайт. – URL: https:/uraite.ru https://urait.ru/

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Reader

LMS Moodle

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Справочно-правовая система «КонсультантПлюс» (http://www.consultant.ru/) КонсультантПлюс : справочно-правовая система : база данных / Региональный центр правовой информации Информправо. – Москва, 1992 – . – Режим доступа: из читальных залов библиотеки. – Текст : электронный.

2. Научная электронная библиотека eLIBRARY.RU (https://elibrary.ru/defaultx.asp?) eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского и лабораторного 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.

Учебный кабинет для занятий лекционного и семинарского типа, расположенный по адресу:

456313, Россия, Челябинская обл., г. Миасс, ул. Керченская, д. 1

Номер аудитории в соответствии с документами бюро технической инвентаризации: литер А2, 3 этаж, № 6, аудитория № 305 на 34 посадочных места

Доска ученическая обычная, настенная - 1 шт.,

стол преподавателя - 1 шт., стул - 1 шт.,

учебные парты (стол, совмещенный со скамейкой) 2-х местных - 17,

компьютер AMD,

проектор BENQ MP720,

экран настенный,

колонки MicroLab

Учебный кабинет (компьютерный зал) для занятий семинарского типа, расположенный по адресу:

456313, Россия, Челябинская обл., г. Миасс, ул. Керченская, д. 1

Номер аудитории в соответствии с документами бюро технической инвентаризации: литер А2, 3 этаж, № 9, аудитория № 309 на 20 посадочных мест

Компьютерные столы -20 шт.,

компьютер 20 шт. Intel Pentium,

видеопроектор Epson EMP-1710,

экран настенный,

принтер Canon Laser Shot LBP1120

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

Для проведения занятий предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий: презентации по темам лекций и практических занятий, видеоматериалы, материалы для тестирования.

Необходимое оборудование при реализации дисциплины с использованием ЭО и ДОТ (компьютер, колонки, микрофон, камера).

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

Обучение по дисциплине «Информационная безопасность» предполагает изучение курса на аудиторных занятиях (лекции и семинарские занятия) и самостоятельной работы студентов. Семинарские занятия дисциплины «Информационная безопасность» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения студент 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 семинарским и практическим занятиям:

- внимательно прочитайте материал лекций относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
- выпишите основные термины;

- ответьте на контрольные вопросы по семинарским 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 семинарского 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 экзамену. К экзамену 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 студент должен владеть;
- контрольными мероприятиями;
- учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету, экзамену.

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 семинарских занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

На самостоятельной работе студентам 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 по-мощь студентам при подготовке к семинарским занятиям, написанию контрольных, курсовых и других видов научных работ.

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, MS Office365, 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, 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.