Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю)

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

Троицк, 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки: *02.03.02 Фундаментальная информатика и информационные технологии*
Направленность (профиль) Математические и алгоритмические основы интеллектуальных систем
Дисциплина: *Информационная безопасность и защита информации*
Семестр (семестры) изучения: *6 семестр.*
Форма (формы) промежуточной аттестации: *зачет - 6 семестр.*
Примечание: для оценивания результатов обучения используется балльно-рейтинговая система.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины *Информационная безопасность и защита информации* направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
1	2	3	4
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	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	**Знать:** основы информационной безопасности и защиты информации в сфере управления проектами. **Уметь:** выявлять и анализировать различные способы решения задач информационной безопасности и защиты информации в рамках цели проекта и обосновывать их выбор. **Владеть:** навыками обеспечения информационной безопасности при решении задач проекта, выбирая оптимальный способ защиты информации, исходя из действующих правовых норм и имеющихся ресурсов.

		ограничений.	
УК-10	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	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.	**Знать:** методы информационной безопасности в сфере противодействия экстремизму и терроризму **Уметь:** противодействовать экстремизму и терроризму в информационной среде **Владеть:** навыками защиты информации от проявлений экстремизма и терроризма
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	ПК-3.1. Обладает знаниями о методах и средствах проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов. ПК-3.2. Демонстрирует умения: разрабатывать требования к программному продукту, применять методы и средства проектирования программного обеспечения, структур	**Знать:** методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов с учетом информационной безопасности и защиты информации. **Уметь:** разрабатывать требования информационной безопасности к программному продукту, применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов с защитой информации **Владеть:**

		данных, баз данных, программных интерфейсов. ПК-3.3. Имеет практический опыт (навыки): проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.	практическим опытом (навыками): обеспечения информационной безопасности при проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Код компетенции/ планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1	УК-2	Правовая основа информационной безопасности информационных систем.	Тестирование, устный опрос	Теоретические вопросы к зачету №1-3, Задания теста №1
2	УК-2	Технологические основы информационной безопасности. Основные понятия и определения.	Тестирование, устный опрос	Теоретические вопросы к зачету №4-7, Задания теста №2
3	УК-2	Общеметодологические принципы теории информационной безопасности.	Тестирование, устный опрос	Теоретические вопросы к экзамену №8-10, Задания теста №3-4
4	УК-2, УК-10, ПК-3	Классификация и анализ угроз информационной безопасности.	Тестирование, устный опрос	Теоретические вопросы к зачету №11-13, Задания теста № 5
5	УК-2, УК-10, ПК-3	Причины, виды, каналы утечки и искажения информации.	Тестирование, устный опрос	Теоретические вопросы к зачету №14-17, Задания теста №6
6	УК-2	Функции и задачи защиты информации.	Тестирование, устный опрос	Теоретические вопросы к зачету №18-20, Задания теста №7
7	УК-2	Криптографические методы защиты информации.	Тестирование, устный опрос	Теоретические вопросы к зачету №21-24,

				Задания теста №8
8	УК-2, УК-10, ПК-3	Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей.	Тестирование, устный опрос	Теоретические вопросы к зачету №25-27, Задания теста №9
9	УК-2	Архитектура и методы организации систем защиты информации.	Тестирование, устный опрос	Теоретические вопросы к зачету №28-29, Задания теста №10

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

3.2 Порядок проведения промежуточной аттестации и содержание оценочных средств

Оценочные средства для промежуточной аттестации представлены базой контрольных вопросов и задач к зачету.

3.2.1. База контрольных вопросов к зачету

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.

3.2.2. Пример зачетного теста

Полный набор тестовых заданий различных типов (выбор вариантов ответов, ввод правильного ответа, установка соответствия, классификация) подготовлен в тестовой системе Айрен.

№ п/п	Формулировка вопроса	Варианты ответов
1	Сведения, воспринимаемые человеком или	А) потоки;

	специальными устройствами как отражение фактов материального мира в процессе коммуникации - это	Б) процессы; В) функции; Г) информация; Д) задания.
2	Одним из ключевых законов о защите информации является …	А) закон о «Защите универсальных данных»; Б) закон о «Защите персональных данных»; В) закон о «Защите животных»; Г) закон о «Защите прав потребителей».
3	К формам защиты информации не относится…	А) аналитическая; Б) правовая; В) организационно-техническая; Г) страховая.
4	Информация, составляющая государственную тайну не может иметь гриф…	А) «для служебного пользования»; Б) «секретно»; В) «совершенно секретно»; Г) «особой важности».
5	Какие из технических каналов утечки информации относятся к речевой информации?	А) Электромагнитные; Б) Вибрационные; В) Оптико-электронный; Г) Электрический.
6	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.
7	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.
8	Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ):	А) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивно-

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

4. КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Промежуточная аттестация в 6 семестре проводится письменно в форме зачета. Студенту выдается один теоретический вопрос и одна задача. Время выполнения – до 45 минут.

При дистанционном обучении устный опрос, в том числе защита курсовых работ, реализуется в Microsoft Teams, практические задания и

письменные ответы размещаются в Moodle, ответы должны сданы также в Moodle, тестирование осуществляется также в Moodle.

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

4.2.1. Критерии оценивания на зачете.

Оценка качества подготовки студентов должна включать текущую и промежуточную оценку. Текущий контроль представляет собой проверку усвоения учебного материала, регулярно осуществляемую на протяжении семестра.

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.

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

4.3.Результаты промежуточной аттестации и уровни сформированности компетенций

Код компетенции	Планируемые результаты обучения по дисциплине	Критерии оценивания	
		Зачтено	Не зачтено
УК-2	**Знает:** основы информационной безопасности и защиты информации в сфере управления проектами. **Умеет:** выявлять и анализировать различные способы решения задач информационной безопасности и защиты информации в рамках цели проекта и обосновывать их выбор. **Владеет:** навыками обеспечения информационной безопасности при решении задач проекта, выбирая оптимальный способ защиты информации, исходя из действующих правовых норм и имеющихся ресурсов.	**Знает:** основы информационной безопасности и защиты информации в сфере управления проектами. **Умеет:** выявлять и анализировать различные способы решения задач информационной безопасности и защиты информации в рамках цели проекта и обосновывать их выбор. **Владеет:** навыками обеспечения информационной безопасности при решении задач проекта, выбирая оптимальный способ защиты информации, исходя из действующих правовых норм и имеющихся ресурсов.	**Не знает:** основы информационной безопасности и защиты информации в сфере управления проектами. **Не умеет:** выявлять и анализировать различные способы решения задач информационной безопасности и защиты информации в рамках цели проекта и обосновывать их выбор. **Не владеет:** навыками обеспечения информационной безопасности при решении задач проекта, выбирая оптимальный способ защиты информации, исходя из действующих правовых норм и имеющихся ресурсов.
УК-10	**Знает:** методы информационной безопасности в сфере противодействия экстремизму и терроризму **Умеет:** противодействовать экстремизму и терроризму в информационной среде **Владеет:** навыками защиты информации от проявлений экстремизма и терроризма	**Знает:** методы информационной безопасности в сфере противодействия экстремизму и терроризму **Умеет:** противодействовать экстремизму и терроризму в информационной среде **Владеет:** навыками защиты информации от проявлений экстремизма и терроризма	**Не знает:** методы информационной безопасности в сфере противодействия экстремизму и терроризму **Не умеет:** противодействовать экстремизму и терроризму в информационной среде **Не владеет:** навыками защиты информации от проявлений экстремизма и терроризма
ПК-3	**Знает:** методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов с учетом информационной безопасности и защиты информации. **Умеет:** разрабатывать требования информационной безопасности к программному продукту, применять методы и средства проектирования программного обеспечения, структур данных,	**Знает:** методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов с учетом информационной безопасности и защиты информации. **Умеет:** разрабатывать требования информационной безопасности к программному продукту, применять методы и средства проектирования	**Не знает:** методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов с учетом информационной безопасности и защиты информации. **Не умеет:** разрабатывать требования информационной безопасности к программному продукту, применять методы и средства проектирования

	баз данных, программных интерфейсов с защитой информации **Владеет:** практическим опытом (навыками): обеспечения информационной безопасности при проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.	программного обеспечения, структур данных, баз данных, программных интерфейсов с защитой информации **Владеет:** практическим опытом (навыками): обеспечения информационной безопасности при проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.	программного обеспечения, структур данных, баз данных, программных интерфейсов с защитой информации **Не владеет:** практическим опытом (навыками): обеспечения информационной безопасности при проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

02.03.02 Фундаментальная информатика и информационные технологии,

Математические и алгоритмические основы интеллектуальных систем, Информационная безопасность и защита информации, 2025 год набора, очная

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

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