Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таскаев Сергей Валерьевич
Должность: Ректор
Дата подписания: 02.10.2026 10:04:43
Уникальный программный ключ:
04c19ed8bfb98f3b6cb77a486b9a8788b8322525



# Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю)

Информационная безопасность

Направление подготовки (специальность)
38.05.01 Экономическая безопасность

Направленность (профиль)
Экономико-правовое обеспечение экономической безопасности

Присваиваемая квалификация (степень)
экономист (специалист)

Форма обучения
очная

Год(ы) набора 2025

Челябинск 2025 г.

© ФГБОУ ВО «ЧелГУ»

**Содержание**

1. Паспорт фонда оценочных средств
2. Перечень формируемых компетенций
2.1. Компетенции, закреплённые за дисциплиной
3. Содержание оценочных средств по дисциплине
3.1. Виды оценочных средств
3.2. Содержание оценочных средств
4. Порядок проведения и критерии оценивания промежуточной аттестации
4.1. Порядок проведения промежуточной аттестации
4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств
4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

© ФГБОУ ВО «ЧелГУ»

# 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки: **38.05.01 Экономическая безопасности**
Направленность (профиль) **Экономико-правовое обеспечение экономической безопасности**
Дисциплина: **Информационная безопасность**
Семестр изучения: **3**
Форма (формы) промежуточной аттестации: **зачет**

# 2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

## 2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Информационная безопасность» 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 | | 4 |
| ОПК-6 | Способен использовать современные информационные технологии и программные средства при решении профессиональных задач | **ОПК-6.1.** Знает основные программные средства и сферу их применения в области профессиональных задач<br>**ОПК-6.2.** Владеет основными информационными технологиями для решения профессиональных задач<br>**ОПК-6.3.** Применяет современные информационные технологии и программные средства для решения профессиональных задач | **Знать** основные программные средства и сферу их применения в области профессиональных задач<br>**Уметь** применять современные информационные технологии и программные средства для решения профессиональных задач<br>**Владеть** основными информационными технологиями для решения профессиональных задач |
| ОПК-7 | Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности | **ОПК-7.1.** Знает принципы работы современных информационных технологий<br>**ОПК-7.2.** Понимает принципы работы современных информационных технологий<br>**ОПК-7.3.** Использует | **Знать** принципы работы современных информационных технологий<br>**Уметь** применять принципы работы современных информационных технологий<br>**Владеть** принципами работы современных информационных технологий для решения задач профессиональной деятельности |

© ФГБОУ ВО «ЧелГУ»

| | | | |
|---|---|---|---|
| | | принципы работы современных информационных технологий для решения задач профессиональной деятельности | |

# 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 | **ОПК-6**<br>Знать основные программные средства и сферу их применения в области профессиональных задач<br>Уметь применять современные информационные технологии и программные средства для решения профессиональных задач<br>Владеть основными информационными технологиями для решения профессиональных задач | Информационная безопасность в системе национальной безопасности Российской Федерации | Лабораторные работы | Тестовые вопросы №1-4<br>Вопросы №1-2 |
| | | Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности | Лабораторные работы | Тестовые вопросы №5-7<br>Вопросы №3-6 |
| | | Методы и средства обеспечения информационной безопасности. Защита информации криптографическими методами | Лабораторные работы | Тестовые вопросы №8-11<br>Вопросы №7-15 |
| 2 | **ОПК-7**<br>Знать принципы работы современных информационных технологий<br>Уметь применять принципы работы современных информационных технологий<br>Владеть принципами работы современных информационных технологий для решения задач профессиональной деятельности | Основы комплексного обеспечения информационной безопасности. Модели, стратегии (политики) и системы обеспечения информационной безопасности | Лабораторные работы | Тестовые вопросы №12-14<br>Вопросы №16-22 |
| | | Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей | Лабораторные работы | Тестовые вопросы №15-16<br>Вопросы №23-28 |

© ФГБОУ ВО «ЧелГУ»

| | | | | |
|---|---|---|---|---|
| | | Методология построения и анализа систем обеспечения информационной безопасности | Лабораторные работы | Тестовые вопросы №17-18<br>Вопросы №29-31 |

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 Содержание оценочных средств

**1. База тестовых вопросов для зачета**

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?

© ФГБОУ ВО «ЧелГУ»

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?

© ФГБОУ ВО «ЧелГУ»

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

© ФГБОУ ВО «ЧелГУ»

**2. База практических вопросов для зачета:**

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

Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

## 4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

© ФГБОУ ВО «ЧелГУ»

## 4.1. Порядок проведения промежуточной аттестации

На **зачете** обучающимся предлагается 15 тестовых вопросов из разных тем и 2 задания по вариантам. Продолжительность – 90 минут.

## 4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

### 4.2.1 Критерии оценивания тестовых вопросов

Максимальный балл за ответы на тест — 20 баллов.

| | | |
|---|---|---|
| **Зачтено/ 17-20 баллов** | Высокий уровень освоения проверяемых компетенций | Абсолютное большинство ответов верные. Обучающийся глубоко понимает особенности работы современных информационных технологий. |
| **Зачтено/ 12-16 баллов** | Средний уровень освоения проверяемых компетенций | Большая часть ответов верные. Обучающийся понимает работы современных информационных технологий на среднем уровне. |
| **Зачтено/ 8-11 баллов** | Базовый уровень уровень освоения проверяемых компетенций | Многие ответы содержат неточности. Обучающийся понимает работы современных информационных технологий на базовом уровне. |
| **Не зачтено/ 0-7 балла** | Недостаточный уровень освоения проверяемых компетенций | Абсолютное большинство ответов неверные. Обучающийся недостаточно понимает особенности теоретических моделей рассуждений, поведения, обучения на базовом уровне. |

### 4.2.2. Критерии оценивания задания для зачета

Максимальный балл за задание — 20 баллов.

| | | |
|---|---|---|
| **Зачтено/ 17-20 баллов** | Высокий уровень освоения проверяемых компетенций | Задание выполнено полностью. Обучающийся глубоко понимает принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности. |
| **Зачтено/ 12-16 баллов** | Средний уровень освоения проверяемых компетенций | Задание выполнено на достаточном уровне, обучающийся понимает принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности на среднем уровне. |
| **Зачтено/** | Базовый уровень | Обучающийся способен выполнить задачу |

© ФГБОУ ВО «ЧелГУ»

| | | |
|---|---|---|
| **8-11 баллов** | уровень освоения проверяемых компетенций | только на базовом уровне, решение задач содержит существенные ошибки. Обучающийся понимает принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности на базовом уровне. |
| **Не зачтено/ 0-7 балла** | Недостаточный уровень освоения проверяемых компетенций | Обучающийся не способен решить задачу. |

## 4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:

0-49 баллов - не зачтено;
50-100 - зачтено.

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

Уровни сформированности компетенций определяется следующим образом:

1. Высокий уровень сформированности компетенций соответствует оценке зачтено:
   - Обучающийся глубоко понимает принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;

2. Средний уровень соответствует оценке зачтено:
   - Обучающийся понимает особенности принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности на среднем уровне.

3. Базовый уровень соответствует оценке зачтено:
   - Обучающийся понимает особенности принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности на базовом уровне.

4. Низкий уровень соответствует оценке не зачтено.

© ФГБОУ ВО «ЧелГУ»

© ФГБОУ ВО «ЧелГУ»