Фонд оценочных средств
для промежуточной аттестации
по дисциплине (модулю)
Основы информационной безопасности

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль)
специализация № 4 «Безопасность автоматизированных систем критически важных объектов»

Присваиваемая квалификация
специалист по защите информации

Форма обучения
очная

Год набора 2025

Челябинск 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки (специальность): 10.05.03 «Информационная безопасность автоматизированных систем».
Направленность (профиль): специализация № 4 «Безопасность автоматизированных систем критически важных объектов».
Дисциплина: **Основы информационной безопасности**.
Семестр изучения: 7 семестр.
Форма промежуточной аттестации: экзамен.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Основы информационной безопасности» 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
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Имеет представление об объективных потребностях личности, общества и государства в информационных технологиях и информационной безопасности. ОПК-1.2. Обладает навыками оценивать роль и значение информации, информационных технологий и информационной безопасности в современном обществе.	Знать: Для достижения индикатора ОПК-1.1: Знать основные термины по проблематике информационной безопасности; цели, задачи, принципы и основные направления обеспечения информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; содержание информационной войны, методы и средства ее ведения; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь: Для достижения индикатора ОПК-1.2: Уметь пользоваться современной

			научно-технической информацией по исследуемым проблемам и задачам Владеть: Для достижения индикатора ОПК-1.2: Владеть навыками использования профессиональной терминологии в области информационной безопасности.

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-1	Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации	Вопросы для устного опроса	Теоретические вопросы к экзамену
2.	ОПК-1	Раздел 2. Основы государственной политики Российской Федерации в области информационной безопасности	Вопросы для устного опроса Тесты	Теоретические вопросы к экзамену
3.	ОПК-1	Раздел 3. Информационное противоборство, методы и средства его осуществления	Вопросы для устного опроса	Теоретические вопросы к экзамену
4.	ОПК-1	Раздел 4. Виды защищаемой информации ограниченного доступа.	Вопросы для устного опроса Тесты	Теоретические вопросы к экзамену
5.	ОПК-1	Раздел 5. Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры	Вопросы для устного опроса Тесты	Теоретические вопросы к экзамену

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

3.2.1. Вопросы устного опроса на практических занятиях

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы, угрозы национальной безопасности Российской Федерации.
3. Понятие информационной безопасности, основные составляющие национальных интересов в информационной сфере.
4. Факторы, способствующие повышению роли информационной безопасности в системе национальной безопасности.
5. Основные положения государственной политики и организационная основа обеспечения информационной безопасности.
6. Компетенция федеральных и региональных органов государственной власти в сфере обеспечения информационной безопасности.
7. Правовая и организационная система обеспечения информационной безопасности Челябинской области.
8. Интересы личности общества и государства в информационной сфере.
9. Характеристика основных видов угроз информационной безопасности.
10. Принципы обеспечения информационной безопасности.
11. Понятие информационной войны, цели и средства её ведения.
12. Основные компоненты информационной войны.
13. Понятие информационного оружия.
14. Классификация информационного оружия.
15. Понятие и свойства информации.
16. Виды защищаемой информации.
17. Обязанности обладателя по обеспечению защиты информации.
18. Режим конфиденциальности информации и порядок его введения, на примере режима коммерческой тайны
19. Конституция Российской Федерации о правах и обязанностях граждан в информационной сфере.
20. Структура законодательства в сфере обеспечения информационной безопасности.
21. Перечень статей УК РФ, предусматривающих уголовную ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
22. Федеральные органы, осуществляющие контрольные функции в сфере обеспечения информационной безопасности.
23. Административная ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
24. Понятие автоматизированной информационной системы.
25. Виды угроз безопасности информационных и телекоммуникационных систем.
26. Основные каналы утечки защищаемой информации.
27. Внешние источники угроз безопасности информационных систем.
28. Внутренние источники угроз безопасности информационных систем.
29. Элементы обстановки на объекте защиты, процедура оценки обстановки.
30. Критерии оценки защищенности автоматизированных информационных

систем.

31. Структура службы безопасности предприятия.

32. Основные этапы создания службы безопасности предприятия.

33. Основные задачи, решаемые подразделением обеспечения информационной безопасности.

34. Обязанности руководителя подразделения информационной безопасности.

35. Обязанности системного администратора (администратора безопасности).

36. Обязанности пользователя автоматизированной информационной системы по обеспечению информационной безопасности.

37. Понятие и основные виды терроризма.

38. Роль информационных технологий в управлении критически важными объектами государства.

39. Способы совершения террористического акта в отношении объектов информационной инфраструктуры.

40. Использование террористическими организациями сети Интернет.

41. Понятие объекта, критически важного для обеспечения национальной безопасности государства, классификация критически важных объектов.

42. Угрозы уязвимости информационной инфраструктуры критически важных объектов.

43. Негативные последствия нарушения функционирования систем управления критически важных объектов.

44. Определение требований к защите информации в АСУ ТП.

45. Разработка и внедрение защиты АСУ ТП.

46. Обеспечение защиты информации в ходе эксплуатации АСУ ТП.

3.2.2. Перечень вопросов к экзамену

1. Понятие национальной безопасности. Основные угрозы и критерии оценки состояния национальной безопасности России.
2. Категории персональных данных. Уровни защищенности информационной системы персональных данных (ИСПД).
3. Понятие информационной безопасности. Интересы личности, общества и государства в информационной сфере.
4. Обязанности обладателя конфиденциальной информации по ее защите.
5. Основные положения государственной политики и организационная основа обеспечения информационной безопасности РФ.
6. Требования к обеспечению безопасности ИСПД в зависимости от уровня защищенности ИСПД.
7. Угрозы информационной безопасности Российской Федерации.
8. Понятие информационной войны, цели и средства её ведения.
9. Контроль и надзор в сфере обеспечения информационной безопасности.
10. Понятие и основные свойства информации. Виды защищаемой информации.
11. Конституция РФ о правах и обязанностях граждан в информационной сфере.
12. Общие принципы и методы обеспечения информационной безопасности РФ.
13. Основные направления обеспечения информационной безопасности объектов критической информационной инфраструктуры (КИИ). Порядок категорирования объектов КИИ.

14. Состав преступления, предусмотренный статьей 274 УК РФ.
15. Задачи единой государственной системы обнаружения и предупреждения компьютерных атак на критически важную информационную инфраструктуру (ГосСОПКА)..
16. Должностные обязанности руководителя подразделения информационной безопасности.
17. Правовой режим защиты государственной тайны. Порядок допуска к сведениям, составляющим гостайну.
18. Состав и содержание организационных и технических мер по защите ИСПД.
19. Правовой режим защиты коммерческой тайны.
20. Процедура оценки обстановки на объекте защиты.
21. Состав преступления, предусмотренный статьей 272 УК РФ.
22. Типовые и частные модели угроз безопасности ИСПД.
23. Состав преступления, предусмотренный статьей 273 УК РФ.
24. Состав и содержание организационных и технических мер по защите значимого объекта КИИ.
25. Состав преступления, предусмотренный статьей 274.1 УК РФ.
26. Этапы создания и структура службы безопасности предприятия.
27. Понятие и виды административной ответственности за нарушение требований информационной безопасности.
28. Задачи подразделения информационной безопасности предприятия.
29. Комплексная защита информации – сущность и задачи.
30. Должностные обязанности администратора безопасности АИС.
31. Компетенция ФСБ России в сфере обеспечения информационной безопасности.
32. Обязанности пользователя АИС по обеспечению информационной безопасности.
33. Понятие объекта КИИ. Порядок категорирования объектов КИИ.
34. Компетенция ФСТЭК России в сфере обеспечения информационной безопасности.
35. Обязанности оператора по защите персональных данных.
36. Классификация информационного оружия.

База тестовых вопросов

№ п/п	Формулировка вопроса	Варианты ответов (полужирным шрифтом – верные варианты)
	История операционных систем, общие понятия	
1	В каком году утверждена действующая Доктрина информационной безопасности РФ:	а) 2010 г.; **б) 2016 г.;** в) 2015 г.
2	Сколько групп национальных интересов в информационной сфере сформулировано в действующей Доктрине информационной безопасности РФ:	а) 3; б) 4; **в) 5.**
3	Какая группа национальных интересов в информационной сфере отсутствовала в предыдущей Доктрине информационной безопасности РФ:	**а) содействие формированию системы международной информационной безопасности;** б) доведение до российской и международной общественности достоверной информации о государственной политике РФ; в) обеспечение и защита прав и свобод человека и гражданина в информационной сфере.
4	Фраза «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» содержится в:	**а) статье Конституции РФ;** б) статье Уголовного Кодекса РФ; в) статье Гражданского Кодекса РФ.
5	Какая статья Конституции РФ разрешает на законном основании ограничивать права и свободы граждан РФ в информационной сфере:	а) статья 23; б) статья 33; **в) статья 55**.
6	К основным принципам обеспечения информационной безопасности относится:	а) принцип объективности; б) принцип своевременности; **в) принцип законности общественных отношений в информационной сфере**
7	Какой Федеральный закон РФ является базовым с точки зрения регулирования общественных отношений в информационной сфере:	а) № 152-2006 г.; **б) № 149-2006 г.;** в) № 98-2004 г.
8	Согласно закону "Об информации, информационных технологиях и о защите информации", информация это:	**а) сведения (сообщения, данные) независимо от формы их представления;** б) сведения, зафиксированные на материальном носителе; в) сведения, которые кого-либо интересуют.
9	Защита какого из перечисленных видов конфиденциальной информации осуществляется ее обладателем на добровольной основе:	**а) коммерческая тайна;** б) врачебная тайна; в) тайна следствия и судопроизводства.
10	Какая государственная структура осуществляет разработку стандартов информационной безопасности в банковской сфере:	а) ФСБ России; **б) Банк России;** в) ФСТЭК России.
11	Информационная система - это:	**а) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;** б) совокупность субъектов, осуществляющих сбор, формирование, распространение и использование информации; в) технологическая система, предназначенная для

		передачи информации по линиям связи, доступ к которой осуществляется с использованием СВТ.
12	Возможные воздействия на информационную систему, которые прямо или косвенно могут нанести ущерб - это:	а) атака на информационную систему; **б) угроза безопасности информационной системы;** в) неправомерный доступ к защищаемой информации.
13	Политика информационной безопасности предприятия - это:	**а) совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты информационной инфраструктуры от актуальных угроз безопасности;** б) документ, устанавливающий правила доступа к защищаемой информации; в) комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии.
14	Антропогенные источники угроз безопасности информации – это:	**а) источники, обусловленные действиями субъекта;** б) источники, обусловленные техническими средствами; в) стихийные бедствия.
15	Кадровая безопасность - это:	**а) состояние защищенности организации от угроз, обусловленных человеческим фактором;** б) комплекс мер по обеспечению состояния защищенности персонала; в) наука, изучающая подходы к исследованию угроз персоналу.
16	Санкционированный доступ - это:	а) получение от субъекта доступа к сведениям (имя, учетный номер и т.д.), позволяющим выделить его из множества субъектов; **б) доступ с выполнением правил разграничения доступа к информации;** в) получение от субъекта сведений (пароль, биометрические параметры и т.д.), подтверждающих, что идентифицируемый субъект является тем, за кого себя выдает.
17	Аутентификация - это:	а) проверка количества переданной и принятой информации; б) поиск файлов, которые изменены в информационной системе несанкционированно; **в) проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы.**
18	Атака на информационную систему - это:	**а) действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы;** б) исследование возможности расшифровки информации без знания ключей; в) создание средств уничтожения, искажения, или хищения информационных массивов
19	Основное средство обеспечения конфиденциальности информации, передаваемой по открытым каналам связи -	а) аутентификация; б) идентификация; **в) шифрование.**

	это:	
20	Должностной регламент сотрудника подразделения информационной безопасности – это:	а) инструкция руководителя, которую необходимо выполнять в обязательном порядке; б) документ, в котором перечислены возможные нарушения распорядка дня; **в) организационно-распорядительный документ длительного или постоянного срока действия, в котором определены права и обязанности сотрудника.**

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

В течении семестра на практических занятиях проводится регулярный устный опрос. Предусмотрены 9 устных опросов.

Набранные баллы на практических занятиях являются допуском к экзамену.

Максимальный балл за один устный опрос – 10 баллов.

Максимальный балл за все устные опросы – 90 баллов.

Допуском к экзамену является более 50 набранных баллов, недопуском –менее 50.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Устный опрос на практических занятиях	9x10=90
2	Экзамен	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания устного опроса на практических занятиях

Максимальный балл за ответ на теоретический вопрос – 10 баллов.

Отлично/зачтено/9-10 баллов	**Хорошо/зачтено/7-8 баллов**	**Удовлетворительно/зачтено/5-6 баллов**	**Неудовлетворительно/не зачтено/0-4 балла**
Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.	Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.2.2. Критерии оценивания теста на экзамене

Тест формируется в системе электронного обучения MOODLE.
Максимальный балл за тест – 100 баллов.

Оценка	**Отлично/зачтено**	**Хорошо/зачтено**	**Удовлетворительно/зачтено**	**Неудовлетворительно/не зачтено**
Баллы	**91-100 баллов**	**70-90 баллов**	**50-69 баллов**	**0-49 баллов**
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

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 - 60 баллов - неудовлетворительно (2);
61 - 69 баллов - удовлетворительно (3);
70 - 90 баллов - хорошо (4);
91 - 100 баллов - отлично (5).

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 отлично:
   - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности: формируются навыки составления информационных обзоров по национальной и международной практике аудита, навыки систематизации данных, необходимых для решения экономических задач
   - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, критически оценивать информацию о состоянии и проблемах развития аудиторской деятельности, формулировать собственные выводы.
2. Средний уровень соответствует оценке хорошо:
   - предполагает формирование компетенций на более высоком уровне: формируется комплексное знание особенностей применения и понимания национальных и международных стандартов аудита, умение сбора, анализа и обработки данных, необходимых для решения ситуаций в процессе аудиторских проверок;
   - студент способен давать развернутые ответы на теоретические вопросы дисциплины на уровне не ниже оценки «удовлетворительно».
3. Базовый уровень соответствует оценке удовлетворительно:
   - предполагает формирование компетенций на начальном уровне: знание основных положений национальных и международных стандартов аудиторской деятельности;
   - студент способен отвечать на вопросы в форме закрытого теста. Количество правильных ответов – не менее 50%.
4. Низкий уровень соответствует оценке неудовлетворительно.

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом физического факультета

Протокол заседания № 05 от 06.02.2025

Председатель Ученого совета физического факультета согласовано М.А. Загребин

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 08 от 01.02.2025

Заведующий кафедрой согласовано А.Н. Ручай

Автор (составитель) А.Н. Ручай

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