Фонд оценочных средств для промежуточной аттестации
по дисциплине (модулю)
Введение в специальность

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Специализация №4
Безопасность автоматизированных систем критически важных объектов

Присваиваемая квалификация (степень)
Специалист по защите информации

Форма обучения
Очная

Год набора 2026

Челябинск, 2026 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность: 10.05.03 Информационная безопасность автоматизированных систем
Специализация: Безопасность автоматизированных систем критически важных объектов
Дисциплина: Введение в специальность
Семестр: 1, 2
Форма промежуточной аттестации: зачет
Система оценивания: оценивание результатов осуществляется в рамках бинарной системы «зачтено», «не зачтено».

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Введение в специальность» направлено на формирование следующих компетенций:

Коды компетенции (по ФГОС)	Содержание компетенций согласно ФГОС	Индикаторы достижения компетенций согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-1	Способен разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных научно-исследовательских работ в области защиты информации.	ПК-1.1. Обладает знаниями национальных, межгосударственных и международных стандартов, нормативных правовых актов, а также руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации. ПК-1.2. Демонстрирует умение выполнять сбор, обработку, анализ и систематизацию научно-технической информации, нормативных и методических материалов в области защиты информации. ПК-1.3. Имеет практический опыт (навыки) разработки научно-технической документации, отчетов, обзоров, публикаций по результатам выполненных научно-исследовательских работ в области защиты информации.	Для достижения индикатора ПК-1.1: Знать национальные, межгосударственные и международные стандарты, нормативные правовые акты, а также руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Для достижения индикатора ПК-1.2: Уметь выполнять сбор, обработку, анализ и систематизацию научно-технической информации, нормативных и методических материалов в области защиты информации. Для достижения индикатора ПК-1.3: Владеть навыками разработки научно-технической документации, отчетов, обзоров, публикаций по результатам выполненных научно-исследовательских работ в области защиты информации.
ПК-2	Способен создавать и исследовать модели автоматизированных систем, проводить анализ их защищенности, а также предлагать и обосновывать	ПК-2.1. Обладает знаниями моделирования и исследования систем защиты информации автоматизированных систем. ПК-2.2. Демонстрирует умение разрабатывать и исследовать	Для достижения индикатора ПК-2.1: Знать моделирование и исследование систем защиты информации автоматизированных систем (систему организации научно-исследовательской работы в

	выбор решений по обеспечению эффективности средств и способов защиты информации.	математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач, и применять эти модели при проектировании систем защиты информации автоматизированных систем. ПК-2.3. Имеет практический опыт (навыки) оценки защищенности информации в автоматизированных системах и выбора обоснованных решений по обеспечению эффективности средств и способов их защиты.	образовательном учреждении, стандарты и методы управления информационной безопасностью телекоммуникационной системы, основные проблемы, тенденции, методы и понятия в области защиты информации в современных условиях). Для достижения индикатора ПК-2.2: Уметь разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач, и применять эти модели при проектировании систем защиты информации автоматизированных систем (анализировать состав задач, к решению которых должен быть подготовлен специалист по информационной безопасности). Для достижения индикатора ПК-2.3: Владеть навыками оценки защищенности информации в автоматизированных системах и выбора обоснованных решений по обеспечению эффективности средств и способов их защиты (основными понятиями профессиональной терминологии по информационной безопасности).

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Контролируемые темы/ разделы	Код компетенции	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации
1.	Введение в информационную безопасность автоматизированных систем.	ПК-1 ПК-2	Реферат	Вопросы к зачету
2.	Государственная система защиты информации.	ПК-1 ПК-2	Реферат	Вопросы к зачету
3.	Введение в специальность	ПК-1 ПК-2	Реферат	Вопросы к зачету

3.2 Содержание оценочных средств

Примерная тематика рефератов:

1. Цифровые приемные устройства, SDR-технология, проект GNU-радио, комерчески-доступные ЦПУ
2. Перехват изображения ЭЛТ монитора (работа Ван Эйка)
3. Перехват изображения ЖК монитора (работа Маркуса Куна, проект TempestSDR)
4. Лев Термен – проект «Златоуст», проект «Буран», сигнализация и терменвокс

5. Програмный ПЭМИН (Soft TEMPEST) проект system bus radio
6. ПЭМИН (TEMPEST) - история
7. Фоноскопия и разборчивость речи (история вопроса)
8. Охота на Лис (история вопроса), радиопеленгация, радиоориентирование
9. Глобальные системы позиционирования GPS, ГЛОНАСС, DORIS, COMPASS, GALILEO.
10. Радиолокация (историческая справка), пассивная радиолокация
11. Системы передачи аэронавигационной информации (ADS-B - транспондеры)
12. Радиочастотное опознование (история), уязвимости RFID и NFC
13. Уязвимости системы спекулятивного выполнения кода (MELTDOWN/SPECTRE)
14. Уязвимости беспроводных сетей Bluetooth и Wi-FI
15. Межсетевое экранирование, задачи, эволюция средств, программные и аппаратные, NGFW
16. Уязвимости связанные с виртуализацией, Joanna Rutkowska, Blue-Red Pill
17. Гипервизоры и «виртуальные машины», основные виды, функциональные возможности, уязвимости
18. Облачные и безсерверные вычисления, модели, уязвимости, применение для сервисов ИБ
19. Сертифицированные ФСТЭК ОС, защищенные и специального назначения. Astra Linux
20. Анализ уязвимости сетей и рабочих станций, инструменты, pentest и forensic дистрибутивы
21. Машинное обучение, Глубокое обучение
22. Интернет вещей, ссистемы IoT, уязвимости
23. Блокчейн-системы, концепция, уязвимости, недостатки
24. Локальные и глобальные сети, сетевая модель OSI, уровни, протоколы модели IP
25. Интернет-ресурсы, разработка системы управления контентом CMS
26. Языки программирования, спецификация, стандартизация, классификация. Языки низкого и высокого уровня. Компилируемые, интерпретируемые и встраиваемые языки.
27. Интернет-мошеничество, фишинг, сертификаты – доверенные, самоподписанные
28. Атаки на отказ в обслуживании, классификация DoS-атак, примеры.
29. Системы управления базами данных, примеры.
30. Архитектура программного обеспечения. Шаблоны, фреймворки.

Реферат – творческая исследовательская работа, основанная, прежде всего, на изучении значительного количества научной и иной литературы по теме исследования. Цель написания реферата – привитие студенту навыков краткого и лаконичного представления собранных материалов и фактов в соответствии с требованиями, предъявляемыми к научным отчетам, обзорам и статьям. Реферат оценивается руководителем исходя из установленных показателей и критериев оценки реферата:

Рекомендации по написанию реферата:

1) Тема реферата выбирается в соответствии с интересами студента и не обязательно должна соответствовать приведенному примерному перечню. Важно, чтобы в реферате были освящены стороны проблемы, а также представлены теоретические положения и конкретные примеры.
2) Реферат должен основываться на проработке нескольких дополнительных к основной литературе источников. Как правило это научные монографии или статьи.
3) План реферата должен быть авторским. В нем проявляется подход автора, его мнение, анализ проблемы.
4) Все приводимые в реферате факты и заимствованные соображения должны

сопровождаться ссылками на источник информации.
5) Недопустимо просто скомпоновать реферат из кусков заимствованного текста. Все цитаты должны быть представлены в кавычках с указанием в скобках источника и страницы.
6) Реферат оформляется в виде текста на листах формата А-4. Работа начинается с титульного листа, в котором указывается название университета, название кафедры, учебной дисциплины, тема реферата, ФИО студента, номер группы, год и географическое место местонахождения университета. Затем следует оглавление с указанием страниц разделов. Сам текст реферата желательно подразделить на разделы: главы, подглавы и озаглавить их. Приветствуется использование в реферате количественных данных и иллюстраций (графики, таблицы, диаграммы, рисунки).
7) Завершают реферат разделы «Заключение» и «Список использованной литературы». В заключении должны быть представлены основные выводы, ясно сформулированные в тезисной форме.
8) Источник литературы должен быть составлен в полном соответствии с действующим стандартом (правилами), включая особую расстановку знаков препинания.

Вопросы к зачёту:
1. Стандартизация в области построения систем управления. История развития. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р СО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, BS 25999 и др.).
2. Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни.
3. Что понимается под системой безопасности?
4. Какие вопросы, касающиеся информационной безопасности, содержатся в Конституции РФ?
5. Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процессами?
6. Какие вопросы, касающиеся информационной безопасности, содержатся в Гражданском кодексе РФ?
7. Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию.
8. Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?
9. Какие основные понятия рассматриваются в Законе РФ"Об информации, информатизации и защите информации"?
10. Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации.
11. Дайте определение лицензирования. Кто такие лицензиат и лицензирующие органы? Почему лицензирование и сертификация выступают в качестве средства защиты информации? Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии.
12. Дайте определение информационной безопасности, прокомментируйте его составляющие. Перечислите основные категории информационной безопасности.
13. Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации?

14. Какие Вам известны международные стандарты, напрямую связанные с ИБ?
15. Что можно сказать о законодательстве других стран по вопросам ИБ?
16. Приведите основные направления деятельности по вопросам ИБ на законодательном уровне.
17. Прокомментируйте основные составляющие информационной безопасности РФ.
18. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
19. Классифицируйте угрозы ИБ РФ для личности, для общества, для Государства по общей направленности.
20. Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность.
21. В чем специфика деятельности ФСТЭК России?
22. Что такое вредоносное программное обеспечение? Дайте определение, «вируса», «эксплойта», «вирусного оружия», «червя». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?
23. Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация?
24. Дайте определение защищаемой информации и охарактеризуйте ее основные признаки.
25. Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты?
26. Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне. Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности.
27. Прокомментируйте возможности биометрической идентификации (аутентификации).
28. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
29. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
30. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Студент допускается к зачету по дисциплине в случае выполнения им учебного плана по дисциплине (выполненных и защищенных работ). В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.

В 1 семестре зачет проводится по билетам в устной форме. Студент выбирает билет в случайном порядке. Время подготовки студента для устного ответа на зачете должно составлять не менее 40 минут, время ответа – не более 20 минут. При подготовке и ответе на вопросы билета студент должен вести необходимые записи в листе устного ответа, который по окончании зачета подписывается студентом, сдаётся преподавателю и сохраняется им до окончания экзаменационной сессии.

Во 2 семестре зачет проходит в виде защиты реферата.

Проявленные студентом в ходе зачета знания оцениваются словами «зачтено», «не зачтено».

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

Критерии оценивания ответа (устного опроса) на зачете в 1 семестре:

«Зачтено» выставляется:

1) содержание материала билета раскрыто полностью;
2) материал изложен грамотно, в определенной логической последовательности, точно используется терминология;
3) показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации;
4) продемонстрировано усвоение ранее изученных сопутствующих вопросов;
5) ответ самостоятельный, без наводящих вопросов;
6) допущены одна–две неточности при освещении второстепенных вопросов, которые исправляются после замечаний или наводящих вопросов.

«Не зачтено» выставляется:

1) не раскрыто основное содержание учебного материала;
2) обнаружено незнание или непонимание большей или наиболее важной части учебного материала;
3) допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.

Критерии оценивания реферата во 2 семестре:

1) Новизна реферированного текста (Макс. - 5 баллов)
- актуальность проблемы и темы;
- новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы;
- наличие авторской позиции, самостоятельность суждений.

2) Степень раскрытия сущности проблемы (Макс. - 5 баллов)
- соответствие плана теме реферата;
- соответствие содержания теме и плану реферата;
- полнота и глубина раскрытия основных понятий проблемы;
- обоснованность способов и методов работы с материалом;
- умение работать с литературой, систематизировать и структурировать материал;
- умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.

3) Обоснованность выбора источников (Макс. - 5 баллов)
- круг, полнота использования литературных источников по проблеме;
- привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).

4) Соблюдение требований к оформлению (Макс. - 5 баллов)
- правильное оформление ссылок на используемую литературу;
- грамотность и культура изложения;
- владение терминологией и понятийным аппаратом проблемы;
- соблюдение требований к объему реферата;
- культура оформления: выделение абзацев.

5) Грамотность (Макс. - 5 баллов)
- отсутствие орфографических и синтаксических ошибок, стилистических погрешностей;
- отсутствие опечаток, сокращений слов, кроме общепринятых;
- литературный стиль

Реферат оценивается по 25 балльной шкале, балы переводятся в оценки успеваемости следующим образом:
15 баллов и выше - "зачтено"
меньше 15 баллов - "не зачтено"

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

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

1. Высокий, средний и базовый уровень сформированности компетенций соответствует оценке «зачтено».
2. Низкий уровень сформированности компетенций соответствует оценке «не зачтено».

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:
Проректор по учебной работе утверждено 27.02.26 А.А. Саламатов

Ученым советом физического факультета

Протокол заседания № 04 от 05.02.2026

Председатель Ученого совета
физического факультета согласовано М.А. Загребин

Заседанием кафедры радиофизики и электроники

Протокол заседания № 07 от 03.02.2026

Заведующий кафедрой согласовано А.В. Бутаков

Автор (составитель) М.Е. Беленков

Структура фондов оценочных средств соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от 27 сентября 2022 №573-1