Фонд оценочных средств для промежуточной аттестации
по дисциплине (модулю)
Защищенные интернет-технологии

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 2025

Челябинск, 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность: 10.05.03 Информационная безопасность автоматизированных систем
Специализация: Безопасность автоматизированных систем критически важных объектов
Дисциплина: Защищенные интернет-технологии
Семестр: 5
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 «Защищенные интернет-технологии» направлено на формирование следующих компетенций:

Коды компетенции (по ФГОС)	Содержание компетенций согласно ФГОС	Индикаторы достижения компетенций согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-7	Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1. Обладает базовыми знаниями в области программирования. ОПК-7.2. Демонстрирует умения создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач. ОПК-7.3. Имеет практический опыт осуществлять обоснованный выбор инструментария программирования и способов организации программ.	Для достижения индикатора ОПК-7.1: Знать базовые понятия в области программирования (технологию разработки web-приложений). Для достижения индикатора ОПК-7.2: Уметь создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач (разрабатывать web-приложения). Для достижения индикатора ОПК-7.3: Владеть навыками осуществления обоснованного выбора инструментария программирования и способов организации программ.
ОПК-13	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.1. Обладает знаниями о диагностике, тестировании и анализе уязвимостей систем защиты информации автоматизированных систем. ОПК-13.2. Демонстрирует умения организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем. ОПК-13.3. Имеет	Для достижения индикатора ОПК-13.1: Знать о диагностике, тестировании и анализе уязвимостей систем защиты информации автоматизированных систем (основные подходы к процессам аудита, мониторинга, самообследования и контроля СУИБ, основные приемы поиска и анализа информации, методы и технологии проектирования и развертывания защищённых систем в локальных вычислительных сетях). Для достижения индикатора ОПК-13.2: Уметь организовывать и проводить

		практический опыт проводить анализ уязвимостей систем защиты информации автоматизированных систем.	диагностику и тестирование систем защиты информации автоматизированных систем (анализировать защищенность автоматизированных систем, организовывать и управлять зашифрованными соединениями, настраивать средства межсетевого экранирования, системы обнаружения и предотвращения вторжений). Для достижения индикатора ОПК-13.3: Владеть навыками проведения анализа уязвимостей систем защиты информации автоматизированных систем (навыками поиска и анализа регулирующих и методических документов, навыками анализа уязвимостей систем защиты информации автоматизированных систем).

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Код компетенции	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	ОПК-7 ОПК-13	Раздел 1. Государственная система защиты информации.	Собеседование	Вопросы к зачету № 1 - 9
		Раздел 2. Локальные вычислительные сети и интернет- технологии	Собеседование и отчеты по лабораторным работам.	Вопросы к зачету № 7 – 11
		Раздел 3. Защищенные протоколы	Собеседование и отчеты по лабораторным работам.	Вопросы к зачету № 12 - 17
		Раздел 4. Основы программирования сетевых приложений	Собеседование и отчеты по лабораторным работам.	Вопросы к зачету № 13 - 19

3.2 Содержание оценочных средств

Вопросы для собеседования по лабораторным работам:

1) Нормативно-правовые акты в сфере информационной безопасности, действующие на территории Российской Федерации;

2) Государственные стандарты в области защиты информации и сетевых технологий;
3) Криптографические стандарты и средства, базовые технологии обеспечения информационной безопасности;
4) Анализ защищенности автоматизированных систем;
5) Базовые технологии проектирования систем мониторинга средств защиты информации;
6) Разработке защищенных автоматизированных систем в сфере профессиональной деятельности;
6) Оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;
7) Проектировании средств защиты информации автоматизированной системы;
8) Эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
9) Проектирование, внедрение и использование системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов.

Критерии оценивания собеседования и отчета по лабораторным работам:

В процессе выполнения лабораторной работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование.

Лабораторная работа засчитывается студенту, если он представил правильно оформленный отчет; владеет методикой обработки данных; усвоил теоретический материал по данной теме (последовательно, грамотно и логически стройно его излагает, уверенно отвечает на вопросы). Допускаются несущественные неточности в оформлении и ответах на вопросы.

Лабораторная работа не засчитывается студенту в случаях: наличия ошибок в расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.

Вопросы к зачету:

1. Государственная система защиты информации. Правовое и методическое обеспечение в области защиты информации.
2. Эталонная модель TCP/IP. Эталонная модель RM OSI. Стандартизация технологий сети Интернет (RFC).
3. Схема адресации в сети Интернет. Числовые адреса IPv4, IPv6. TCP адреса и UDP-адреса. Адресация сервисов. Символические адреса, DNS-серверы.
4. Базовые протоколы Протоколы IP, ICMP, UDP.
5. Протоколы маршрутизации. Основные характеристики протоколов RIP, OSPF, IGRP, EGP, BGP.
6. Socket API - прикладной программный интерфейс для программирования сетевых приложений. Понятие гнезда (socket). Примеры функций Socket API.
7. Криптографические основы сетевой безопасности. Криптография. Криптоанализ. Сеть Фейштеля. Критерии разработки криптоалгоритмов.
8. Криптографические алгоритмы защиты информации. Понятия симметричного шифрования, открытого ключа, хэш-функции, электронной подписи, примеры. Понятие инфраструктуры открытых ключей и проблемы ее создания.

9. Назначение и особенности применения алгоритмов DES и 3DES, Blowfish, IDEA, ГОСТ 28147, ГОСТ Р 34.12. Алгоритмы симметричного шифрования.
10. Создание случайных чисел. Алгоритм AES. Алгоритм Rijndael. Алгоритм RC6.
11. Алгоритмы асиммитричного шифрования. Diffie-Hellman, RSA.
12. Хэш-функции. Алгоритмы SHA и MD5.
13. Цифровая подпись. Прямая и арбитражная цифровые подписи. Стандарт цифровой подписи DSS. Отечественный стандарт цифровой подписи ГОСТ 34.10.
14. Алгоритм цифровой подписи на основе эллиптических кривых ECDSA.
15. Шифрование/дешифрование с использованием эллиптических кривых.
16. Протоколы защищенной передачи данных. Назначение протоколов SSL, SSH, PGP, IPSec, PPTP, L2TP.
17. Автоматизированное рабочее место в информационной системе. Защита конечных точек. Аппаратно-программные системы защиты информации от НСД, обеспечения доверенной загрузки.
18. Аппаратно-программные средства защиты информации и управления сетью. Сервер доступа и центр управления сетью. Криптошлюз. Криптографический коммутатор. Детектор атак.
19. Межсетевые экраны. Классификация, классы защищенности. Реализация МСЭ на канальном и сетевом уровнях. Шлюзы сеансового уровня. Посредники прикладного уровня. Типы окружений для МСЭ. DMZ-сети, конфигурации с одной и двумя DMZ-сетями.

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.

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.

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:

«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.

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 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 радиофизики и электроники

Протокол заседания № 07 от 04.02.2025

Заведующий кафедрой согласовано А.В. Бутаков

Автор (составитель) А.В. Бутаков

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