Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю) Методы и средства криптографической защиты информации

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: Методы и средства криптографической защиты информации
Семестр: 7, 8
Форма промежуточной аттестации: зачет (7 семестр)
Система оценивания: оценивание результатов осуществляется в рамках бинарной системы «зачтено», «не зачтено».
Форма промежуточной аттестации: экзамен (8 семестр)
Система оценивания: оценивание результатов осуществляется в рамках 5-балльной системы

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Методы и средства криптографической защиты информации» 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-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Обладает базовыми знаниями в области криптографии. ОПК-10.2. Демонстрирует умения использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	Для достижения индикатора ОПК-10.1: Знать базовые понятия в области криптографии (основные понятия и классификацию средств криптографической защиты информации, различия между стеганографией и криптографией, основные методы симметричного шифрования, классификацию методов симметричного шифрования, основные свойства симметричных криптосистем, понятие хеш-функции, основные понятия, основные алгоритмы электронной цифровой подписи, основные стандарты на алгоритмы цифровой подписи). Для достижения индикатора ОПК-10.2: Уметь использовать средства криптографической защиты информации при решении задач профессиональной деятельности (использовать блочные алгоритмы шифрования для формирования хеш-функции, криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем, односторонние функции в целях построения криптосистем, криптографические методы защиты информации для обеспечения безопасности как локальных,

			так и распределенных систем, алгоритмы генерации, хранения и распределения ключей, проектировать и использовать системы электронной цифровой подписи). Для достижения индикатора ОПК-10.2: Владеть навыками использования средства криптографической защиты информации при решении задач профессиональной деятельности (навыками симметричного шифрования, формирования хеш-функций, по обеспечению безопасной работы в сети Интернет, применения асимметричных криптосистем, управления ключами в системах с открытым ключом, по созданию электронной цифровой подписи).

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-10	Криптографические методы защиты информации: история криптографии; виды информации, подлежащие закрытию, их модели и свойства. Введение в криптографические методы защиты информации.	Собеседование и отчеты по практическим работам.	Вопросы к зачёту №1-4, 8-12.
		Шифры простой замены и перестановки. Поточные и блочные шифры простой замены. Шифры гаммирования.	Собеседование и отчеты по практическим работам.	Вопросы к зачёту №5-7, 13.
		Криптографическая стойкость шифров: основные требования к шифрам. Совершенные шифры.	Собеседование и отчеты по практическим работам.	Вопросы к зачёту №14.
		Блочные системы шифрования. Стандарты шифрования ГОСТ 28147-89, DES. Анализ алгоритмов блочного шифрования. Поточные	Собеседование и отчеты по практическим работам.	Вопросы к зачёту №15-18.

		системы шифрования.		
		Псевдослучайные последовательности.	Собеседование и отчеты по практическим работам.	Вопросы к зачёту №19.
		Криптоанализ блочных шифров.	Собеседование и отчеты по практическим работам.	Вопросы к зачёту №20.
		Асимметричные системы шифрования. Алгоритмы Диффи-Хеллмана. Шифрсистемы RSA, Эль-Гамаля, Мак-Элиса, Рабина.	Собеседование и отчеты по практическим работам.	Вопросы к экзамену №1-7.
		Криптографические хеш-функции. Требования. Назначение. Схемы построения. Стандарты. Криптоанализ.	Собеседование и отчеты по практическим работам.	Вопросы к экзамену №8-12.
		Электронная цифровая подпись. Модель ЭЦП. Задачи ЭЦП. Алгоритмы и стандарты ЭЦП.	Собеседование и отчеты по практическим работам.	Вопросы к экзамену №13-21.

3.2 Содержание оценочных средств

Темы практических работ:
1. Шифры простой замены.
2. Шифры подстановки.
3. Стандарты шифрования DES, ГОСТ 28147 - 89, AES.
4. Система RSA.
5. Криптографические хеш-функции.
6. Электронная цифровая подпись.

Критерии оценивания собеседования и отчета по практическим работам:

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

Практическая 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.

Практическая 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. Задачи и основные цели криптографии.
2. Основные типы криптоаналитического вскрытия.
3. Безопасность алгоритмов.
4. Стеганография.
5. Подстановочные шифры.
6. Шифры перестановки.
7. Гаммирование.
8. Протоколы. Характеристики протоколов.
9. Протоколы с посредником.
10. Арбитражные протоколы.
11. Передача информации с использованием симметричной криптографии.
12. Передача информации с использованием криптографии с открытыми ключами.
13. Шифры гаммирования: Шифр модульного гаммирования Виженера; Шифр Вернама.
14. Надежность шифров.
15. Сеть Фейстеля.
16. Алгоритм шифрования DES.
17. Стандарт шифрования ГОСТ 28147-89.
18. Поточные системы шифрования.
19. Генерация случайных и псевдослучайных последовательностей.
20. Криптоанализ блочных шифров.

Вопросы к экзамену:

1. Алгоритм Диффи-Хеллмана. Задача Диффи-Хеллмана. Задача дискретного логарифмирования.
2. Криптосистема RSA. Задача RSA.
3. Атаки на RSA.
4. Алгоритмы факторизации.
5. Выбор параметров криптосистемы RSA.
6. Схема шифрования RSA-OAEP.
7. Криптосистемы с открытым ключом.
8. Хеш-функции. Требования.
9. Хеш-функции. Предназначение.
10. Стандарты хеш-функций.
11. Общая схема алгоритмов MD4, MD5, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94, SHA.
12. Криптоанализ хеш-функций. Модель случайного оракула (ROM).
13. Электронная цифровая подпись (ЭЦП). Задачи ЭЦП.
14. Схема ЭЦП Диффи-Лампорта. Вероятностная схема ЭЦП Рабина.
15. Схема ЭЦП Эль-Гамаля. Уменьшение размера подписи в схеме Эль-Гамаля.
16. ЭЦП DSA.
17. ЭЦП ГОСТ Р 34.10-94.
18. ЭЦП Онга-Шнорра-Шамира.
19. ЭЦП Шнорра.
20. Схемы ЭЦП с восстановлением сообщений (на основе RSA, на основе ЭЦП Эль-Гамаля, ЭЦП Рабина).

21. Слепая ЭЦП Чаума (на основе RSA).

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

В 7 семестре 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».

В 8 семестре студент допускается к экзамену 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.

Экзамен проводится по билетам в устной форме. При проведении экзамена экзаменуемый выбирает билет в случайном порядке. Экзаменатору предоставляется право по ходу экзамена задавать экзаменуемому уточняющие и дополнительные вопросы. Время подготовки студента для устного ответа на экзамене должно составлять не менее 40 минут, время ответа экзаменуемого – не более 20 минут. При подготовке и ответе на вопросы билета экзаменуемый должен вести необходимые записи в листе устного ответа, который по окончании экзамена подписывается студентом, сдаётся экзаменатору и сохраняется им до окончания экзаменационной сессии. Студент, испытавший затруднения при подготовке к ответу по выбранному билету, вправе выбрать второй билет с продлением времени на подготовку. При этом окончательная оценка студента снижается на один балл. Выбор студентом третьего билета не допускается.

Проявленные студентом в ходе экзамена знания оцениваются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

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.

Критерии оценивания ответа (устного опроса) на экзамене:

Оценка «отлично» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знания по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.

Оценка «хорошо» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.

Оценка «удовлетворительно» выставляется:

Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

Оценка «неудовлетворительно» выставляется:

1) Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.
2) Ответ на вопрос полностью отсутствует.
3) Отказ от ответа.

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 уровень сформированности компетенций соответствует оценке «отлично» («зачтено»).
2. Средний уровень сформированности компетенций соответствует оценке «хорошо» («зачтено»).
3. Базовый уровень сформированности компетенций соответствует оценке «удовлетворительно» («зачтено»).
4. Низкий уровень сформированности компетенций соответствует оценке «неудовлетворительно» («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) О.О. Павлухина

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