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

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Направленность (профиль)
специализация № 1 «Анализ безопасности компьютерных систем»

Присваиваемая квалификация
специалист по защите информации

Форма обучения
очная

Челябинск 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.
Специализация № 1 «Анализ безопасности компьютерных систем».
Дисциплина: **Методы и средства криптографической защиты информации**.
Семестр (семестры) изучения: 7,8 семестры.
Форма (формы) промежуточной аттестации:
зачет 7 семестр, экзамен 8 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

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 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-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты. ОПК-10.2 Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов. ОПК-10.3 Владеет навыками использования типовых криптографических алгоритмов.	Знать: – 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; – основные актуальные модели атак на алгоритмы цифровой подписи и их

			возможные результаты. Уметь: – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.

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-10	Раздел 1. Криптографические методы защиты информации: история криптографии; виды информации, подлежащие закрытию, их модели и свойства; Математические модели шифров и открытых текстов.	Проверочная работа	Вопросы к зачету
2.	ОПК-10	Раздел 2. Шифры простой замены и перестановки. Поточные и блочные шифры простой замены. Дисковые многоалфавитные шифры замены. Шифры гаммирования. Криптоанализ шифра Виженера.	Проверочная работа	Вопросы к зачету
3.	ОПК-10	Раздел 3. Криптографическая стойкость шифров: основные требования к шифрам. Совершенные шифры; теоретико-информационный подход к оценке криптостойкости шифров; вопросы практической стойкости; имитостойкость и помехоустойчивость шифров. Энтропия и избыточность языка. Расстояние единственности.	Проверочная работа	Вопросы к зачету
4.	ОПК-10	Раздел 4. Блочные системы шифрования. Стандарты шифрования ГОСТ 28147-89 и DES. Анализ алгоритмов блочного	Проверочная работа	Вопросы к зачету

		шифрования. Поточные системы шифрования. Синхронизация поточных шифрсистем. Примеры поточных шифрсистем. Линейные регистры сдвига. Методы анализа поточных шифрсистем.		
5.	ОПК-10	Раздел 5. Алгоритмы классификации псевдослучайных последовательностей. Криптостойкие генераторы на основе односторонних функций. Тестирование псевдослучайных последовательностей.	Проверочная работа	Вопросы к зачету
6.	ОПК-10	Раздел 6. Криптоанализ блочных шифров. Линейный криптоанализ. Шифр SPN. Дифференциальный криптоанализ.	Проверочная работа	Вопросы к зачету
7.	ОПК-10	Раздел 7. Асимметричные системы шифрования. Алгоритмы Диффи-Хеллмана. Шифрсистемы RSA, Эль-Гамаля, Мак-Элиса, Рабина. Криптоанализ асимметричных систем шифрования. Алгоритмы факторизации и дискретного логарифмирования.	Проверочная работа	Вопросы к экзамену
8.	ОПК-10	Раздел 8. Криптографические хеш-функции. Требования. Назначение. Схемы построения. Стандарты. Криптоанализ.	Проверочная работа	Вопросы к экзамену
9.	ОПК-10	Раздел 9. Электронная цифровая подпись. Модель ЭЦП. Задачи ЭЦП. Алгоритмы и стандарты ЭЦП.	Проверочная работа	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. Список вопросов для проверочных работ:

1 Формальные модели шифров, включая шифр простой замены и шифр перестановки.
2 Математические модели открытых текстов.
3 Шифры простой замены.
4 Блоковые шифры простой замены.
5 Шифры гаммирования.
6 Надежность шифров.
7 Сеть Фейстеля.
8 Поточные системы шифрования:
9 Методы криптоанализа симметричных криптосистем.
10 Алгоритм Диффи-Хеллмана. Задача Диффи-Хеллмана. Задача дискретного логарифмирования. Атаки.
11 Криптосистема RSA (шифрование, расшифрование, корректность). Задача RSA.
12 Атаки на RSA.
13 Алгоритмы факторизации.
14 Выбор параметров криптосистемы RSA. Генерация сильно простых чисел методом Гордона. Использование китайской теоремы об остатках в RSA.
15 Криптосистемы с открытым ключом.
16 Алгоритмы дискретного логарифмирования:
17 Хеш-функции. Требования. Предназначение.
18 Стандарты хеш-функций.
19 Общая схема алгоритмов MD4, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94.
20 Криптоанализ хеш-функций.
21 Электронная цифровая подпись (ЭЦП). Задачи ЭЦП.
22 Схема ЭЦП Диффи-Лампорта. Вероятностная схема ЭЦП Рабина.
23 Схема ЭЦП Эль-Гамаля. Уменьшение размера подписи в схеме Эль-Гамаля.

3.2.2. Список теоретических вопросов для зачёта (7 семестр):

№ п/п	Формулировка вопроса
1	Основные понятия: 1. Формальные модели шифров, включая шифр простой замены и шифр перестановки. 2. Математические модели открытых текстов.
2	Шифры простой замены: 1. Аффинный шифр простой замены; 2. Криптоанализ поточного шифра простой замены.
3	Блоковые шифры простой замены: 1. Шифр Плейфера; 2. Шифр Хилла.
4	Шифры гаммирования: 1. Шифр модульного гаммирования Виженера; 2. Шифр Вернама.
5	Надежность шифров: 1. Энтропия H языка, избыточность языка R; 2. Неопределенность шифра по ключу H(K|Y), неопределенность шифра по открытому тексту H(X|Y), формула Шеннона для неопределенности шифра по ключу; 3. Расстояние единственности; 4. Совершенные шифры, теорема Шеннона о совершенном шифре.
6	Стандарты шифрования: 1. Сеть Фейстеля; 2. Алгоритмы шифрования DES, ГОСТ 28147 - 89.
7	Поточные системы шифрования: 1. Принципы построения поточных шифр-систем; 2. Статистическое тестирование псевдослучайных последовательностей: тест 2-серий, тест на основе приращения энтропии, тест, основанный на алгоритме сжатия Лемпеля - Зива. 3. Псевдослучайные последовательности, линейный регистр сдвига с обратной связью. Минимальный характеристический многочлен, линейная сложность ЛРП, период ЛРП, ЛРП максимального периода. 4. Шифр-система A5; 5. Усложнение линейных рекуррентных последовательностей; 6. Генератор ANSI X9.17, BBS - алгоритм генерации псевдослучайных последовательностей.
8	Методы криптоанализа симметричных криптосистем: 1. Линейный криптоанализ Митсуру Матсуи.

3.2.3. Список теоретических вопросов для экзамена (8 семестр):

№ п/п	Формулировка вопроса
1	Алгоритм Диффи-Хеллмана. Задача Диффи-Хеллмана. Задача дискретного логарифмирования. Атаки: - использование в качестве g числа малого порядка - навязывание в качестве g^x (g^y) числа малого порядка - при малых значениях секретных ключей x; y навязывание малых значений g^y, g^x. Использование надежных простых чисел (safe prime). Уменьшение размера надежного простого числа.
2	Криптосистема RSA (шифрование, расшифрование, корректность). Задача RSA. Сведение задачи RSA к другим задачам (факторизации, дискретного логарифмирования, извлечения корней). Связь параметров системы p, q, φ(n), d.
3	Атаки на RSA: - малое значение открытого текста; - шифрование одного открытого текста на одинаковых малых открытых экспонентах; - частично известный открытый текст (линейное соотношение, произвольные соотношения); - метод повторного шифрования при малом порядке открытой экспоненты по модулю n (для расшифрования) либо по модулю p (для факторизации); - нахождение закрытого ключа другого пользователя при использовании одного основания n; - шифрование одного открытого текста на взаимно простых открытых экспонентах при использовании одного основания n; - нахождение φ(n) по d; - биты сообщения – взаимосвязь p(y), h(y), D(y); - использование одинаковых ключей для шифрования и цифровой подписи.
4	Алгоритмы факторизации: - метод пробных делений; - метод Ферма; - метод больших и малых шагов; - p - 1 – метод Полларда; - ρ – метод Полларда; - алгоритм Диксона.
5	Выбор параметров криптосистемы RSA. Генерация сильно простых чисел методом Гордона. Использование китайской теоремы об остатках в RSA.
6	Схема шифрования RSA-OAEP.
7	Криптосистемы с открытым ключом. - система Голдвассера-Микали; - рюкзачный метод шифрования Меркла-Хеллмана; - система Эль-Гамаля; - система Рабина; - система Мак-Элиса.
8	Алгоритмы дискретного логарифмирования: - метод больших и малых шагов; - ρ – метод Полларда; - индекс метод; - метод Полига Хеллмана.
9	Хеш-функции. Требования. Предназначение. Модель Меркле-Дамгарда. Функция губки (sponge function).
10	Стандарты хеш-функций.
11	Общая схема алгоритмов MD4, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94.
12	Криптоанализ хеш-функций. Модель случайного оракула (ROM). Атака на основе парадокса дней рождений:

	- ρ – метод Полларда; - λ – метод Полларда. Time-memory Trade-off: - метод Хеллмана; - радужные таблицы. Криптоанализ схемы Меркле-Дамгарда.
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 течение каждого семестра студентам необходимо выполнить проверочные работы, которые в случае безупречного выполнения оцениваются в 25 баллов.

В рамках зачета студентам предлагается 1 вопрос, оцениваемый в 20 баллов.

В рамках экзамена студентам предлагается 2 вопроса, каждый из которых оценивается в 25 баллов.

Сводная таблица рейтинга успеваемости (7 семестр)

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Проверочная работа №1,2	2x25=50
2	Зачет (теоретический вопрос)	20
	Итого	70

Сводная таблица рейтинга успеваемости (8 семестр)

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Проверочная работа №1,2	2x25=50
2	Экзамен (теоретический вопрос)	2x25=50
	Итого	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

4.2.1 Критерии оценивания теоретического вопроса для зачета

Максимальный балл за ответ на теоретический вопрос – 20 баллов.

Отлично/зачтено/ 17-20 баллов	**Хорошо/зачтено/ 13-16 баллов**	**Удовлетворительно/зачтено/ 9-12 баллов**	**Неудовлетворительно/незачтено/ 0-8 баллов**
Обучающийся отлично знает материал, понимает основы симметричной криптографии. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, понимает основы симметричной криптографии. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом, владеет базовыми знаниями симметричной криптографии. 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 теоретического вопроса для экзамена

Максимальный балл за ответ на теоретический вопрос – 25 баллов.

Отлично/зачтено/21-25 баллов	**Хорошо/зачтено/16-20 баллов**	**Удовлетворительно/зачтено/11-15 баллов**	**Неудовлетворительно/незачтено/0-10 балла**
Обучающийся отлично знает материал, понимает основы асимметричной криптографии. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, понимает основы асимметричной криптографии. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом, владеет базовыми знаниями асимметричной криптографии. 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

4.2.3. Критерии оценивания проверочных работы

Максимальный балл за работу – 25 баллов.

Оценка	**Отлично/зачтено**	**Хорошо/зачтено**	**Удовлетворительно/зачтено**	**Неудовлетворительно/не зачтено**
Баллы	**21-25 баллов**	**16-20 баллов**	**11-15 баллов**	**0-10 баллов**
Критерии	Проверочная работа выполнена правильно, в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу.	Выполнено 3/4 проверочной работы, обучающийся хорошо знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу, но допускает незначительные ошибки.	Выполнено 1/2 проверочной работы, либо работа сдана значительно позднее, чем предполагалось, при этом обучающийся знает материал, но допускает ошибки.	Работа не выполнена, либо обучающийся не может ответить на контрольные вопросы, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
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:

При подведении итогов зачета учитываются:

0 – 35 баллов – не зачтено;

36 – 70 баллов – зачтено.

При подведении итогов экзамена учитываются :

0 – 60 баллов – неудовлетворительно (2);

61 – 74 баллов – удовлетворительно (3);

75 – 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,
   - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, формулировать собственные выводы.
2. Средний уровень соответствует оценке «Хорошо»:
   - предполагает формирование компетенций на достаточном уровне,
   - студент способен давать развернутые ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Хорошо».
3. Базовый уровень соответствует оценке «Удовлетворительно»:
   - предполагает формирование компетенций на начальном уровне,
   - студент способен давать ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Удовлетворительно»,
   - студент способен отвечать на вопросы в закрытой форме. Количество правильных ответов – не менее 50%.
4. Низкий уровень соответствует оценке «Неудовлетворительно».

Специальность 10.05.01 Компьютерная безопасность
Специализация № 1 «Анализ безопасности компьютерных систем»
Фонд оценочных средств по дисциплине «Методы и средства криптографической защиты информации»
2025 год набора, очная форма обучения

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

Проректор по учебной работе	утверждено 24.02.25	А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета математического факультета	согласовано	Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 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