Фонд оценочных средств
для промежуточной аттестации
по дисциплине
Дополнительные главы криптографии

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: **Дополнительные главы криптографии**.
Семестр (семестры) изучения: 10 семестр.
Форма (формы) промежуточной аттестации: зачёт 10 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Дополнительные главы криптографии» 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**
ПК-3	Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	Знать: – роль эллиптических кривых в современных асимметричных шифрах; – формальные требования, предъявляемые к криптографическим эллиптическим кривым. Уметь: – анализировать криптографические эллиптические кривые на предмет их защищённости; – конструировать эллиптические кривые, обладающие заданными свойствами. Владеть: – навыками разработки и конфигурирования программно-аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых.

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.	ПК-3	Раздел 1. Основы	Контрольная работа	Теоретические вопросы к зачету
2.	ПК-3	Раздел 2. Эллиптические кривые над конечными полями	Контрольная работа	Теоретические вопросы к зачету
3.	ПК-3	Раздел 3. Криптосистемы на эллиптических кривых	Лабораторная работа №1	Теоретические вопросы к зачету
4.	ПК-3	Раздел 4. Атаки, связанные с операцией дискретного логарифмирования	Лабораторная работа №2	Теоретические вопросы к зачету
5.	ПК-3	Раздел 5. Криптосистемы, основанные на сопряжении Вейля	Лабораторная работа №3	Теоретические вопросы к зачету
6.	ПК-3	Раздел 6. Вспомогательные алгоритмы для криптографии на эллиптических кривых	Лабораторная работа №4	Теоретические вопросы к зачету

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. Задания контрольной работы:

№ п/п	Формулировка задания
1	Дана эллиптическая кривая $y^2 = x^3 - x + 1$ над R и точки P = (0, 1), Q = (1, 1), T = (3, 5), лежащие на данной кривой. Высчитать точку 2P + 3Q - T.
2	Дана эллиптическая кривая $y^2 = x^3 - x + 1$ над Z_{11}. Построить таблицу Кэли для группы точек этой кривой.
3	Дана эллиптическая кривая $y^2 = x^3 - x + 1$ над Z_{13}. Определить какой абелевой группе изоморфна группа точек этой кривой.
4	Продемонстрировать на примере кривой $y^2 = x^3 - x + 1$ над Z_{13} полный цикл генерации общего ключа по протоколу Диффи-Хеллмана для эллиптических кривых.
5	Продемонстрировать на примере кривой $y^2 = x^3 - x + 1$ над Z_{13} работу алгоритма ECDSA.

3.2.2. Список лабораторных работ:

№ п/п	Формулировка задания
1	Написать программу, реализующую алгоритм Шуфа.
2	Написать программу, реализующую алгоритмы: Полига-Хеллмана, "Baby step - giant step", Ро-алгоритм Полларда, Лямбда-алгоритм Полларда.
3	Написать программу, реализующую алгоритм ECDSA.
4	Написать программу, реализующую криптосистему Эль-Гамаля, реализовать две различные атаки на эту криптосистему.

3.2.3. Список теоретических вопросов к зачету:

№ п/п	Формулировка вопроса
1	Что есть криптография на эллиптических кривых?
2	Группа точек эллиптической кривой (определение операции и свойства).
3	Определение и примеры изоморфизмов эллиптических кривых. j-инвариант
4	Эндоморфизмы, степень, отделимость. Примеры эндоморфизмов. Точки кручения. Полиномы деления.
5	Теорема Хассе. Алгоритм Шуфа и его модификации.
6	Криптосистема Эль-Гамаля и атаки на неё. Определение цифровой подписи на эллиптической кривой. Идентификация и подпись Шнорра. Безопасность подписи Шнорра. Алгоритм ECDSA.
7	Алгоритм Полига-Хеллмана. Алгоритм "Baby step - giant step". Ро-алгоритм Полларда. Лямбда-алгоритм Полларда.
8	Гомоморфное шифрование (определение и обзор гомоморфных криптосистем).

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

В течение семестра студентам необходимо выполнить контрольную работу, которая в случае безупречного выполнения оценивается в 30 баллов.

Также в течение семестра выполняется три лабораторные работы, каждая из которых оценивается в 10 баллов.

Кроме того, в рамках зачета студентам предлагается 2 вопроса, каждый из которых оценивается в 10 баллов.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Контрольная работа	30
2	Лабораторная работа №1-4	4x10=40
3	Зачет (теоретический вопрос)	2x10=20
	Итого	90

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания теоретического вопроса зачета и лабораторной работы

Максимальный балл за ответ на теоретический вопрос и за одну лабораторную работу – 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 грамотно сформулировать доказательство.	Обучающийся хорошо знает материал, умеет анализировать проблему, но допускает ошибки в доказательствах.	Обучающийся знаком с материалом, но 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 задания контрольной работы

Максимальный балл за работу – 30 баллов.

Максимальный балл за задание – 6 баллов.

Оценка	**Отлично/ зачтено**	**Хорошо/ зачтено**	**Удовлетворительно /зачтено**	**Неудовлетворительно/ не зачтено**
Баллы	**6 баллов**	**4-5 балла**	**3 балла**	**0-2 балла**
Критерии	Задание выполнено в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно сформулировать доказательство.	Задание выполнено в срок, обучающийся хорошо знает материал, умеет анализировать проблему, но допускает ошибки в доказательствах.	Задание выполнено и сдано позднее, чем предполагалось, либо обучающийся допускает фактические ошибки.	Задание не выполнено, 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:

0 – 59 баллов – не зачтено;

60 – 90 баллов – зачтено.

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 «Дополнительные главы криптографии»
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