

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»

Уфимский филиал Финуниверситета

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Основы криптографии»

Разработчик: кафедра «Математика и информатика»

Направления подготовки: 09.03.03 Прикладная информатика

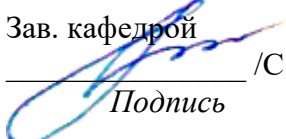
Образовательная программа: Прикладная информатика

Профиль: ИТ-сервисы и технологии обработки данных в экономике и финансах

Форма образования: заочная

РАССМОТРЕН
На заседании кафедры
«Математика и информатика»

Протокол № 12
от « 30 » июня 2023 г.

Зав. кафедрой

_____/С.А. Фархиева
Подпись

Разработан на основе

*ОС ФГОС ВО по направлению подготовки
09.03.03 Прикладная информатика
(уровень бакалавриата)
№ 922 от 19.09.2017 г.*

Паспорт фонда оценочных средств

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины Основы криптографии.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля и промежуточной аттестации.

1 Описание показателей и критериев оценивания компетенций

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство ¹
	«неудовлетворительно» минимальный не достигнут	«удовлетворительно» минимальный пороговый	«хорошо» средний	«отлично» высокий	
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий с учетом основных требований информационной безопасности.					
Индикатор 1. Использует информационно-коммуникационные технологии и библиографические источники при поиске информации, для решения стандартных задач.					
<u>Знать:</u> методы и инструменты информационно-коммуникационных технологий для эффективного поиска и использования библиографических источников в области криптографии.	Не знает эффективных методов и инструментов информационного поиска и использования библиографических источников с использованием информационно-коммуникационных технологий.	Должен знать основы использования информационно-коммуникационных технологий и библиографических ресурсов для поиска информации в сфере криптографии.	Должен знать базовые принципы и методы информационного поиска и использования библиографических источников через информационно-коммуникационные технологии в контексте информационной безопасности.	Должен знать передовые методы информационного поиска и использования библиографических источников в сочетании с современными информационно-коммуникационными технологиями для решения сложных задач в области информационной безопасности.	Тестовые задания, вопросы для устного/письменного опроса, задания в виде расчетных задач
<u>Уметь:</u> применять эти технологии для получения, анализа и использования специализированной информации при решении задач в сфере информационной безопасности.	Не умеет находить необходимую информацию для решения базовых задач в области криптографии и информационной безопасности.	Должен уметь находить базовую информацию, необходимую для выполнения стандартных задач по информационной безопасности.	Должен уметь искать и применять соответствующую информацию для решения конкретных криптографических задач..	Должен уметь эффективно находить, анализировать и применять специализированную информацию для разработки и реализации комплексных криптографи-	Тестовые задания, вопросы для устного/письменного опроса, задания в виде расчетных задач

¹ Виды оценочных средств: *тестовые задания, вопросы для устного/письменного опроса, задания в виде расчетных задач, мини-кейсы, ситуационные задачи, практико-ориентированные задания.*

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство ¹
	«неудовлетворительно» минимальный не достигнут	«удовлетворительно» минимальный пороговый	«хорошо» средний	«отлично» высокий	
				ческих решений.	
Индикатор 2. Демонстрирует умение решать стандартные задачи разработки информационных систем.					
<u>Знать:</u> основные принципы и методы криптографической защиты данных, применяемые при разработке информационных систем.	Не знает основных принципов разработки информационных систем и применения криптографии для обеспечения информационной безопасности.	Должен знать базовые аспекты разработки информационных систем и использования криптографии для защиты данных.	Должен знать основные принципы и подходы к разработке информационных систем с использованием стандартных криптографических средств безопасности.	Должен знать современные методологии и инструменты разработки информационных систем, включая применение криптографических технологий для обеспечения их безопасности.	Тестовые задания, вопросы для устного/письменного опроса, задания в виде расчетных задач
<u>Уметь:</u> интегрировать криптографические алгоритмы и протоколы для обеспечения безопасности данных и транзакций в разрабатываемых информационных системах.	Не умеет адекватно задействовать доступные методы и инструменты при создании информационных систем.	Должен уметь применять стандартные инструменты для создания и обеспечения минимальной безопасности информационных систем.	Должен уметь реализовывать функционально-полные информационные системы, соответствующие базовым требованиям безопасности.	Должен уметь самостоятельно проектировать, разрабатывать и внедрять комплексные информационные системы с высоким уровнем защищенности.	Тестовые задания, вопросы для устного/письменного опроса, задания в виде расчетных задач
Индикатор 3. Владеет навыками обеспечения информационной безопасности автоматизированных систем.					
<u>Знать:</u> основные криптографические алгоритмы и принципы обеспечения информационной безопасности автоматизированных систем и основ криптографии.	Не знает ключевых основ обеспечения информационной безопасности автоматизированных систем и основ криптографии.	Должен знать базовые принципы обеспечения информационной безопасности и некоторые криптографические методы защиты данных в автоматизированных системах.	Должен знать основные концепции и методы обеспечения информационной безопасности автоматизированных систем, включая основные криптографические механизмы.	Должен знать передовые принципы и методы обеспечения информационной безопасности, в том числе криптографические методы защиты данных автоматизированных систем.	Тестовые задания, вопросы для устного/письменного опроса, задания в виде расчетных задач
<u>Уметь:</u> адаптировать и применять эти алгоритмы для защиты информации в различных информационных системах.	Не умеет адекватно применять знания для защиты информации в рамках автоматизированных систем.	Должен уметь использовать типовые средства и методы для решения стандартных задач обеспечения безопасности информации.	Должен уметь применять стандартные методы и инструменты для защиты информации в автоматизированных системах.	Должен уметь разрабатывать и реализовывать комплексные стратегии обеспечения информационной безопасности, адаптиро-	Тестовые задания, вопросы для устного/письменного опроса, задания в виде расчетных задач

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство ¹
	«неудовлетворительно» минимальный не достигнут	«удовлетворительно» минимальный пороговый	«хорошо» средний	«отлично» высокий	
				ванные под специфические требования различных автоматизированных систем.	

2. Оценочные средства для оценки сформированности компетенций (контроль остаточных знаний)

Примеры тестовых заданий

Тесты (ОПК-3)

Вопрос 1. (ОПК-3) Укажите верно, как называется процесс поиска и исправления ошибок в программном коде

- (1) Debugging (Отладка)
- (2) Refactoring (Рефакторинг)
- (3) Patching (Патчинг)
- (4) Compiling (Компиляция)

Вопрос 2. (ОПК-3) Свойство информации, предотвращающее ее неавторизованное изменение или разрушение называется

Вопрос 3. (ОПК-3) Советский и Российский стандарт симметричного шифрования, введенный в 1990 году

- (1) ГОСТ 3344-2006
- (2) ГОСТ 21874-98
- (3) ГОСТ 28147-89
- (4) ГОСТ 11345-91

Вопрос 4. (ОПК-3) Отношение эквивалентности не обладает свойством

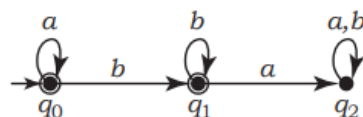
- (1) рефлексивность
- (2) симметричность
- (3) антисимметричность
- (4) транзитивность

Вопрос 5. (ОПК-3) На рисунке ниже приведена таблица истинности булевых функций двух аргументов. Под каким обозначением находится функция с названием «штрих Шеффера»?

		0	·	\rightarrow'	x	\leftarrow'	y	+	\vee	\downarrow	\leftrightarrow	y'	\leftarrow	x'	\rightarrow		1
x	y	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

- (1) g_1
- (2) g_{14}
- (3) g_8
- (4) g_2

Вопрос 6. (ОПК-3) Какой язык распознает конечный автомат



- (1) ab^*
- (2) a^*b^*
- (3) ba
- (4) b^*a

Вопрос 7. (ОПК-3) Что не относится к вероятностным моделям источников открытых сообщений?

- (1) Стационарный источник независимых символов алфавита
- (2) Стационарный источник независимых биграмм
- (3) Стационарная модель полужависимых конечных грамматик
- (4) Стационарный источник марковски зависимых букв

Вопрос 8. (ОПК-3) Какой из свойств не относится к поточным методам шифрования

- (1) Передача гаммы в линию связи
- (2) Кодирование гаммы симметричным ключом до отправки в канал
- (3) Повторное использование гаммы
- (4) Восстановление текста, зашифрованного неравновероятной гаммой

Вопрос 9. (ОПК-3) Какой из пунктов не имеет отношения к режимам использования блочных шифров?

- (1) режим асимметричной открытой замены
- (2) с зацеплением блоков шифротекста;
- (3) с обратной связью по выходу;
- (4) с обратной связью по выходу и нелинейной функцией

Вопрос 10. (ОПК-3) Схема шифрования Эль-Гамала – это...

- (1) поточный шифр
- (2) блочный шифр в режиме шифрования с зацеплением
- (3) синхронный поточный шифр
- (4) криптосистема с открытым ключом

Вопрос 11. (ОПК-3) В число единиц криптостойкости не входит...

- (1) временная сложность наилучшего известного алгоритма, нарушающего безопасность
- (2) требуемый объем памяти для вскрытия ключа
- (3) сложность генератора ключа
- (4) физический объем вычислительной модели для вскрытия ключа

Вопрос 12. (ОПК-3) Что такое алгоритм, используемый для кодирования информации?

Вопрос 13. (ОПК-3) Как называется метод криптографии, при котором используется один ключ для шифрования и расшифрования данных?

Вопрос 14. (ОПК-3) Какой термин обозначает характеристику системы шифрования, означающую то, насколько сложно взломать шифр и получить доступ к зашифрованным данным без ключа?

Вопрос 15. (ОПК-3) Какой вид шифрования основан на использовании двух ключей: публичного и приватного?

Ключ к тесту

Вопрос	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ответ	4	целостность	3	3	2	2	3	2	1	4	3	Шифр	Симметричный	Стойкость	Асимметричный
Баллы	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

3 Методические материалы, определяющие процедуры оценивания знаний и умений, характеризующих степень сформированности компетенций

Критерии оценки знаний при проведении устного/письменного опроса

Оценка «**отлично**» (зачтено) – выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания вопросов дисциплины.

Оценка «**хорошо**» (зачтено) – выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, но допускает в ответе некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «**удовлетворительно**» (зачтено) – выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными понятиями, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «**неудовлетворительно**» (не зачтено) – выставляется обучающемуся, который не знает большей части основного содержания вопросов тем дисциплины, допускает грубые ошибки в формулировках основных понятий.

Критерии оценки знаний при решении задач

Оценка «**отлично**» (зачтено) – выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания вопросов дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «**хорошо**» (зачтено) – выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе некоторые не-

точности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка **«удовлетворительно»** (зачтено) – выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными понятиями, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка **«неудовлетворительно»** (не зачтено) – выставляется обучающемуся, который не знает большей части основного содержания вопросов тем дисциплины, допускает грубые ошибки в формулировках основных понятий, не умеет использовать полученные знания при решении типовых практических задач.

Критерии оценки знаний при проведении тестирования

Оценка **«отлично»** (зачтено) выставляется при условии правильного ответа студента не менее чем на 85 % тестовых заданий;

Оценка **«хорошо»** (зачтено) выставляется при условии правильного ответа студента не менее чем на 70 % тестовых заданий;

Оценка **«удовлетворительно»** (зачтено) выставляется при условии правильного ответа студента не менее чем на 51 %;

Оценка **«неудовлетворительно»** (не зачтено) выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.