

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

Уфимский филиал Финуниверситета

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
«КРИПТОГРАФИЯ И РАСПРЕДЕЛЕННЫЕ РЕЕСТРЫ»

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 № 11
от « 30 » июня 2021 г.

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

Зав. кафедрой

_____/С.А. Фархиева
Подпись

1. Цель, задачи и результаты изучения дисциплины

Цель: овладение студентами общими принципами и современными методами криптографии и распределенных реестров.

Задачи дисциплины:

- освоение студентами базовых знаний в области криптографии;
- приобретение теоретических знаний и практических умений и навыков в области криптографии;
- накопление опыта осуществления будущей профессиональной деятельности.

Перечень планируемых результатов изучения дисциплины

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (знания и умения) соотнесенные с компетенциями/индикаторам и достижения компетенций
ПКП-3	Способность применять методы разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем	1. Демонстрирует знание назначения и функционал типовых модулей корпоративных информационных систем, основные методы разработки приложений на их платформе.	Знать: назначение и функционал типовых модулей корпоративных информационных систем в сфере экономики и финансов Уметь: применять методы разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем
		2. Владеет методологией разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем	Знать: методологию разработки приложений в сфере экономики и финансов на платформе корпоративных информационных систем Уметь: разрабатывать приложения в сфере экономики и финансов на платформе корпоративных информационных систем.

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

Примеры тестовых заданий

1. Шифрование – это...

Варианты ответов:

1. совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
2. удобная среда для вычисления конечного пользователя
3. способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

2. Кодирование – это...

Варианты ответов:

1. написание программы
2. преобразование
3. преобразование обычного, понятного текста в код

3. Что требуется для восстановления зашифрованного текста

Варианты ответов:

1. матрица
2. ключ
3. вектор

4. Когда появилось шифрование

Варианты ответов:

1. четыре тысячи лет назад
2. пять тысяч лет назад
3. две тысячи лет назад

5. Первым известным применением шифра считается

Варианты ответов:

1. египетский текст
2. русский
3. нет правильного ответа

6. Алфавит – это...

Варианты ответов:

1. конечное множество используемых для кодирования информации знаков
2. буквы текста
3. нет правильного ответа

7. Текст – это...

Варианты ответов:

1. все правильные
2. упорядоченный набор из элементов алфавита
3. конечное множество используемых для кодирования информации знаков

8. Шифрование – это...

Варианты ответов:

1. преобразовательный процесс исходного текста в зашифрованный
2. упорядоченный набор из элементов алфавита
3. нет правильного ответа

9. Дешифрование – это...

Варианты ответов:

1. на основе ключа шифрованный текст преобразуется в исходный
2. сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере
3. пароли для доступа к сетевым ресурсам

10. Пространство ключей k – это...

Варианты ответов:

1. длина ключа
2. нет правильного ответа
3. набор возможных значений ключа

11. Как называется метод шифрования, который использует один и тот же ключ для шифрования и дешифрования данных?
12. Какое слово описывает тип алгоритма, который генерирует публичный и приватный ключи для шифрования и дешифрования сообщений?
13. Как называется процесс выполнения сложных математических задач, который используется для подтверждения транзакций в блокчейне?
14. Какое одно слово описывает запись, которая не может быть изменена или удалена после того, как была записана в блокчейн?
15. Как называется сеть, в которой все участники имеют доступ к одной и той же информации в распределенном реестре и могут проводить транзакции непосредственно друг с другом?

Ключи к тестам

Вопрос	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ответ	3	3	2	1	1	1	2	1	1	3	Симметричное	Асимметричное	Майнинг	Неизменяемость	Децентрализованная
Баллы	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

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 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, 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.