МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Информационной безопасности

|  |  |  |
| --- | --- | --- |
| СОГЛАСОВАНОДекан факультетавычислительной техники\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Н. Пылькин«\_\_\_»\_\_\_\_\_\_\_\_\_201\_\_ г. |  | УТВЕРЖДАЮПроректорпо учебной работе\_\_\_\_\_\_\_\_\_\_\_\_\_ К.В. Бухенский«\_\_\_»\_\_\_\_\_\_\_\_\_201\_\_ г. |
| Руководитель ОПОП\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Н. Пржегорлинский«\_\_\_»\_\_\_\_\_\_\_\_\_201\_\_ г. |  |  |

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

дисциплины

**«****Теоретико-числовые метолы в криптографии» (****Б1.3.Б13)**

Направление подготовки — 10.00.00 «Информационная безопасность»

Специальности 10.05.01 — Компьютерная безопасность

Направленность (профиль) подготовки:

Специализация № 8 — Информационная безопасность объектов

информатизации на базе компьютерных систем

ОПОП — «Компьютерная безопасность»

Квалификация выпускника — специалист

Форма обучения — очная

Срок обучения — 5,5 лет

Рязань 2018 г.

# Общие положения

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур, оцениваемых ресурсов в дистанционных учебных курсах), предназначенных для оценки качества освоения обучающимися дисциплины «Теоретико-числовые метолы в криптографии» как части основной образовательной программы.

## **Назначение**

Цель – оценить соответствие знаний, умений и уровня приобретённых компетенций, обучающихся целям и требованиям основной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний, обучающихся проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся: на занятиях; по результатам выполнения контрольных работ; по результатам выполнения обучающимися типовых расчётов; по результатам проверки качества конспектов лекций и иных материалов. При оценивании (определении) результатов освоения дисциплины применяется традиционная шкала оценивания («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

Текущая аттестация студентов проводится на основании результатов выполнения ими типовых расчётов (ТР) и контрольных работ (КР).

По итогам изучения разделов дисциплины «Теоретико-числовые метолы в криптографии», обучающиеся в конце каждого учебного семестра, проходят промежуточную аттестации. Форма проведения аттестации – экзамен в устной, письменной формах или тест: электронный билет, формируемый случайным способом. Экзаменационные билеты и перечни вопросов, задач, примеров, выносимых на промежуточную аттестацию, составляются с учётом содержания тем учебной дисциплины и подписываются заведующим кафедрой.

В экзаменационный билет или вариант теста включаются два теоретических вопроса и до четырёх практических задач по темам дисциплины (Протокол заседания кафедры ИБ №10 от 26 апреля 2017г.).

## **Паспорт оценочных материалов по дисциплине**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Контролируемые модули (темы) дисциплины (результаты по разделам) | Код контролируемой компетенции (или её части) | Вид, метод, форма оценочного мероприятия |
| **Семестр 6** |
| 1.1. | Основные алгоритмы  | ОПК–2 | Экзамен |
| 1.2. | Простые числа. Факторизация  | ОПК–2 | Контрольная работа, экзамен |
| 1.3. | Арифметика остатков  | ОПК–2 | Типовой расчет, экзамен |
| 1.4. | Псевдопростые числа  | ОПК–2 | Типовой расчет, контрольная работа, экзамен |
| 1.5. | Системы сравнения  | ОПК–2 | Типовой расчет, экзамен |
| **Семестр 7** |
| 2.1. | Группы  | ОПК–2 | Зачет |
| 2.2. | Тесты на простоту | ОПК–2 | Типовой расчет, зачет |
| 2.3. | Система шифрования RSA  | ОПК–2 | Типовой расчет, зачет |

## Критерии оценивания компетенций (результатов)

1) Уровень усвоения материала, предусмотренного программой.

2) Умение анализировать материал, устанавливать причинно-следственные связи.

3) Качество ответа на вопросы: полнота, аргументированность, убежденность, логичность.

4) Содержательная сторона и качество материалов, приведенных в отчетах студента по типовым расчетам, практическим занятиям.

5) Использование дополнительной литературы при подготовке ответов.

Уровень освоения сформированности знаний, умений и навыков по дисциплине оценивается в форме бальной отметки. Критерии оценивания промежуточной аттестации представлены в таблице.

|  |  |  |
| --- | --- | --- |
| **Четырёхбальная шкала оценивания** | **Двухбалльная шкала оценивания** | **Критерии оценивания** |
| **«отлично»** | **«зачтено»** | **студент должен**: продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; уметь сделать выводы по излагаемому материалу; безупречно ответить не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой;  |
| **«хорошо»** | **«зачтено»** | **студент должен:** продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; уметь сделать достаточно обоснованные выводы по излагаемому материалу; ответить на все вопросы билета; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой, при этом возможно допустить непринципиальные ошибки. |
| **«удовлетворительно»** | **«зачтено»** | **студент должен:** продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины; уметь устранить допущенные погрешности в ответе на теоретические вопросы и/или при выполнении практических заданий под руководством преподавателя, либо (при неправильном выполнении практического задания) по указанию преподавателя выполнить другие практические задания того же раздела дисциплины. |
| **«неудовлетворительно»** | **«не зачтено»** | **ставится в случае:** незнания значительной части программного материала; не владения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу. Оценка «неудовлетворительно» («незачтено») выставляется также, если студент после начала экзамена отказался его сдавать или нарушил правила сдачи экзамена (списывал, подсказывал, обманом пытался получить более высокую оценку и т.д.).  |

## Фонд оценочных средств дисциплины «Теоретико-числовые метолы в криптографии» включает

– задачи для практических занятий;

– варианты контрольных работ;

– варианты типовых расчётов;

– оценочные средства промежуточной аттестации;

– варианты тестовых заданий в дистанционных учебных курсах;

– задачи для проверки остаточных знаний.

### Задачи для практических занятий

В ходе практических занятий происходит решение задач, представленных в сборниках задач для практических занятий и самостоятельной работы, доступны для скачивания в электронном виде.

1. Кащеев, А.А. Основы криптографии: метод. указ. к самост. работам и практ. занятиям / А. А. Кащеев, В. Т. Дмитриев; РГРТУ. - Рязань, 2010. - 32с. - Библиогр.: с.31-32(6 назв.).
2. Кукина Е.Г. Введение в криптографию [Электронный ресурс]: сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. — 91 c. — 978-5-7779-1588-7. — Режим доступа: <http://www.iprbookshop.ru/24876.html>

### Варианты контрольных работ.

Текущая проверка знаний, умений и навыков предусматривает в течение каждого семестра периодические опросы и выполнение контрольных работ на практических занятиях. Типовые контрольные работы реализуется в виде типовых вариантов контрольных работ по отдельным темам, которые выполняются студентами в аудиториях. Контрольные опросы производятся на основании соответствующих типовых вопросов промежуточной аттестации. Пример варианта контрольной работы приведен ниже.

|  |
| --- |
| Вариант 011. Вычислить НОД(a,b) двумя способами: алгоритмом Евклида с делением с остатком и бинарным алгоритмом Евклида. Сравнить количество итераций для этих алгоритмов. а) a=18, b=35; б) a=329, b=826; в) a=26, b=738; г) a=288, b=15.2. Определить, являются ли числа a, b, c взаимно простыми? Попарно простыми? а) a=13, b=17, c=15; б) a=105, b=91, c=26; в) a=22, b=121, c=209.3. Вычислить функцию Эйлера от следующих чисел: а) 13; б) 17; в) 9; г) 16; д) 6; е) 24; ж) 227; з) 725; и) 94836.4. Пользуясь асимптотическим законом распределения простых чисел, вычислить примерное количество простых чисел в промежутке от 2 000 до 10 000. |

### Варианты типовых расчётов.

В процессе изучения каждой темы студенты обязаны самостоятельно выполнить типовые расчёты по отдельным темам.

Типовые расчёты реализуется в виде типовых вариантов расчётных заданий по отдельным темам, которые выполняются студентами самостоятельно во внеаудиторное время. Контрольные опросы при защите типового расчёта производятся на основании соответствующих типовых вопросов промежуточной аттестации.

Все задания типовых расчетов представлены в электронном виде и доступны для скачивания. URL: http://cdo.rsreu.ru/course/view.php?id=1584. Пример задач варианта типового расчёта приведён ниже.



### Оценочные средства промежуточной аттестации

Фонд оценочных средств промежуточной аттестации, проводимой в форме экзамена или теста, включает

1. типовые теоретические вопросы;
2. дополнительные вопросы;
3. типовые практические задачи.

Оценочные средства приведены ниже для каждого из семестров обучения. Разрешается и иная формулировка вопроса или примера, без изменения его смысла или содержания, например, дробление, изменение условий или иное. На промежуточной аттестации разрешается использовать таблицы интегралов, распределений и калькуляторы.

### Примеры типовых теоретических вопросов (уровень усвоения хорошо и отлично)

Семестр 6

1. Алгоритм деления.
2. Теорема деления.
3. Алгоритм Евклида. Доказательство истинности алгоритма Евклида.
4. Расширенный алгоритм Евклида.
5. Теорема разложения целого числа на множители. Существование разложения целого числа в произведение.
6. Эффективность алгоритма разложения методом проб. Единственность разложения целого числа.
7. Алгоритм Ферма разложения на множители. Доказательство корректности алгоритма Ферма.
8. Фундаментальное свойство простых чисел.
9. Полиномиальные формулы.
10. Числа Мерсенна.
11. Числа Ферма.
12. Теорема о бесконечности множества простых чисел.
13. Решето Эратосфена.
14. Сравнения.
15. Арифметика остатков.
16. Китайская теорема остатков
17. Критерии делимости.
18. Степени.
19. Диофантовы уравнения.
20. Деление по модулю.

Семестр 7

1. Определение группы. Её свойства
2. Арифметические группы
3. Подгруппы. Теорема Лагранжа
4. Циклические подгруппы
5. Теорема Эйлера
6. Числа Мерсенна
7. Числа Ферма
8. Метод Ферма
9. Метод Эйлера
10. Тест Люка –Лемера
11. Теста Люка
12. Тест Брилхарта
13. Числа Кармайкла
14. Примитивные корни
15. Вычисление порядка элемента
16. Система шифрования RSA

### Примеры типовых теоретических вопросов (уровень усвоения удовлетворительно)

1. Алгоритм деления.
2. Алгоритм Евклида.
3. Алгоритм Ферма разложения на множители.
4. Фундаментальное свойство простых чисел.
5. Решето Эратосфена.
6. Китайская теорема остатков.
7. Степени.
8. Диофантовы уравнения.

Семестр 7

1. Теорема Лагранжа
2. Циклические подгруппы
3. Теорема Эйлера
4. Метод Ферма
5. Метод Эйлера
6. Вычисление порядка элемента
7. Система шифрования RSA

### Примеры типовых задач (уровень усвоения удовлетворительно)



### Варианты тестовых заданий в дистанционных учебных курсах

Текущий контроль знаний студентов в может проводится в виде компьютерного тестирования по различным модулям (темам) дисциплины. Компьютерные тесты представлены в дистанционных учебных курсах на базе системы управления обучением Moodle: <http://cdo.rsreu.ru/>. Доступ к курсам предоставляется по паролю из внутренней информационной системы организации и из глобальной сети Интернет.

1. Дистанционный учебный курс «**Теоретико-числовые метолы в криптографии**» [Электронный ресурс]: Система дистанционного обучения РГРТУ: – Режим доступа: http://cdo.rsreu.ru/course/view.php?id=1584. Получено положительное экспертное заключение № 42 от 18.01.16, свидетельство о регистрации ОФЭРНиО № 20187 от 10.06.2014.

При создании тематических тестов по теории вероятностей и математической статистике использовались следующие типы вопросов:

1. множественный выбор – необходимо выбрать один или несколько верный ответов среди предложенных,
2. числовой ответ – необходимо впечатать числовой ответ с клавиатуры,
3. на соответствие – ответ на каждый из вопросов нужно выбрать из предложенного списка,
4. краткий ответ – необходимо впечатать одно или несколько «слов» (это могут быть как собственно слова, так и наборы определенных символов),
5. вычисляемый – необходимо ввести числовой ответ с клавиатуры.

Примеры тестовых заданий представлены ниже.



Внутри каждого раздела сформирован обширный банк разнообразных вопросов, которые разбиты на категории. Каждая категория содержит однотипные задачи, объединенные одним учебным вопросом, например, вычисление остатков, неполных частных, разложения на множители и т.д. Тест формируется на основе выбора случайного вопроса из каждой указанной категории.

### Задачи для проверки остаточных знаний

При проверке остаточных знаний студентам разрешается использовать конспекты лекций, справочную литературу и калькуляторы. Примеры типовых задач для проверки остаточных знаний

1. С помощью расширенного алгоритма Эвклида найти решение уравнения $2425500α+1732500β=НОД(2425500,1732500)$. В качестве ответа указать сумму найденных неизвестных $α+β$.
2. Найти $НОД(134380878125,494284375)$
3. В результате применения алгоритма деления числа $17608$ на число $1203$ на 10-ом цикле алгоритма остаток (переменная $R$) примет значение
4. Найти вычет натурального числа $1079125^{390}$ по модулю $79$
5. Найти вычет натурального числа $118937700^{473}⋅6364800^{172}$ по модулю $43$
6. Найти все решения линейного уравнения $40⋅x≡95(mod 17)$ на множестве $Z\_{17}$
7. Найти решение системы уравнений $\left\{\begin{matrix}x=5 mod 7,\\x=3 mod 5.\end{matrix}\right.$ в $Z$.

Фонд оценочных средств входит в состав рабочей программы дисциплины «Теоретико-числовые метолы в криптографии» (Б1.3.Б13) ОПОП «Компьютерная безопасность», направление подготовки - 10.00.00 «Информационная безопасность», специальности 10.05.01 - «Компьютерная безопасность», направленность (профиль) подготовки: специализация № 8 — Информационная безопасность объектов информатизации на базе компьютерных систем

|  |  |  |
| --- | --- | --- |
| Составил:к.ф.-м.н., доцент каф. ИБ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | (Ильин М.Е.) |
| Заведующий кафедрой ИБ,ктн, доцент | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | (Пржегорлинский В.Н.) |