Министерство образования и науки Российской
Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

Рязанский государственный радиотехнический
университет

Факультет вычислительной техники

Кафедра «Информационной безопасности»

|  |  |  |
| --- | --- | --- |
| СОГЛАСОВАНОДекан факультета вычислительной техники\_\_\_\_\_\_\_\_\_\_\_\_ А.Н. Пылькин«\_\_\_»\_\_\_\_\_\_\_\_\_201\_\_ г. |  | УТВЕРЖДАЮПроректор по учебной работе\_\_\_\_\_\_\_\_\_\_ К.В. Бухенский«\_\_\_»\_\_\_\_\_\_\_\_\_201\_\_ г. |
| Руководитель ОПОП\_\_\_\_\_\_\_\_\_\_\_\_ В.Н. Пржегорлинский «\_\_\_»\_\_\_\_\_\_\_\_\_201\_\_ г. |  |

**РАБОЧАЯ ПРОГРАММА**

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.

# Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательных программ специалитета

Рабочая программа по дисциплине «Теоретико-числовые метолы в криптографии» является составной частью основной профессиональной образовательной программы по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), разработанной в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденным приказом Минобрнауки России от 01.12.2016 г. № 1512

## Цель изучения дисциплины

1) приобретение базовых знаний и умений в соответствии с Федеральным государственным образовательным стандартом;

2) формирование у студентов способности к логическому мышлению, анализу и восприятию информации, воспитание математической культуры, посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.

## Задачи дисциплины «Теоретико-числовые метолы в криптографии»

– обучение базовым математическим методам, необходимым для анализа и моделирования устройств, процессов и явлений при поиске оптимальных решений;

– обучение методам обработки и анализа результатов численных экспериментов.

Дисциплина «Теоретико-числовые метолы в криптографии» направлена на формирование общекультурных и общепрофессиональных компетенций в соответствии с учебным планом. Выпускник должен обладать следующими компетенциями, приобретаемыми в процесс изучения дисциплины «Теоретико-числовые метолы в криптографии».

|  |  |
| --- | --- |
| Коды компетенции | Содержание компетенций |
| ОПК-2 | Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов |

## Перечень планируемых результатов обучения по дисциплине

В результате изучения дисциплины «Теоретико-числовые метолы в криптографии» студент должен

|  |  |
| --- | --- |
| **Компетенции** | **Перечень планируемых результатов обучения по дисциплине** |
| ОПК – 2 | Знать способы корректного применения при решении профессиональных задач аппарата математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методовУметь корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методовВладеть способами корректного применения при решении профессиональных задач аппарата математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов. |

# Место дисциплины в структуре ОПОП специалитета

Дисциплина «Теоретико-числовые метолы в криптографии» относится к базовой части блока №1 (Б1.3.Б13) основной профессиональной образовательной программы подготовки специалистов направления 10.05.01 «Компьютерная безопасность» направленности «Информационная безопасность объектов информатизации на базе компьютерных систем»

До начала изучения учебной дисциплины обучающиеся должны знать основные методы геометрии, алгебры и начала анализа в рамках программы средней школы.

Дисциплина «Теоретико-числовые метолы в криптографии» является основой для дальнейшего изучения дисциплин профессионального цикла и подготовки выпускной работы.

# Объём дисциплины в зачётных единицах с указанием академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетные единицы (ЗЕ), 144 часа.

Форма обучения - очная

|  |  |  |
| --- | --- | --- |
| Вид занятий | Всего ЗЕ/час. | Семестры |
| 6 | 7 |
| Общая трудоёмкость | 144/4 | 90/2.5 | 54/1.5 |
| Аудиторные занятия (всего). В том числе | 48 | 32 | 16 |
|  Лекции | 32 | 16 | 16 |
|  Практические занятия | 16 | 16 | - |
| Самостоятельная работа (всего). В том числе | 96 | 58 | 38 |
|  Самостоятельные занятия | 50 | 15 | 35 |
|  Консультации в семестре | 6 | 3 | 3 |
|  Промежуточная аттестация: экзамен/зачёт | 40 | 40 | - |

# Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

В структурном отношении программа представлена следующими разделами:

**Модуль 1**

**Раздел 1.1.** основные алгоритмы.

**Раздел 1.2.** Простые числа. Факторизация.

**Раздел 1.3.** Арифметика остатков.

**Раздел 1.4.** Псевдопростые числа.

**Раздел 1.5.** Системы сравнения.

**Модуль 2**

**Раздел 2.1.** Группы.

**Раздел 2.2.** Тесты на простоту.

**Раздел 2.3.** Система шифрования RSA.

## Содержание дисциплины, структурированное по темам (разделам)

|  |
| --- |
| **Модуль 1** |
| **Раздел модуля** | **Содержание** |
| 1.1. Основные алгоритмы | Введение. Алгоритм деления. Теорема деления. Алгоритм Евклида. |
| 1.2. Простые числа. Факторизация  | Факторизация. Теорема о разложении. Метод проб. Алгоритм Ферма. Фундаментальное свойство простых чисел. Полиномиальная формула. Числа Мерсенна. Числа Ферма. Решето Эратосфена.  |
| 1.3. Арифметика остатков | Отношение эквивалентности. Сравнения. Арифметика остатков. Критерий делимости. Степени. Диофантовы уравнения. Деление по модулю. Теорема Ферма. Вычисление корней.  |
| 1.4. Псевдопростые числа | Псевдопростые числа. Числа Кармайкла. Тест Миллера. Тестирование простоты.  |
| 1.5. Системы сравнения | Линейные уравнения. Китайский алгоритм остатков. Степени.  |
| **Модуль 2** |
| 2.1. Группы | Основные определения и примеры. Арифметические группы. Подгруппы. Циклические подгруппы. Теорема Лагранжа.  |
| 2.2. Тесты на простоту | Числа Мерсенна. Числа Ферма. Тест Люка – Лемера. Теста Люка. Примитивные корни. Вычисление порядков.  |
| 2.3. Система шифрования RSA | Шифрование и дешифрование. Выбор простых. Цифровая подпись. |

## Разделы дисциплины и трудоемкость по видам занятий (в академических часах)

Форма обучения - очная

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Раздел дисциплины** | **Общая трудоемкость, всего часов** | **Контактная работа обучающихся с преподавателем** | **Самостоятельная работа обучающихся** |
| всего | лекции | семинары, практические занятия |
|  | **Всего** | 144 | 48 | 32 | 16 | 96 |
| **Семестр 6** |
|  | **Всего** | 90 | 32 | 16 | 16 | 58 |
| 1.1. | Основные алгоритмы  | 9 | 6 | 2 | 4 | 3 |
| 1.2. | Простые числа. Факторизация  | 9 | 4 | 2 | 2 | 5 |
| 1.3. | Арифметика остатков  | 11 | 8 | 4 | 4 | 3 |
| 1.4. | Псевдопростые числа  | 11 | 8 | 4 | 4 | 3 |
| 1.5. | Системы сравнения  | 10 | 6 | 4 | 2 | 4 |
|  | Экзамены и консультации | 40 |  |  |  | 40 |
| **Семестр 7** |
|  | **Всего** | 54 | 16 | 16 | 0 | 38 |
| 2.1. | Группы  | 4 | 6 | 6 | 0 | 12 |
| 2.2. | Тесты на простоту  | 26 | 6 | 6 | 0 | 14 |
| 2.3. | Система шифрования RSA  | 30 | 4 | 4 | 0 | 12 |

# Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Для обеспечения самостоятельной работы студентам предоставляются методические указания, входящие в состав учебно-методических ресурсов ОПОП:

## Методические указания

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.). - б/ц.
2. **Саблина, В.А.** Математические вычисления в MATLAB: метод. указ. к лаб. работам / В. А. Саблина; РГРТУ. - Рязань, 2012. - 24с. - Библиогр.: с.24 (6 назв.). - Б/ц.
3. **Швечкова, О.Г.** Современные алгоритмы криптографической защиты информации: метод. указ. к лаб. работам / О. Г. Швечкова, О. А. Москвитина, Н. С. Курдюков; РГРТУ. - Рязань, 2012. - 40с. - Библиогр.: с.39-40 (13 назв.). - Б/ц.
4. **Швечкова, О.Г.** Основы теории и практики реализации криптографических алгоритмов защиты информации: метод. указ. к лаб. работам / О. Г. Швечкова, О. А. Москвитина, Н. С. Курдюков; РГРТУ. - Рязань, 2012. - 47с. - Библиогр.: с.47 (13 назв.). - Б/ц.
5. **Гришина, В.В.** Алгебра и теория чисел: метод. указ. / В. В. Гришина, А. А. Зенин, К. А. Ципоркова; РГРТУ. - Рязань, 2014. - 52с. - Библиогр.: с.47 (5 назв.). - б/ц.

# Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине представлен в виде оценочных материалов и приведен в Приложении.

# Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

## Основная литература

1. Гашков, С.Б. Криптографические методы защиты информации: учеб. пособие / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - М.: Академия, 2010. - 304с. - (Высш. проф. образ.). - Библиогр.: с.287-294 (157 назв.). - ISBN 978-5-7695-4962-5: 360-00.
2. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко; Ин-т пробл. информ. безопасности МГУ. - М.: МЦНМО, 2003. - 325с. - Библиогр.: с.303-321(292 назв.). - ISBN 5-94057-103-4: 65-00.
3. Вся высшая математика: Учеб.для втузов. Т.7 / М. Л. Краснов [и др.]. - М.: КомКнига, 2006. - 203с. - ISBN 5-484-00521-3 : 229-00,166-00.

## Дополнительная литература

1. Теоретико-числовые методы в криптографии [Электронный ресурс]: учебное пособие /. — Электрон. текстовые данные. — Ставрополь: Северокавказский федеральный университет, 2017. — 107 c. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/75601.html>
2. Аграновский А.В. Практическая криптография. Алгоритмы и их программирование [Электронный ресурс] / А.В. Аграновский, Р.А. Хади. — Электрон. текстовые данные. — М.: СОЛОН-ПРЕСС, 2009. — 256 c. — 5-98003-002-6. — Режим доступа: <http://www.iprbookshop.ru/8641.html>
3. Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях [Электронный ресурс]: практическое пособие / С.И. Алешников, Е.В. Козьминых. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Эммануила Канта, 2006. — 97 c. — 5-88874-689-4. — Режим доступа: <http://www.iprbookshop.ru/23851.html>
4. Алешников С.И. Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых [Электронный ресурс]: практическое пособие / С.И. Алешников, Ю.Ф. Болтнев. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Эммануила Канта, 2007. — 58 c. — 978-5-88874-803-9. — Режим доступа: <http://www.iprbookshop.ru/23795.html>
5. Романьков В.А. Алгебраическая криптография [Электронный ресурс]: монография / В.А. Романьков. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. — 136 c. — 978-5-7779-1600-6. — Режим доступа: <http://www.iprbookshop.ru/24868.html>
6. 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>
7. Гультяева Т.А. Основы теории информации и криптографии [Электронный ресурс] : конспект лекций / Т.А. Гультяева. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2010. — 88 c. — 978-5-7782-1425-5. — Режим доступа: <http://www.iprbookshop.ru/44987.html>
8. Ожиганов А.А. Криптография [Электронный ресурс]: учебное пособие / А.А. Ожиганов. — Электрон. текстовые данные. — СПб.: Университет ИТМО, 2016. — 142 c. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/67231.html>
9. Левина А.Б. Моделирование криптосистем [Электронный ресурс] : учебное пособие / А.Б. Левина. — Электрон. текстовые данные. — СПб.: Интермедия, 2017. — 144 c. — 978-5-4383-0136-3. — Режим доступа: http://www.iprbookshop.ru/66794.html

# Перечень ресурсов информационно–телекоммуникационной сети «Интернет», необходимых для изучения дисциплины

1. Сайт кафедры Высшей математики РГРТУ: <http://www.rsreu.ru/content/view/167/601/>.

Обучающимся по дисциплине «Теоретико-числовые метолы в криптографии» предоставляется доступ к дистанционным курсам, расположенным в системе дистанционного обучения ФГБОУ ВО «РГРТУ»: <http://cdo.rsreu.ru/>. Система дистанционного обучения ФГБОУ ВО «РГРТУ» доступна по паролю, как из внутренней информационной системы организации, так 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 10.06.2016.

Общедоступные Интернет-ресурсы

1. сайт Экспонента: <http://old.exponenta.ru/>
2. Единое окно доступа к образовательным ресурсам: <http://window.edu.ru/>
3. Интернет Университет Информационных Технологий: <http://www.intuit.ru/>
4. Сайт GeoGebra: <https://www.geogebra.org/>

Обучающимся предоставлена возможность индивидуального доступа к следующим электронно-библиотечным системам.

1. Электронная библиотека РГРТУ, режим доступа с любого компьютера без пароля. – URL: <http://elib.rsreu.ru/>
2. Электронно-библиотечная система «IPRbooks», режим доступа – с любого компьютера РГРТУ без пароля, из сети интернет по паролю. – URL: <https://iprbookshop.ru/>

# Методические указания для обучающихся по освоению дисциплины

Дисциплина «Теоретико-числовые метолы в криптографии» предусматривает еженедельные лекции и практические занятия в соответствии с учебным планом. В каждом семестре изучение тем дисциплины завершается промежуточной аттестацией.

Успешное изучение курса требует посещения лекций, активной работы на практических занятиях самостоятельных занятий, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

## Работа с лекциями

При изучении дисциплины очень полезно самостоятельно изучать материал, который еще не прочитан на лекции и не применялся на практическом занятии. Тогда лекция будет гораздо понятнее.

Однако легче при изучении курса следовать изложению материала на лекции. Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий.

После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня.

Лекцию необходимо прочитать, заполнить пропуски, расшифровать и уточнить некоторые сокращения, дополнить некоторые недописанные примеры. Особое внимание следует уделить содержанию понятий.

Все новые понятия должны выделяться в тексте, чтобы их легко можно было отыскать и запомнить.

Лекционный материал является важным, но не единственным для изучения учебной дисциплины. Его необходимо дополнить материалом из рекомендуемой литературы по теме.

Если обучающемуся самостоятельно не удалось разобраться в материале, необходимо сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

При подготовке к следующей лекции, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции.

## Подготовка к практическому занятию

Подготовка состоит в теоретической подготовке (изучение конспекта лекций и дополнительной литературы) и выполнении практических заданий (решение задач, ответы на вопросы и т.д.). Во время самостоятельных занятий студенты выполняют задания, выданные им на предыдущем практическом занятии, готовятся к контрольным работам, выполняют задания типовых расчётов.

## Указания в рамках подготовки к промежуточной аттестации

Промежуточная аттестация проходит в виде экзамена (зачета) или теста, к которому допускаются обучающиеся, выполнившие и сдавшие (защитившие) все предусмотренные учебной программой контрольные мероприятия: контрольные работы и типовые расчёты. Промежуточная аттестация может проводиться в следующих формах:

- Устная форма экзамена (зачета) предусматривает устные ответы на вопросы билета к экзамену. При этом, для уточнения оценки, студенту могут быть заданы дополнительные вопросы.

- Письменная форма экзамена (зачета) предусматривает проверку письменных ответов на вопросы билета к экзамену.

- Тестовая форма (электронный билет, формируемый случайным способом) предусматривает выполнение студентом заданий теста в письменной форме (теоретических или практических), которые проверяются преподавателем или автоматически.

При подготовке к промежуточной аттестации в дополнение к изучению конспектов лекций, учебных пособий, слайдов и другого раздаточного материала, предусмотренного рабочей программой дисциплины, необходимо пользоваться учебной литературой, рекомендованной к настоящей рабочей программе. При подготовке к промежуточной аттестации следует изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала и самостоятельно решить по нескольку типовых задач из каждой темы, из задачника или дистанционного учебного курса. При решении задач всегда необходимо уметь качественно интерпретировать итог решения. Обязательно присутствовать на консультации перед промежуточной аттестации.

## Указания в рамках самостоятельной работы студентов

Самостоятельная работа студентов по дисциплине играет важную роль в ходе всего учебного процесса. Методические материалы, рекомендации и дистанционные учебные курсы для обеспечения самостоятельной работы студентов готовятся преподавателем и выдаются студентам в виде раздаточных материалов или оформляются в виде электронного ресурса, используемого в рамках системы дистанционного обучения ФГБОУ ВО «РГРТУ».

Для реализации компетентностного подхода используются как традиционные формы и методы обучения, так и интерактивные формы, направленные на формирование у студентов навыков коллективной работы и умения анализировать различные материалы.

Для полноценного закрепления материала, представляемого на лекционных занятиях, требуется решение примеров и задач на практических занятиях, а также регулярное выполнение самостоятельной работы, которые необходимы для проверки теоретических знаний и формирования практических навыков.

Обучающимся рекомендуется внимательно ознакомиться с вопросами, которые предусматривают самостоятельное изучение, и осмыслить характер задания. Затем следует найти источники информации по соответствующему вопросу, используя предложенный преподавателем список обязательной и дополнительной литературы, а также ресурсы интернета.Вовремя рекомендуется осуществлять теоретический анализ текста: выделять главные мысли, находить аргументы, подтверждающие основные тезисы, а также иллюстрирующие их примеры и т.д. После этого можно приступать к выполнению задания, при этом важно помнить, что выполненное задание во всех случаях должно отражать основные выводы, к которым пришли в процессе самостоятельной учебной деятельности.

В качестве текущей аттестации используются результаты выполнения контрольных работ и типовых расчётов по материалам пройдённых тем и разделов.

# Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При проведении практических занятий и самостоятельной работы студентов используется программное обеспечение:

- лицензионная копия операционной системы Windows или иной свободно распространяемой операционной системы;

- свободно распространяемая программа интерактивной математики GeoGebra;

- свободно распространяемая система дистанционного обучения Moodle;

- браузер (Firefox, Google, Opera);

- дистанционные курсы по темам дисциплины, разработанные в системе дистанционного обучения преподавателями кафедры Moodle.

# Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для лекционных занятий используются лекционные аудитории РГРТУ, оборудованные доской для наглядного изложения учебного материала.

Для практических занятий используются учебные аудитории РГРТУ, оборудованные доской для представления учебного материала.

|  |  |  |
| --- | --- | --- |
| Программу составил:к.ф.-м.н., доцент каф. ИБ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | (Ильин М.Е.) |
| Программа рассмотрена и одобрена на заседании кафедры ИБ | 26 июня 2018г. | (протокол № 12) |
| Заведующий кафедрой ИБ, ктн., доцент | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | (Пржегорлинский В.Н.) |