МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Теоретико-числовые методы в криптографии
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс ___3___ семестр ____5____
лекции __36_ час.
практические занятия____36___час.
лабораторные работы____00___час.
в том числе с использованием МАО лек.__9___/пр.__12___/лаб.___00__ час.
в том числе в электронной форме лек.___00__/пр.___00_/лаб.__00__ час.
всего часов аудиторной нагрузки____72____ час.
в том числе с использованием МАО ___21__ час.
в том числе в электронной форме __00__час.
самостоятельная работа _____72____ час.
в том числе на подготовку к экзамену ___27___ час.
курсовая работа / курсовой проект не предусмотрены
зачет__не предусмотрен__
экзамен_____5_____семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Боршевников А.Е. Ассистент

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ABSTRACT

Specialist's degree in 10.05.01 Computer Security
Specialization "Mathematical Methods for Information Security"
Course title: *Number theoretic methods in cryptography*
Basic part of Block 1, 4 credits
Instructor: *Borshevnikov A.E.*

At the beginning of the course a student should be able to:

• *ability to apply research methodology in professional activities, including in the work on interdisciplinary and innovative projects (OPK-4).*

Learning outcomes:

(OPK-2) the ability to correctly apply the apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, probability theory, mathematical statistics, information theory, number-theoretic methods in solving professional problems.

Course description:

The course of the discipline's lectures is built on step-by-step narration from the properties of the functions of estimating the complexity of arithmetic operations and elements of number theory to discrete logarithmic algorithms and testing numbers for simplicity.

Main course literature:

1. Глухов М.М. Введение в теоретико-числовые методы криптографии: учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466#book_name

2. Рябко Б.Я. Основы современной криптографии и стеганографии: монография / Б.Я. Рябко, А.Н. Фионов — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192#book_name

3. Червяков Н.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии: монография / Н.И. Червяков, А.А. Евдокимов, А.И. Галушкин, И.Н. Лавриненко — Москва : Физматлит, 2012. — 280 с. — Режим доступа: https://e.lanbook.com/book/5300#book_name

Form of final control: *exam.*

Аннотация к рабочей программе дисциплины
«Теоретико-числовые методы в криптографии»

Курс учебной дисциплины «Теоретико-числовые методы в криптографии» предназначен для обучения студентов направления специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.38.

Общая трудоемкость дисциплины составляет 144 академических часа (4 з.е.). Учебным планом предусмотрены лекции (36 часов), практические занятия (36 часов), самостоятельная работа студента (45 часов), подготовка к экзамену (27 часов). Дисциплина реализуется на 3 курсе в 5 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Теоретико-числовые методы в криптографии» основывается на знаниях, полученных при изучении дисциплин «Математический анализ», «Математическая логика и теория алгоритмов», «Теория вероятностей».

Курс лекций дисциплины построен на пошаговом повествовании от свойств функций оценки сложности арифметических операций и элементов теории чисел к алгоритмам дискретного логарифмирования и тестирования чисел на простоту.

Цель изучение дисциплины «Теоретико-числовые методы в криптографии» – формирование у студентов знаний в области современной алгоритмической теории чисел и ее применении в криптологии.

Задачи дисциплины:

- четкое осознание необходимости и важности математической подготовки для специалиста по компьютерной безопасности;
- ознакомление с основами классической и современной теории чисел, имеющими практические приложения к решению некоторых важных криптографических задач;

•умение давать строгую с математической точки зрения оценку применяемых алгоритмов.

Для успешного изучения дисциплины «Теоретико-числовые методы в криптографии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции:

Код и формулировка компетенции	**Этапы формирования компетенции**	
(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	Знает	основные понятия математической логики и теории алгоритмов. Основные понятия и методы дискретной математики, включая дискретные функции, конечные автоматы, комбинаторный анализ. Основы теории групп и теории групп подстановок. Основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности.
	Умеет	применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием.
	Владеет	математическим аппаратом, изученным в данном курсе и необходимым для дальнейшего совершенствования профессиональной деятельности.

Для формирования вышеуказанных компетенций в рамках дисциплины «Теоретико-числовые методы в криптографии» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах.

Используемые оценочные средства: конспекты (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Вводный (16 час.)

Тема 1. Оценка сложности арифметических операций (8 час.)

Свойства функций оценки сложности. Сложность арифметических операций с целыми числами. Сложность алгоритма Евклида. Сложность операций в кольце вычетов.

Тема 2. Элементы теории чисел (8 час.)

Непрерывные дроби и их свойства. Квадратичные вычеты и невычеты. Теорема Чебышева о распределении простых чисел. Использование модульной арифметики. Вычисления с многочленами. Дискретное преобразование Фурье.

Раздел II. Вводный (20 час.)

Тема 1. Факторизация целых чисел (6 час.)

Метод пробных делений. Факторизация Ферма. Алгоритм Диксона. Алгоритм Брилхарта-Моррисона. Метод квадратичного решета. Метод Полларда. Алгоритм Полларда-Штрассена. $(p-1)$-метод Полларда.

Тема 2. Алгоритмы дискретного логарифмирования (6 час.)

Метод Полига-Хеллмана. Шаги младенца и шаги гиганта. ρ-метод Полларда. λ-метод Полларда. Параллельный ρ-метод.

Тема 3. Тестирование чисел на простоту (8 час.)

Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Тест Соловея-Штрассена. Тест Рабина-Миллера. Полиномиальный тест распознавания простоты.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 час.)

Занятие 1. Введение в математические проблемы криптографии (18 час.)

1. Основы теории чисел.

2. Теория сравнений. Вычеты.

3. Сравнения первой степени. Системы сравнений первой степени.

Занятие 2. Теоретико-числовые методы в криптографии (18 час.)

1. Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.

2. Алгоритмы криптоанализа шифров с открытым ключом.

3. Конечные группы и поля многочленов.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Теоретико-числовые методы в криптографии» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Вводный	ОПК-2	знает	Конспект (ПР-7)	1-10
			умеет	собеседование (ОУ-1)	1-10
			владеет	собеседование (ОУ-1)	1-10
2	Раздел II. Основной	ОПК-2	знает	Конспект (ПР-7)	11-29
			умеет	собеседование (ОУ-1)	11-29
			владеет	собеседование (ОУ-1)	11-29

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Глухов М.М. Введение в теоретико-числовые методы криптографии: учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466#book_name
2. Рябко Б.Я. Основы современной криптографии и стеганографии: монография / Б.Я. Рябко, А.Н. Фионов — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192#book_name
3. Червяков Н.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии: монография / Н.И. Червяков, А.А. Евдокимов, А.И. Галушкин, И.Н. Лавриненко — Москва : Физматлит, 2012. — 280 с. — Режим доступа: https://e.lanbook.com/book/5300#book_name

Дополнительная литература

(печатные и электронные издания)

1. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г.А. Ганеш — Москва : Издательство "Лаборатория знаний", 2015. — 428 с. — Режим доступа: https://e.lanbook.com/book/70724#book_name
2. Глухов, М.М. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии: учебное пособие / М.М. Глухов, И.А. Круглов — Санкт-Петербург : Лань, 2015. — 176 с. — Режим доступа: https://e.lanbook.com/book/65044#book_name
3. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. дан. — Москва :

ДМК Пресс, 2008. — 448 с. — Режим доступа: https://e.lanbook.com/book/3027

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Лекции. Криптография [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://habr.com/company/yandex/blog/324866/
2. Лекции. Теоретико-числовые методы [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://docplayer.ru/69224460-Teoretiko-chislovye-metody-v-kriptografii.html
3. Лекции. Теоретико-числовые методы в криптографии [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://window.edu.ru/resource/316/78316

Перечень информационных технологий и программного обеспечения

Для работы с литературой из списка необходимо наличие у студента аккаунта в электронно-библиотечной системе «Лань» (https://e.lanbook.com/)

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Теоретико-числовые методы в криптографии», составляет 72 часа. На самостоятельную работу – 72 часа, в том числе 27 часов на подготовку к экзамену. При этом аудиторная нагрузка состоит из 36 лекционных часов и 36 часов практических занятий.

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических заданий. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

При подготовке к практическим занятиям также необходимо повторить теоретический материал.

Промежуточная форма аттестации по данной дисциплине – экзамен. Вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к экзамену студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 608, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 30) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Дальневосточный федеральный университет»

(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Теоретико-числовые методы в криптографии»

Направление подготовки 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Форма подготовки очная

Владивосток

2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	45	Отчет о выполнении практического задания
2	Сессия	Подготовка и сдача экзамена	27	Экзамен

Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

Методические указания к выполнению отчета по занятию

Для получения **«зачтено»** отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка **«незачтено»** выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Теоретико-числовые методы в криптографии»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	**Этапы формирования компетенции**	
(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	Знает	основные понятия математической логики и теории алгоритмов. Основные понятия и методы дискретной математики, включая дискретные функции, конечные автоматы, комбинаторный анализ. Основы теории групп и теории групп подстановок. Основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности.
	Умеет	применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием.
	Владеет	математическим аппаратом, изученным в данном курсе и необходимым для дальнейшего совершенствования профессиональной деятельности.

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Вводный	ОПК-2	знает	Конспект (ПР-7)	1-10
			умеет	собеседование (ОУ-1)	1-10
			владеет	собеседование (ОУ-1)	1-10
2	Раздел II. Основной	ОПК-2	знает	Конспект (ПР-7)	11-29
			умеет	собеседование (ОУ-1)	11-29
			владеет	собеседование (ОУ-1)	11-29

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

1. Свойства функций оценки сложности.
2. Сложность арифметических операций с целыми числами.

3. Сложность алгоритма Евклида
4. Сложность операций в кольце вычетов.
5. Непрерывные дроби и их свойства.
6. Квадратичные вычеты и невычеты.
7. Теорема Чебышева о распределении простых чисел.
8. Использование модульной арифметики.
9. Вычисления с многочленами.
10. Дискретное преобразование Фурье.
11. Метод пробных делений.
12. Факторизация Ферма.
13. Алгоритм Диксона.
14. Алгоритм Брилхарта-Моррисона.
15. Метод квадратичного решета.
16. Метод Полларда.
17. Алгоритм Полларда-Штрассена.
18. $(p-1)$-метод Полларда.
19. Метод Полига-Хеллмана.
20. Шаги младенца и шаги гиганта.
21. ρ-метод Полларда.
22. λ-метод Полларда.
23. Параллельный ρ-метод.
24. Решето Эратосфена.
25. Критерий Вильсона.
26. Тест на основе малой теоремы Ферма.
27. Тест Соловея-Штрассена.
28. Тест Рабина-Миллера.
29. Полиномиальный тест распознавания простоты.

Критерии выставления оценки на экзамене

Оценка	**Требования к сформированным компетенциям**
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно

	обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач по методологии научных исследований.
«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Кроткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы,	Вопросы по темам/разделам

			раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	дисциплины
3	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины