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. 0 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 54 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрены
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: Власов А.А.

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:

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

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

Course description: The content of the discipline covers the following range of issues: estimation of the complexity of arithmetic operations, elements of number theory, factorization of integers, discrete logarithmization algorithms, testing of numbers for simplicity

Main course literature:

1. Глухов, М.М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — 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 [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — 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 [Электронный ресурс] : монография / Н.И. Червяков, А.А. Евдокимов, А.И. Галушкин, И.Н. Лавриненко. — Электрон. дан. — 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 специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть дисциплин учебного плана Б1.Б.12.07.

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 академических часа. Учебным планом предусмотрены лекции (36 часов), практические занятия (36 часов), самостоятельная работа студента (72 часа, в том числе 54 часа на подготовку к экзамену). 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».

Содержание дисциплины охватывает следующий круг вопросов: оценка сложности арифметических операций, элементы теории чисел, факторизация целых чисел, алгоритмы дискретного логарифмирования, тестирование чисел на простоту

Цель дисциплины – 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 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 (ОПК-2).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

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. Оценочные средства: конспект (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	собеседование (ОУ-1),	1-10
			умеет	коллоквиум (ОУ-2).	1-10
			владеет	конспект (ПР-7),	1-10
2	Раздел II. Основной	ОПК-2	знает	собеседование (ОУ-1),	11-29
			умеет	коллоквиум (ОУ-2).	11-29
			владеет	конспект (ПР-7),	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 [Электронный ресурс] : учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — 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 [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — 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 [Электронный ресурс] : монография / Н.И. Червяков, А.А. Евдокимов, А.И. Галушкин, И.Н. Лавриненко. — Электрон. дан. — 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 [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш ; под ред. С. М. Молявко ; пер. с англ. В. Д. Хорева. — Электрон. дан. — 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 [Электронный ресурс] : учебное пособие / М.М. Глухов, И.А. Круглов. — Электрон. дан. — 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/reader/book/3027/#1

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

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 569, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 549, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 733а, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

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 54 часа 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 569, 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 – 40) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 549, Компьютерный класс, 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 – 15) Оборудование: "Моноблок lenovo C360G-i34164G500UDK Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор, Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718" Доска аудиторная
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 733а, Компьютерный класс, 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 – 15) Оборудование: Компьютер (твердотельный диск - объемом 128 ГБ; жесткий диск - объем 1000 ГБ; форм-фактор - Tower; комплектуется клавиатурой, мышью, монитором AOC i2757Fm; комплектом шнуров эл. питания) модель - M93p 1 Доска аудиторная

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»

Специальность 10.05.01 Компьютерная безопасность

(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 недели обучения	Подготовка практического задания (выполнение отчетов к практическим работам № 1-2)	18	Отчеты о выполнении
2	Сессия	Подготовка к экзамену	54	Экзамен

Подготовка отчета по практическим работам предполагает повторение лекционного материала и выполнение задания для практических работ по темам из Раздела II РПУД.

В ходе самостоятельной работы обучающийся должен подготовить для сдачи отчёт по проделанной работе. Необходимо указать в отчёте следующую информацию: название и цель работы, краткий теоретический материал, задание на практическую работу, ход работы, полученные результаты и выводы. По результатам защиты отчёта студенту выставляется «зачтено» или «не зачтено». Студент получает «зачтено», если отчёт содержит все перечисленные ранее пункты и оформлен в соответствии с правилами оформления письменных работ.

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки к экзамену, а также методические рекомендации по оцениванию представлены в Приложении 2 РПУД

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»

Специальность 10.05.01 Компьютерная безопасность

(Математические методы защиты информации)

Форма подготовки очная

Владивосток

2019

Паспорт ФОС

Шкала оценивания уровня сформированности компетенций

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

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	собеседование (ОУ-1),	1-10
			умеет	коллоквиум (ОУ-2).	1-10
			владеет	конспект (ПР-7),	1-10
2	Раздел II. Основной	ОПК-2	знает	собеседование (ОУ-1),	11-29
			умеет	коллоквиум (ОУ-2).	11-29
			владеет	конспект (ПР-7),	11-29

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине - экзамен.

Для допуска к экзамену необходимо сдать все практические задания. В случае, если ко дню проведения экзамена обучающийся не сдал какие-либо из практических заданий, он получает возможность сдать их на консультации перед экзаменом. Экзамен выставляется на основании сдачи всех практических заданий и сдачи экзаменационного билета.

При определении оценки ответа обучающегося как на экзамене, так и на практическом занятии учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

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.

Каждый экзаменационный билет содержит два вопроса из списка выше. Результаты экзамена оцениваются по четырёхбалльной системе («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, сведениям из информационных ресурсов Интернет.

Оценка **«отлично».** Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания дисциплины. Соблюдаются нормы литературной речи.

Оценка **«хорошо».** Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.

Оценка **«удовлетворительно».** Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.

Оценка **«неудовлетворительно».** Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи.

В случае неявки студента на экзамен в экзаменационной ведомости делается отметка «не явился».

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются конспект (ПР-7) и лабораторные работы (ПР-6).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.

Для оценки продвинутого и высокого уровня сформированности компетенции проводятся лабораторные работы. Темы практических работ представлены в Разделе II РПУД. Критерии оценки представлены в таблице:

Оценка	Критерий
Зачтено	Отчёт по практической работе содержит все необходимые пункты (цель работы, краткий теоретический материал, задание на практическую работу, ход работы, полученные результаты, выводы). Оформление отчёта соответствует правилам оформления письменных работ. Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Незачтено	Отчёт по практической работе не содержит какого-либо необходимого пункта(ов) и/или оформление отчёта не соответствует правилам оформления письменных работ.

	Конспект не содержит основных понятий, терминов, положений по данной теме