МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Вятский государственный университет»
(ВятГУ)
г. Киров

Утверждаю
Директор/Декан *Бушмелева Н. А.*

_____

Номер регистрации
РПД_3-02.03.01.51_2018_93045
Актуализировано: 27.04.2021

Рабочая программа дисциплины
Математические методы криптографии

наименование дисциплины

Квалификация выпускника	Бакалавр
Направление подготовки	02.03.01 шифр
	Математика и компьютерные науки наименование
Направленность (профиль)	3-02.03.01.51 шифр
	Математические основы компьютерных наук наименование
Формы обучения	Очная наименование
Кафедра-разработчик	Кафедра фундаментальной математики (ОРУ) наименование
Выпускающая кафедра	Кафедра фундаментальной математики (ОРУ) наименование

Киров, 2018 г.

Сведения о разработчиках рабочей программы дисциплины

Чупраков Дмитрий Вячеславович

ФИО

Цели и задачи дисциплины

Цель дисциплины	Систематизация и расширение знаний студентов в области теории чисел и алгебры, овладение методами теории чисел, имеющими криптографические приложения, получение опыта построения и анализа схем криптосистем на основе теоретико-числовых методов.
Задачи дисциплины	1) формирование знаний о математических алгоритмах, лежащих в основе криптографического метода защиты информации 2) формирование знаний, умений и навыков применения и анализа асимметричных шифров; 3) формирование умений и навыков приложения теории чисел в области защиты информации

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Компетенция ПК-3

способностью строго доказывать утверждение, сформулировать результат, увидеть следствия полученного результата		
Знает	Умеет	Владеет
Виды математических теорем и способы их формулировок.	Выделять структуру теоремы, применять разные способы доказательств и выводить следствия.	Методами выбора путей проведения доказательств.

Компетенция ПК-6

способностью использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач		
Знает	Умеет	Владеет
Основные математические алгоритмы, используемые в криптографии	Применять на практике методы математического и алгоритмического программирования при решении задач криптографии	Методами программной реализации математических алгоритмов, используемых в криптографии

Компетенция УК-1

Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач		
Знает	Умеет	Владеет
методы выработки стратегии действий, последствия принятия решений в условиях проблемной ситуации в области криптографии	оценивать критически степень проблемности ситуации в области криптографии на основании системного подхода, вырабатывать стратегию действий	основными математическими методами криптографии, навыками мотивированно вырабатывать стратегию действий в условиях проблемной ситуации

Структура дисциплины

Тематический план

№ п/п	Наименование разделов дисциплины	Шифр формируемых компетенций
1	Теоретико-числовые методы криптографии	ПК-3, УК-1
2	Асимметричные криптосистемы на основе модулярной арифметики	ПК-6, УК-1
3	Подготовка и прохождение промежуточной аттестации	ПК-3, ПК-6, УК-1

Формы промежуточной аттестации

Зачет	7 семестр (Очная форма обучения)
Экзамен	Не предусмотрен (Очная форма обучения)
Курсовая работа	Не предусмотрена (Очная форма обучения)
Курсовой проект	Не предусмотрена (Очная форма обучения)

Трудоемкость дисциплины

Форма обучения	Курсы	Семестры	Общий объем (трудоемкость)		Контактная работа, час	в том числе аудиторная контактная работа обучающихся с преподавателем, час				Самостоятельная работа, час	Курсовая работа (проект), семестр	Зачет, семестр	Экзамен, семестр
			Часов	ЗЕТ		Всего	Лекции	Семинарские, практические занятия	Лабораторные занятия				
Очная форма обучения	4	7	144	4	93.5	56	26	30	0	50.5		7	

Содержание дисциплины

Очная форма обучения

Код занятия	Наименование тем занятий	Трудоемкость, академических часов
Раздел 1 «Теоретико-числовые методы криптографии»		**77.00**
Лекции		
Л1.1	Основные понятия криптографии	2.00
Л1.2	Делимость и сравнения первого порядка	4.00
Л1.3	Квадратичные вычеты	2.00
Л1.4	Простые числа и их свойства. Распознание простоты чисел	2.00
Л1.5	Генерация простых чисел	2.00
Л1.6	Факторизация целых чисел	2.00
Семинары, практические занятия		
П1.1	Криптофункция	2.00
П1.2	Простейшие подстановочные шифры	2.00
П1.3	Алгоритмы нахождения НОД	2.00
П1.4	Модулярная арифметика	2.00
П1.5	Решение сравнений 1 порядка	2.00
П1.6	Вероятностные алгоритмы проверки чисел на простоту	2.00
П1.7	Детерминированные алгоритмы проверки чисел на простоту	4.00
П1.8	Разложение чисел на множители	2.00
Самостоятельная работа		
С1.1	Подготовка к практическим занятиям и выполнение домашнего задания	25.00
Контактная внеаудиторная работа		
КВР1.1	Контактная внеаудиторная работа	20.00
Раздел 2 «Асимметричные криптосистемы на основе модулярной арифметики»		**63.00**
Лекции		
Л2.1	Алгоритм RSA и его свойства	4.00
Л2.2	Протоколы аутентификации на основе модулярной арифметики	4.00
Л2.3	Псевдослучайные последовательности. Алгебраические генераторы	4.00
Семинары, практические занятия		
П2.1	Алгоритм RSA. Его свойства	4.00
П2.2	Протоколы аутентификации и электронной цифровой подписи на базе модулярной арифметики	4.00
П2.3	Генераторы псевдослучайной последовательности	4.00
Самостоятельная работа		
С2.1	Подготовка к практическим занятиям и выполнение домашнего задания	22.00
Контактная внеаудиторная работа		

КВР2.1	Контактная внеаудиторная работа	17.00
Раздел 3 «Подготовка и прохождение промежуточной аттестации»		**4.00**
33.1	Подготовка к сдаче зачета	3.50
КВР3.1	Сдача зачета	0.50
ИТОГО		**144.00**

Содержание дисциплины данной рабочей программы используется при обучении по индивидуальному учебному плану, при ускоренном обучении, при применении дистанционных образовательных технологий и электронном обучении (при наличии).

Методические указания для обучающихся по освоению дисциплины

Успешное освоение дисциплины предполагает активное, творческое участие обучающегося на всех этапах ее освоения путем планомерной, повседневной работы. Обучающийся обязан посещать лекции, семинарские, практические и лабораторные занятия (при их наличии), получать консультации преподавателя и выполнять самостоятельную работу.

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, методических указаний и разработок, указанных в программе, особое внимание уделить целям, задачам, структуре и содержанию дисциплины.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее основных положений. Тематика лекций определяется настоящей рабочей программой дисциплины.

Лекции – это систематическое устное изложение учебного материала. На них обучающийся получает основной объем информации по каждой конкретной теме. Лекции обычно носят проблемный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов.

Предполагается, что обучающиеся приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендованным программой. Часто обучающимся трудно разобраться с дискуссионными вопросами, дать однозначный ответ. Преподаватель, сравнивая различные точки зрения, излагает свой взгляд и нацеливает их на дальнейшие исследования и поиск научных решений. После лекции желательно вечером перечитать и закрепить полученную информацию, тогда эффективность ее усвоения значительно возрастает. При работе с конспектом лекции необходимо отметить материал, который вызывает затруднения для понимания, попытаться найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь за помощью к преподавателю.

Целью семинарских занятий является проверка уровня понимания обучающимися вопросов, рассмотренных на лекциях и в учебной литературе.

Целью практических и лабораторных занятий является формирование у обучающихся умений и навыков применения теоретических знаний в реальной практике решения задач; восполнение пробелов в пройденной теоретической части курса.

Семинарские, практические и лабораторные занятия в равной мере направлены на совершенствование индивидуальных навыков решения теоретических и прикладных задач, выработку навыков интеллектуальной работы, а также ведения дискуссий. Для успешного участия в семинарских, практических и лабораторных занятиях обучающемуся следует тщательно подготовиться.

Основной формой подготовки обучающихся к практическим (лабораторным) занятиям является самостоятельная работа с учебно-методическими материалами, научной литературой, статистическими данными и т.п.

Изучив конкретную тему, обучающийся может определить, насколько хорошо он в ней разобрался. Если какие-то моменты остались непонятными, целесообразно составить список вопросов и на занятии задать их преподавателю. Практические (лабораторные) занятия предоставляют обучающемуся возможность творчески раскрыться, проявить инициативу и развить навыки публичного ведения дискуссий и общения.

Самостоятельная работа обучающихся включает в себя выполнение различного рода заданий (изучение учебной и научной литературы, материалов лекций, систематизацию прочитанного материала, подготовку контрольной работы, решение

задач, подготовка докладов, написание рефератов, публикация тезисов, научных статей, подготовка и защита курсовой работы / проекта и другие), которые ориентированы на глубокое усвоение материала изучаемой дисциплины.

Обучающимся рекомендуется систематически отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки.

Внутренняя система оценки качества освоения дисциплины включает входной контроль уровня подготовленности обучающихся, текущий контроль успеваемости, промежуточную аттестацию, направленную на оценивание промежуточных и окончательных результатов обучения по дисциплине (в том числе результатов курсового проектирования (выполнения курсовых работ) при наличии).

При проведении промежуточной аттестации обучающегося учитываются результаты текущего контроля, проводимого в течение освоения дисциплины.

Процедура оценивания результатов освоения дисциплины осуществляется на основе действующих локальных нормативных актов ФГБОУ ВО «Вятский государственный университет», с которыми обучающиеся ознакамливаются на официальном сайте университета www.vyatsu.ru.

Учебно-методическое обеспечение дисциплины, в том числе учебно-методическое обеспечение самостоятельной работы обучающегося по дисциплине

Учебная литература (основная)

1) Кнауб, Л. В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=229582/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии (2-е издание, дополненное) / О.Н. Василенко. - 2-е изд., доп. - Москва : МЦНМО, 2006. - 336 с. - ISBN 5-94057-103-4 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=61814/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

Учебная литература (дополнительная)

1) Василенко, Олег Николаевич. Теоретико-числовые алгоритмы в криптографии : монография / О. Н. Василенко ; Ин-т проблем информ. безопасности МГУ. - Москва : МЦНМО, 2006. - 336 с. - (Информационная безопасность: криптография). - Библиогр.: с. 303-321. - ISBN 5-94057-103-4 : 150.00 р. - Текст : непосредственный.

2) Романьков, Виталий Анатольевич. Введение в криптографию : учеб. пособие / В. А. Романьков. - 2-е изд., испр. и доп. - Москва : Форум, 2012. - 239, [1] с. - Библиогр.: с. 233-234. - ISBN 978-5-91134-573-0 : 347.00 р. - Текст : непосредственный.

3) Рябко, Б. Я. Основы современной криптографии и стеганографии / Б.Я. Рябко. - Москва : Горячая линия - Телеком, 2010. - 232 с. - ISBN 978-5-9912-0150-6 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=253604/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

Учебно-методические издания

1) Майстренко, Н. В. Основы теории информации и криптографии: учебное электронное издание : учебное пособие / Н.В. Майстренко, А.В. Майстренко. - Тамбов : ФГБОУ ВПО "ТГТУ", 2018. - 81 с. : табл., граф., схем., ил. - Библиогр. в кн. - ISBN 978-5-8265-1950-9 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=570354/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Пушкарев, Игорь Александрович. Введение в теорию кодов, исправляющих ошибки и криптографию : учебно-методич. пособие / И. А. Пушкарев ; ВятГУ,

ФПМТ, каф. ПМиИ. - Киров : ВятГУ, 2009. - х. - Б. ц. - URL: https://lib.vyatsu.ru. - Режим доступа: для авториз. пользователей. - Текст : электронный.

Электронные образовательные ресурсы

1) Портал дистанционного обучения ВятГУ [электронный ресурс] / - Режим доступа: http://mooc.do-kirov.ru/
2) Раздел официального сайта ВятГУ, содержащий описание образовательной программы [электронный ресурс] / - Режим доступа: https://www.vyatsu.ru/php/programms/eduPrograms.php?Program_ID=3-02.03.01.51
3) Личный кабинет студента на официальном сайте ВятГУ [электронный ресурс] / - Режим доступа: https://new.vyatsu.ru/account/
4) Единое окно доступа к образовательным ресурсам http://window.edu.ru/

Электронные библиотечные системы (ЭБС)

- ЭБС «Научная электронная библиотека eLIBRARY» (http://elibrary.ru/defaultx.asp)
- ЭБС «Издательства Лань» (http://e.lanbook.com/)
- ЭБС «Университетская библиотека online» (www.biblioclub.ru)
- Внутренняя электронно-библиотечная система ВятГУ (http://lib.vyatsu.ru/)
- ЭБС «ЮРАЙТ (https://urait.ru)

Современные профессиональные базы данных и информационные справочные системы

- ГАРАНТ
- КонсультантПлюс
- Техэксперт: Нормы, правила, стандарты
- Роспатент (https://www1.fips.ru/elektronnye-servisy/informatsionno-poiskovaya-sistema)
- Web of Science® (http://webofscience.com)

Материально-техническое обеспечение дисциплины

Демонстрационное оборудование

Перечень используемого оборудования
Доска интерактивная Hitachi StarBoard с напольной стойкой
интерактивная система Smart со встроенным проектором
Компьютер персональный
Мультимедиа-проектор Epson EB-X72
Проектор №2
Телевизор LCD с креплением

Специализированное оборудование

Перечень используемого оборудования
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL S253.MI (МОНОБЛОК)
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL S273.Mi (МОНОБЛОК)
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL SafeRay S251.Mi (МОНОБЛОК)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе лицензионное и свободно распространяемое ПО (включая ПО отечественного производства)

№ п.п	Наименование ПО	Краткая характеристика назначения ПО
1	Программная система с модулями для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»	Программный комплекс для проверки текстов на предмет заимствования из Интернет-источников, в коллекции диссертация и авторефератов Российской государственной библиотеки (РГБ) и коллекции нормативно-правовой документации LEXPRO
2	Microsoft Office 365 ProPlusEdu ALNG SubsVL MVL AddOn toOPP	Набор веб-сервисов, предоставляющий доступ к различным программам и услугам на основе платформы Microsoft Office, электронной почте бизнес-класса, функционалу для общения и управления документами
3	Office Professional Plus 2016	Пакет приложений для работы с различными типами документов: текстами, электронными таблицами, базами данных, презентациями
4	Windows Professional	Операционная система
5	Kaspersky Endpoint Security для бизнеса	Антивирусное программное обеспечение
6	Справочная правовая система «Консультант Плюс»	Справочно-правовая система по законодательству Российской Федерации
7	Электронный периодический справочник ГАРАНТ Аналитик	Справочно-правовая система по законодательству Российской Федерации
8	Security Essentials (Защитник Windows)	Защита в режиме реального времени от шпионского программного обеспечения, вирусов.
9	МойОфис Стандартный	Набор приложений для работы с документами, почтой, календарями и контактами на компьютерах и веб браузерах
10	Python	Язык программирования
11	SageMath	система компьютерной алгебры со открытым исходным кодом
12	Maxima	свободная система компьютерной алгебры, написанная на языке Common Lisp
13	WxMaxima	интерфейс для системы компьютерной алгебры Maxima

Обновленный список программного обеспечения данной рабочей программы находится по адресу: https://www.vyatsu.ru/php/list_it/index.php?op_id=93045