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_3-02.04.01.51_2021_120528
Актуализировано: 19.04.2021

Рабочая программа дисциплины
Криптография и защита информации

наименование дисциплины

Квалификация выпускника	Магистр
Направление подготовки	02.04.01 шифр
	Математика и компьютерные науки наименование
Направленность (профиль)	3-02.04.01.51 шифр
	Алгебра и дискретная математика наименование
Формы обучения	Очная наименование
Кафедра-разработчик	Кафедра фундаментальной математики (ОРУ) наименование
Выпускающая кафедра	Кафедра фундаментальной математики (ОРУ) наименование

Киров, 2021 г.

Сведения о разработчиках рабочей программы дисциплины

Чупраков Дмитрий Вячеславович

ФИО

Цели и задачи дисциплины

Цель дисциплины	Формирование у обучающихся знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы 02.04.01 Математика и компьютерные науки.
Задачи дисциплины	1) формирование знаний об основных математических принципах защиты данных и шифрования; 2) формирование знаний об современных направлениях развития криптографии; 3) формирование навыков использования криптографических методов при разработке или внедрении систем шифрования; 4) подготовка студентов к использованию в программных продуктах систем шифрования и защиты данных;

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

Компетенция ОПК-1

Способен находить, формулировать и решать актуальные и значимые проблемы прикладной и компьютерной математики		
Знает	Умеет	Владеет
основные факты и понятия базовых математических дисциплин и компьютерных наук	применять базовые понятия математики и компьютерных наук для решения исследовательских задач в области прикладной и компьютерной математики	методами постановки и решения научно-исследовательских задач в области прикладной и компьютерной математики

Компетенция ОПК-3

Способен самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов, в том числе отечественного производства		
Знает	Умеет	Владеет
современные информационные технологии и основные виды сетевых ресурсов, в том числе отечественного производства	создавать прикладные программные средства технологии и сетевые ресурсы для решения математических и прикладных задач	методами создания прикладные программных средств на основе современных информационных технологий и сетевых ресурсов, в том числе отечественного производства

Структура дисциплины

Тематический план

№ п/п	Наименование разделов дисциплины	Шифр формируемых компетенций
1	Введение в криптографию	ОПК-1, ОПК-3
2	Криптографические преобразования	ОПК-1, ОПК-3
3	Подготовка и прохождение промежуточной аттестации	ОПК-1, ОПК-3

Формы промежуточной аттестации

Зачет	Не предусмотрен (Очная форма обучения)
Экзамен	3 семестр (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	2	3	180	5	99	56	16	24	16	81			3

Содержание дисциплины

Очная форма обучения

Код занятия	Наименование тем занятий	Трудоемкость, академических часов
Раздел 1 «Введение в криптографию»		**70.00**
Лекции		
Л1.1	Криптофункция. Информационный подход	2.00
Л1.2	История развития криптографии	2.00
Л1.3	Представление о криптоанализе	2.00
Л1.4	Криптографические протоколы. Понятие. Классификация. Примеры	2.00
Семинары, практические занятия		
П1.1	Криптофункция и ее стойкость	2.00
П1.2	Псевдослучайные последовательности. Построение и свойства	4.00
П1.3	История криптографии	2.00
Лабораторные занятия		
Р1.1	Исторические шифры	2.00
Р1.2	Частотный криптоанализ	2.00
Р1.3	Проверка качества псевдослучайных последовательностей	2.00
Самостоятельная работа		
С1.1	Подготовка отчетов по лабораторным работам	28.00
Контактная внеаудиторная работа		
КВР1.1	Контактная внеаудиторная работа	20.00
Раздел 2 «Криптографические преобразования»		**83.00**
Лекции		
Л2.1	Симметричные криптопреобразования	4.00
Л2.2	Односторонняя функция	2.00
Л2.3	Асимметричные криптопреобразования	2.00
Семинары, практические занятия		
П2.1	Петля Фейстиля и ее свойства	2.00
П2.2	Криптосистемы над конечными полями	4.00
П2.3	Асимметричные криптофункции на основе факторизации	2.00
П2.4	Асимметричные криптофункции на основе дискретного логарифма	4.00
П2.5	Асимметричные криптофункции над алгебраическими системами	4.00
Лабораторные занятия		
Р2.1	Исследование поточных криптосистем	2.00
Р2.2	Исследование блочных криптосистем	4.00
Р2.3	Анализ асимметричных криптофункций	4.00
Самостоятельная работа		
С2.1	Подготовка отчетов по лабораторным работам	28.50

Контактная внеаудиторная работа		
КВР2.1	Контактная внеаудиторная работа	20.50
Раздел 3 «Подготовка и прохождение промежуточной аттестации»		**27.00**
Э3.1	Подготовка к сдаче экзамена	24.50
КВР3.2	Консультация перед экзаменом	2.00
КВР3.1	Сдача экзамена	0.50
ИТОГО		**180.00**

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) 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.

2) 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.

3) Фороузан, Б. А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. - (Основы информационных технологий). - ISBN 978-5-9963-0242-0 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=428998/ (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) Лидовский, В. В. Основы теории информации и криптографии : курс / В.В. Лидовский. - Москва : Интернет-Университет Информационных Технологий, 2007. - 125 с. - Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=234148/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

Учебно-методические издания

1) Теоретико-числовые методы в криптографии : практикум. - Ставрополь : СКФУ, 2017. - 107 с. : ил. - Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=483838/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Харина, Наталья Леонидовна. Практикум по основам криптографии / Н. Л. Харина ; ВятГУ, ФПМТ, каф.РЭС. - 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=3-02.04.01.51
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
ПРОЕКТОР МУЛЬТИМЕДИЙНЫЙ BENQ MP670 (КОМПЛЕКТ)

Специализированное оборудование

Перечень используемого оборудования
МОНОБЛОК SafeRay S222.Mi (БЕЛЫЙ)
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	Anaconda	дистрибутив языков программирования Python и R с набором приложений. По-умолчанию в Anaconda Navigator доступны следующие приложения: JupyterLab Jupyter Notebook QtConsole Spyder Glue Orange RStudio Visual Studio Code

Обновленный список программного обеспечения данной рабочей программы находится по адресу: https://www.vyatsu.ru/php/list_it/index.php?op_id=120528