МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Рязанский государственный университет имени С.А. Есенина»

Утверждаю

декан физико-математического факультета

_____ Н.Б. Федорова

«31» августа 2020 г.

Рабочая программа дисциплины
«Математические основы защиты информации и информационной безопасности»

Уровень основной образовательной программы: МАГИСТРАТУРА

Направление подготовки: 02.04.02 Фундаментальная информатика и информационные технологии (информационные системы)

Программа: Информационные системы

Форма обучения: очная

Сроки освоения ООП: 2 года **(**нормативный)

Физико-математический факультет

Кафедра: Информатики, вычислительной техники и методики преподавания информатики

Рязань, 2020

1. Цели освоения дисциплины

Целью освоения учебной дисциплины «Математические основы защиты информации и информационной безопасности» является формирование у обучающихся общекультурных и профессиональных компетенций в процессе изучения информатики и программирования для последующего применения в учебной и практической деятельности.

Задачи дисциплины:

- систематизация, формализация и расширение знаний по основным положениям теории информации, математическими моделями и стандартами шифрования;
- изучение математических основ защиты информации: арифметики целых чисел, модульной арифметики, теории чисел, а так же методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и связи;
- дать студенту достаточно прочные представления о информационной безопасности, включая аппаратную часть и математическое обеспечение;
- привитие навыков работы с методами шифрования и криптоанализа
- формирование современной культуры программирования.

2. Место дисциплины в структуре ОПОП магистратуры

2.1. Дисциплина «Математические основы защиты информации и информационной безопасности» относится к части, формируемой участниками образовательных отношений Блока 1.

2.2. Для изучения дисциплины «Математические основы защиты информации и информационной безопасности» необходимы следующие знания, умения, навыки, формируемые предшествующими дисциплинами:

- «Теория алгоритмов»
- «Современные операционные системы»
- «Проектирование информационных систем»

2.3. Перечень последующих дисциплин, для которых необходимы знания, умения, навыки, формируемые данной дисциплиной:

- «Перспективные направления развития баз данных»
- «Объектно-ориентированные CASE-технологии»
- «Параллельное и распределенное программирование»

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

Изучение данной дисциплины направлено на формирование у обучающихся профессиональных (ПК) компетенций:

№ п/п	Код и содержание компетенции	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения по дисциплине В результате изучения дисциплины обучающиеся должны:		
			Знать	Уметь	Владеть (навыками)
1	2	3	4	5	6
1.	ПК-1. Способность демонстрации общенаучных базовых знаний математических и естественных наук, фундаментальной информатики и информационных технологий; способность применять в профессиональной деятельности современные языки программирования и методы параллельной обработки данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии.	ПК-1.1. Знает основы научно-исследовательской деятельности в области информационных технологий, владеет знанием основ философии и методологии науки; знанием методов научных исследований и навыками их проведения	• основные принципы административно-правовой защиты информации • математические принципы, лежащие в основе криптографических моделей • теорию простых чисел и модульной арифметики • этапы решения задачи на компьютере.	• быстро реагировать на различные угрозы информационной безопасности • уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования.	• навыками применения, установки и настройки антивирусных систем и систем распознавания угроз и атак • владеть алгоритмическими языками для разработки прикладных алгоритмов шифрования • владеть навыками решения задач криптоанализа и шифрования.
2.		ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности	• терминологию из области криптографии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений; • основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики; • математические	• выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач; • использовать математические модели для построения криптологических систем; • применять современные технологии создания брандмауэ-	• основными методами, способами и средствами шифрования и криптографии; • навыками решения задач модульной и целочисленной арифметики, теории простых чисел • приемами обнаружения вирусных угроз • приемами обнаруже-

			криптологические системы, включая средства описания.	ров и IDS-комплексов.	ния сетевых проникновений; • навыками работы по обнаружению и защите от DDOS-атак.

ОСНОВНАЯ ЧАСТЬ

1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы		Всего часов	Семестры
			№2
			часов
1		2	3
1. Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)		36	36
В том числе:			
Лекции (Л)		18	18
Практические занятия (ПЗ), Семинары (С)			
Лабораторные работы (ЛР)		18	18
Иные виды занятий			
2. Самостоятельная работа студента (всего)		108	108
3. Курсовая работа (при наличии)	КП		
	КР		
Вид промежуточной аттестации	зачет (З),		
	экзамен (Э)		+
ИТОГО: общая трудоемкость	часов	144	144
	зач. ед.	4	4

Дисциплина частично реализуется с применением дистанционных образовательных технологий с использованием платформы Microsoft Teams, ЭИОС Moodle, корпоративной электронной почты.

2. Содержание дисциплины

2.1. Содержание разделов дисциплины

№ семестра	№ раздела	Наименование раздела дисциплины	Содержание раздела в дидактических единицах
1	2	3	4
2	1	**Основные составляющие информационной безопасности**	Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Криптографические методы защиты и шифрование. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности
2	2	**Криптографические способы защиты информации**	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная

			многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA
2	3	**Антивирусная защита**	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы
2	4	**Сетевая безопасность**	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS

2.2. Перечень лабораторных работ

Лабораторная работа №1. Написание, ввод, отладка и тестирование программ шифрования подстановкой

Лабораторная работа №2. Написание, ввод, отладка и тестирование программ шифрования перестановкой, аналитически и гаммированием

Лабораторная работа № 3. Написание, ввод, отладка и тестирование программ шифрования методом контекстного моделирования, словарными алгоритмами

Лабораторная работа №4. Диагностика антивирусной программы и создание тестовых вирусов

Лабораторная работа №5 Создание цифровой подписи

3. Самостоятельная работа студента

Самостоятельная работа осуществляется в объеме 72 часов.

Видами СРС являются:

- изучение литературы и других источников;
- выполнение индивидуальных домашних заданий
- подготовка к выполнению лабораторной работы;
- подготовка к защите лабораторной работы.

Формами текущего контроля успеваемости являются:

- защита лабораторных работ.

4. Оценочные средства для контроля успеваемости и результатов освоения учебной дисциплины (*см. Фонд оценочных средств*)

4.2. Рейтинговая система оценки знаний обучающихся по учебной дисциплине

Рейтинговая система не используется.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

№ п/п	Автор (ы), наименование, место издания и издательство, год
1	2
1	Конеев, Искандер. Информационная безопасность предприятия [Текст] / И.Конеев, А.Беляев. - СПб. : БХВ-Петербург, 2003. - 752с. : ил. - ISBN 5-94157-280-88 : 218-30.
2	Штарьков, Ю. М. Универсальное кодирование: Теория и алгоритмы [Электронный ресурс] / Ю. М. Штарьков. – М. : Физматлит, 2013. – 280 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=275569 (дата обращения 12.08.2020).

5.2. Дополнительная литература

№ п/п	Автор (ы), наименование, место издания и издательство, год
1	2
1	Буза, М. К. Архитектура компьютеров [Электронный ресурс] : учебник / М. К. Буза. – Минск : Вышэйшая школа, 2015. – 416 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=449925 (дата обращения 12.08.2020).
2	Внуков, А. А. Защита информации [Электронный ресурс] : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. – 2-е изд., испр. и доп. – М. : Издательство Юрайт, 2017. – 261 с. – Режим доступа: https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1 (дата обращения 12.08.2020).
3	Долозов, Н. Л. Программные средства защиты информации [Электронный ресурс] : конспект лекций / Н. Л. Долозов, Т. А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск : НГТУ, 2015. – 63 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438307 (дата обращения 12.08.2020).
4	Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю.Н. Загинайлов. – М. ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения 12.08.2020).
5	Осокин, А. Н. Теория информации [Электронный ресурс] : учебное пособие для прикладного бакалавриата / А. Н. Осокин, А. Н. Мальчуков. – М. : Издательство Юрайт, 2017. – 205 с. – Режим доступа: https://www.biblio-online.ru/book/1D5E1FA9-0F42-4040-A1F4-269E2063616F (дата обращения 12.08.2020).
	Петренко, В. И. Теоретические основы защиты информации же [Электронный ресурс] : учебное пособие / В. И. Петренко ; Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации. – Ставрополь : СКФУ, 2015. – 222 с. – Режим доступа:

	http://biblioclub.ru/index.php?page=book&id=458204 (дата обращения 12.08.2020).
	Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения 12.08.2020).

5.3. Базы данных, информационно-справочные и поисковые системы

1. BOOK.ru [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: https://www.book.ru (дата обращения: 12.08.2020).
2. East View [Электронный ресурс] : [база данных]. – Доступ к полным текстам из сети РГУ имени С.А. Есенина. – Режим доступа: https://dlib.eastview.com (дата обращения: 12.08.2020).
3. Moodle [Электронный ресурс] : среда дистанционного образования / Ряз.гос.ун-т. – Рязань, [Б.г.]. – Доступ, после регистрации из сети РГУ имени С.А. Есенина. – Режим доступа: https://e-learn2.rsu.edu.ru/moodle2 (дата обращения: 12.08.2020).
4. Znanium.com [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: https://znanium.com (дата обращения: 12.08.2020).
5. Труды преподавателей [Электронный ресурс] : коллекция // Электронная библиотека Научной библиотеки РГУ имени С.А. Есенина. – Режим доступа к полным текстам по паролю: http://dspace.rsu.edu.ru/xmlui/handle/123456789/3 (дата обращения: 12.08.2020).
6. Университетская библиотека ONLINE [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://biblioclub.ru/index.php?page=main_ub_red (дата обращения: 12.08.2020).
7. Электронный каталог диссертаций [Электронный ресурс] : официальный сайт / Рос.гос.б-ка. – Москва : Рос.гос.б-ка, 2003. – Доступ к полным текстам из комплексного читального зала НБ РГУ имени С.А. Есенина. – Режим доступа: http://diss.rsl.ru (дата обращения: 12.08.2020).
8. Юрайт [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: https://www.biblio-online.ru (дата обращения: 12.08.2020).

5.4. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://elibrary.ru/defaultx.asp, свободный (дата обращения: 12.08.2020).
2. КиберЛенинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://cyberleninka.ru, свободный (дата обращения: 12.08.2020).
3. Википедия [Электронный ресурс] : свободная энцикл. – Режим доступа: http://ru.wikipedia.org/wiki, свободный (дата обращения: 12.08.2020).
4. ИНТУИТ [Электронный ресурс] : Национальный Открытый Университет. – Режим доступа: http://www.intuit.ru, свободный (дата обращения: 12.08.2020).
5. Российский общеобразовательный портал [Электронный ресурс] : [образовательный портал]. – Режим доступа: http://www.school.edu.ru, свободный (дата обращения: 12.08.2020).
6. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] : федеральный портал. – Режим доступа: http://school-collection.edu.ru, свободный (дата обращения: 12.08.2020).

7. Ватолин, Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео [Электронный ресурс] / Д. Ватолин [и др.]. – М.: ДИАЛОГ-МИФИ, 2002. – 384 с. – Режим доступа: http://www.compression.ru/book, свободный (дата обращения: 12.08.2020).
8. Сэломон, Д. Сжатие данных, изображения и звука [Электронный ресурс] / Д. Сэломон. – М.: Техносфера, 2004. – 367 с. – Режим доступа: http://da.kalinin.ru/books/salmon.pdf, свободный (дата обращения: 12.08.2020).

5.5. Периодические издания

1. Компьютерные и информационные науки. Доступ: Киберленинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: https://cyberleninka.ru/article/c/computer-and-information-sciences, свободный (дата обращения: 12.08.2020).

6. Материально-техническое обеспечение дисциплины

6.1. Требования к аудиториям (помещениям, местам) для проведения занятий: специализированные лекционные аудитории, оборудованные видеопроекционным оборудованием для презентаций.

6.2. Требования к оборудованию рабочих мест преподавателя и обучающихся: видеопроектор, ноутбук, переносной экран, для проведения демонстраций, рабочие места обучающихся оснащены ПК с доступом в Интернет.

6.3. Требования к специализированному оборудованию отсутствуют

7. Методические указания для обучающихся по освоению дисциплины

Вид учебных занятий	Организация деятельности студента
Лекция	Освоение дисциплины идет с помощью объектно-ориентированных сред языков программирования. Учитывая, что курс выстроен по разделам, большинство из которых охватывает теоретические вопросы, преподавателю необходимо соблюсти баланс между количеством материала на самостоятельную работу и лабораторными работами. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям*:* *Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Цифровая подпись. Установление подлинности объекта. Управление ключами. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. угрозы, атаки, целостность, аутентификация, конфиденциальность, доступность, хэш-функции, антивирусы, сигнатуры, эвристический анализ, брандмауэры, шифрование перестановкой, подстановкой, гаммирование*
Лабораторная работа	Лабораторные работы, предложенные в данном курсе, выстраиваются в схему практического освоения алгоритмов криптографии и изучения антивирусной защиты, на изучение которых и нацелены. В лекционной части курса описание работы в антивирусных системах не предусмотрено, поэтому рекомендуется преподавателям давать задание на самостоятельный поиск и изучение сетевого антивирусного ПО. Наилучшим вариантом может служить предоставление лабораторных работ в виде прак-

	тикума с непременной практико-теоретической частью в электронном виде, где были бы представлены практические приемы работы, описание основных инструментов архивации, необходимых для выполнения задания конкретной темы лабораторной работы. В соответствии с запланированным на самостоятельную работу временем изучить соответствующий теоретический материал и практические рекомендации. В соответствии с запланированным на самостоятельную работу временем составить схемы алгоритмов и программы решения соответствующего варианта учебной задачи. Согласовать заранее составленные схемы и программы с преподавателем, ведущим занятие. Тексты программ должны содержать короткие комментарии, отражающие тему и номер лабораторной работы, номер варианта, фамилию студента, связь тех или иных переменных с условием задачи, а также комментарии, отражающие основные шаги алгоритмов. Защитить оформленную лабораторную работу, продемонстрировав теоретические и практические знания, умения и навыки по соответствующей теме.
Подготовка к экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, типовые практические задания и др.

8. Требования к программному обеспечению учебного процесса

Название ПО	№ лицензии
Операционная системаWindowsPro	Договор №65/2019 от 02.10.2019
Антивирус KasperskyEndpointSecurity	Договор № 14-3К-2020 от 06.07.2020г.
Офисное приложениеLibreOffice	Свободно распространяемое ПО
Архиватор 7-zip	Свободно распространяемое ПО
Браузеризображений Fast Stone ImageViewer	Свободно распространяемое ПО
PDFридерFoxitReader	Свободно распространяемое ПО
Медиа проигрывательVLCmediaplayer	Свободно распространяемое ПО
Запись дисков ImageBurn	Свободно распространяемое ПО
DJVU браузерDjVuBrowser Plug-in	Свободно распространяемое ПО

9. Иные сведения

Нет

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ С.А. ЕСЕНИНА»

Утверждаю:
Декан физико-математического
факультета
Н.Б. Федорова
«31» августа 2020 г.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Математические основы защиты информации и информационной безопасности

Направление подготовки
02.04.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) подготовки
Информационные системы

Квалификация
Магистратура

Форма обучения
Очная

Рязань, 2020

1. Цель освоения дисциплины

Целью освоения учебной дисциплины «Математические основы защиты информации и информационной безопасности» является формирование у обучающихся общекультурных и профессиональных компетенций в процессе изучения информатики и программирования для последующего применения в учебной и практической деятельности:

- систематизация, формализация и расширение знаний по основным положениям теории информации, математическими моделями и стандартами шифрования;
- изучение математических основ защиты информации: арифметики целых чисел, модульной арифметики, теории чисел, а так же методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и связи;
- изучение понятия информационной безопасности, включая аппаратную часть и математическое обеспечение;
- привитие навыков работы с методами шифрования и криптоанализа
- формирование современной культуры программирования

2. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.03 «Математические основы защиты информации и информационной безопасности» относится к части, формируемой участниками образовательных отношений Блока 1.

Дисциплина изучается на 1 курсе (2 семестр)

3. Трудоемкость дисциплины: 4 зачетные единицы, 144 академических часа.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы и индикаторами достижения компетенций:

ПК-1.1. Знает основы научно-исследовательской деятельности в области информационных технологий, владеет знанием основ философии и методологии науки; знанием методов научных исследований и навыками их проведения

ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности

5. Форма промежуточной аттестации и семестр прохождения

Экзамен (2 семестр).

Дисциплина реализуется частично с применением дистанционных образовательных технологий.