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
«30» августа 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Уровень основной профессиональной образовательной программы: **бакалавриат**

Направление подготовки: **02.03.03 Математическое обеспечение и администрирование информационных систем**

Направленность (профиль) подготовки: **Администрирование информационных систем**

Форма обучения: **очная**

Срок освоения ОПОП: **нормативный срок освоения 4 года**

Факультет: **физико-математический**

Кафедра: **Информатики, вычислительной техники и методики преподавания информатики**

Рязань, 2019

Вводная часть

1. Цели освоения дисциплины

Целью освоения дисциплины «Криптографические методы защиты информации» является формирование у обучающихся 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 сжатия данных;
- изучение методов, средств и инструментов сжатия данных, 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 антивирусными пакетами и алгоритмами шифрования и криптографии, архиваторами;
- формирование теоретической базы и практических умений и навыков для решения задач создания архиваторов и антивирусных алгоритмов.

2. Место дисциплины в структуре ОПОП ВУЗА

2.1. Дисциплина Б1.В.ДВ.05.02 «Криптографические методы защиты информации» относится к дисциплинам по выбору части Блока 1, формируемой участниками образовательных отношений.

2.2. Для изучения дисциплины «Криптографические методы защиты информации» необходимы предшествующие дисциплины:

- «Основы программирования»
- «Объектно-ориентированное и визуальное программирование»
- «Математический анализ»

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

- Производственная практика
- Итоговая государственная аттестация.

2.4. Перечень планируемых результатов обучения по дисциплине «Криптографические методы защиты информации», соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Изучение данной дисциплины направлено на формирование у обучающих 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	ПКВ-2. Способен осуществлять выбор компонентов и администрирование информационных систем организации	ПКВ-2.2. Способен управлять правами и контролировать права доступа пользователей к программно-аппаратным средствам информационных систем организации, осуществлять мониторинг и восстановление работоспособности программно-аппаратных средств информационных систем и их компонентов	• математические принципы сжатия данных; • математические модели сжатия видео и аудио-информации; • математические принципы, лежащие в основе криптографических моделей • этапы решения задачи на компьютере; • терминологию из области криптологии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений; • основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики; • математические криптологические модели, включая средства описания; • современные системы сетевой безопасности; • антивирусные системы, их особенности и основные характеристики	• уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов сжатия и шифрования • уметь применять современные технологии создания брандмауэров и IDS-комплексов; • пользоваться современным инструментарием сжатия данных; разрабатывать алгоритмы сжатия данных, основанные на стандартных методах	• владеть алгоритмическими языками для разработки прикладных алгоритмов сжатия данных • владеть навыками решения задач криптоанализа и шифрования • Навыками создания архиваторов на основе стандартных алгоритмов сжатия • Приемами обнаружения вирусных угроз • Приемами обнаружения сетевых проникновений • Навыками работы по обнаружению и защите от DDOS-атак • Навыками защиты информации с помощью криптосистем

ОСНОВНАЯ ЧАСТЬ

1. Объем дисциплины и виды учебной работы

Вид учебной работы		Всего часов	Семестры № 6 часов
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)		**36**	**36**
В том числе:			
Лекции (Л)		18	18
Лабораторные работы (ЛР)		18	18
Самостоятельная работа студента (всего)		**72**	**72**
В том числе:			
Изучение литературы и других источников		18	18
Подготовка к выполнению лабораторных работ		18	18
Подготовка к защите лабораторных работ		36	36
Вид промежуточной аттестации	**зачет (З)**		+
ИТОГО: общая трудоемкость	**часов**	**108**	**108**
	зач. ед.	**3**	**3**

2. Содержание дисциплины

2.1. Содержание разделов дисциплины

№ семестра	№ раздела	Наименование раздела дисциплины	Содержание раздела в дидактических единицах
1	2	3	4
8	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

1	2	3	4
8	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
8	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
8	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. Контролеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS
8	5	**Элементы теории информации**	Введение в статистическую теорию информации. Определение количества информации по Шеннону. Сжатие данных методом кодирования неравномерным кодом. Количество информации в автокоррелирущем сообщении. Основы статистической теория информации. Определение количества информации по Колмогорову. Тождественность информации, алгоритма, вычислимой функции. Обоснование словарных методов сжатия данных.

1	2	3	4
8	6	**Алгоритмы сжатия без потерь**	Статистические методы сжатия данных : Алгоритм Шеннона - Фано. Алгоритм Хаффмана. Арифметическое кодирование. Словарные методы сжатия данных : Кодирование длин серий. LZW. Алгоритм Барроуза-Вилье.
8	7	**Алгоритмы сжатия данных с потерями**	Сжатие графической информации : RLE-кодирование; Дискретно-косинусное преобразование; Дискретное вейвлет-преобразование; фрактальное сжатие; Сжатие звука: Частотные преобразования; Коррекция спектра звукового сигнала. Общие принципы сжатия видео.

2.2. Лабораторный практикум

№ семестра	№ раздела	Наименование раздела дисциплины	Наименование лабораторных работ	Всего часов
1	2	3	4	5
6	2	**Криптографические способы защиты информации**	ЛР №1. *Написание, ввод, отладка и тестирование программ шифрования подстановкой*	2
			ЛР №2. *Написание, ввод, отладка и тестирование программ шифрования перестановкой, аналитически и гаммированием*	2
6	3	**Антивирусная защита**	ЛР №4. *Диагностика антивирусной программы и создание тестовых вирусов*	2
6	4	**Сетевая безопасность**	ЛР №4. *Парольная аутентификация*	4
6	6	**Алгоритмы сжатия без потерь**	ЛР №5. *Написание, ввод, отладка и тестирование программ сжатия методом Шеннона-Фэно, Хаффмана и арифметическим кодированием*	4
6	7	**Алгоритмы сжатия данных с потерями**	ЛР №6. *Написание, ввод, отладка и тестирование программ кодирования методом RLE-кодирования, BWT-кодирования*	2
6	8	**Современные стандарты сжатия данных**	ЛР №7. Сравнительный анализ работы различных архиваторов с файлами разных форматов и вычисление степени сжатия для каждого архиватора	2
		ИТОГО		**18**

3. Самостоятельная работа студента

Самостоятельная работа осуществляется в объеме 72 часов.
Видами СРС являются:

- изучение и конспектирование литературы по дисциплине;
- подготовка к лабораторным занятиям;
- подготовка к защите лабораторных работ

Формами текущего контроля успеваемости являются:

- Защита лабораторных работ

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации освоения

(*см. Фонд оценочных средств*)

4.1. Рейтинговая система оценки знаний обучающихся по учебной дисциплине

Рейтинговая система не используется.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

№	Наименование Авторы Год, место издания
1	Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео.[Электронный ресурс] - /Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин.М. - Диалог-МИФИ, 2002 – Режим доступа : Http// www.compression.ru/ (дата обращения 30.08.2019)
2	Конеев И.Р. Информационная безопасность предприятия. [Текст]./ И.Р.Конеев, А.В.Беляев. - СПб.: БХВ-Петербург, 2003 – 752 с.
3	*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. — (Бакалавр и магистр. Академический курс). — Режим доступа : https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1 (дата обращения 30.08.2019)
4	Нестеров, С. А. Информационная безопасность .[Электронный ресурс] : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — Режим доступа : https://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7 (дата обращения 30.08.2019)

5.2. Дополнительная литература

№	Наименование Авторы Год, место издания
4	*Лось, А. Б.* Криптографические методы защиты информации .[Электронный ресурс] : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2017. — 473 с. — Режим доступа : https://www.biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A (дата обращения 30.08.2019)
	Запечников, С. В. Криптографические методы защиты информации .[Электронный ресурс] : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М. : Издательство Юрайт, 2017. — 309 с. — Режим доступа : https://www.biblio-online.ru/book/B27D8A2B-F86C-4F18-9F21-3E0695C0A4C0 (дата обращения 30.08.2019)

5.3. Базы данных, информационно-справочные и поисковые системы

1. BOOK.ru [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://www.book.ru (дата обращения: 30.08.2019).
2. East View [Электронный ресурс] : [база данных]. – Доступ к полным текстам статей научных журналов из сети РГУ имени С.А. Есенина. – Режим доступа: http:/dlib.eastview.com (дата обращения: 30.08.2019).
3. Moodle [Электронный ресурс] : среда дистанционного обучения / Ряз. гос. ун-т. – Рязань, [Б.г.]. – Доступ, после регистрации из сети РГУ имени С.А. Есенина, из любой точки, имеющей доступ к Интернету. – Режим доступа: http://e-learn2.rsu.edu.ru/moodle2 (дата обращения: 30.08.2019).
4. Znanium.com [Электронный ресурс] : [база данных]. – Доступ к полным текстам по паролю. – Режим доступа: http://znanium.com (дата обращения: 30.08.2019).
5. «Издательство «Лань» [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://e-lanbook.com (дата обращения: 30.08.2019).
6. Университетская библиотека ONLINE [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://www.biblioclab.ru (дата обращения: 30.08.2019).

7. Юрайт [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://www.biblio-online.ru (дата обращения: 30.08.2019).

8. Труды преподавателей [Электронный ресурс] : коллекция // Электронная библиотека Научной библиотеки РГУ имени С.А. Есенина. – Доступ к полным текстам по паролю. – Режим доступа: http://dspace.rsu.edu.ru/xmlui/handle/123456789/3 (дата обращения: 30.08.2019).

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: 30.08.2019).
2. Prezentacya.ru [Электронный ресурс] : образовательный портал. – Режим доступа: http://prezentacya.ru/, свободный (дата обращения: 30.08.2019).
3. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] : федеральный портал. – Режим доступа: http://school-collection.edu.ru/, свободный (дата обращения: 30.08.2019).
4. Единое окно доступа к образовательным ресурсам [Электронный ресурс] : федеральный портал. – Режим доступа: http://window.edu.ru/, свободный (дата обращения: 30.08.2019).
5. Интернет Университет Информационных технологий. [Электронный ресурс] : сайт. – Режим доступа: http://www.intuit.ru/, свободный (дата обращения 30.08.2019).
6. КиберЛенинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://cyberleninka.ru, свободный (дата обращения: 30.08.2019).
7. Российский общеобразовательный портал [Электронный ресурс] : образовательный портал. – Режим доступа: http://www.school.edu.ru/, свободный (дата обращения: 30.08.2019).
8. Российское образование [Электронный ресурс] : федеральный портал. – Режим доступа: http://www.edu.ru/, свободный (дата обращения: 30.08.2019).
9. Федеральный центр информационно-образовательных ресурсов [Электронный ресурс] : Единое окно доступа к образовательным ресурсам. – Режим доступа: http://fcior.edu.ru, свободный (дата обращения: 30.08.2019).

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: 30.08.2019).
2. Электротехника, электронная техника, информационные технологии. Доступ: Киберленинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: https://cyberleninka.ru/article/c/electrical-electronic-information-engineering, свободный (дата обращения: 30.08.2019).

3. Архив научных статей из журнала «Информационная безопасность» [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/articles, свободный (дата обращения: 30.08.2019).

6. Материально-техническое обеспечение дисциплины

6.1. Требования к аудиториям для проведения занятий:

Класс персональных компьютеров под управлением MS Windows, включенных в локальную сеть университета с возможностью выхода в Internet.

Стандартно оборудованные лекционные аудитории с мультимедиапроектором, подключенным к компьютеру, настенным экраном.

6.2. Требования к оборудованию рабочих мест преподавателя и обучающихся:

Персональный компьютер под управлением MS Windows, Microsoft Office, системы программирования Turbo-Pascal и Turbo-C++, Delphi, и другие, комплект архиваторов, файлов для архивации, антивирус.

6.3. Требования к специализированному оборудованию: *отсутствует*

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*:* *Энтропия, кодирование, код Хаффмана, вероятность появления символа в блоке, поток, арифметическое кодирование, вэйвлет-сжатие, фрактал, словарное кодирование, BWT-преобразование, угрозы, атаки, целосность, аутентификация, конфидициальность, 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 базовых алгоритмов сжатия данных и криптографии, 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 практикума 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 (раздел 3.1) 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 зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, типовые практические задания и др.

8. Требования к программному обеспечению учебного процесса

1. Операционная система Windows Pro (договор №Tr000043844 от 22.09.15г.);
2. Антивирус Kaspersky Endpoint Security (договор №14/03/2019-0142 от 30/03/2019г.);
3. Офисное приложение LibreOffice (свободно распространяемое ПО);
4. Архиватор 7-zip (свободно распространяемое ПО);
5. Браузер изображений FastStoneImageViewer (свободно распространяемое ПО);
6. PDF ридер FoxitReader (свободно распространяемое ПО);
7. PDF принтер doPdf (свободно распространяемое ПО);
8. Медиа проигрыватель VLC media player (свободно распространяемое ПО);
9. Запись дисков ImageBurn (свободно распространяемое ПО);
10. DJVU браузер DjVu Browser Plug-in (свободно распространяемое ПО).