

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.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**МЕТОДЫ СЖАТИЯ ДАННЫХ И 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, 2020

## **Вводная часть**

### **1. Цели освоения дисциплины**

Целью освоения дисциплины «Методы сжатия данных и защиты информации» является формирование у обучающихся общепрофессиональных 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 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,
- формирование современной культуры программирования.

### **2. Место дисциплины в структуре ОПОП бакалавриата**

**2.1.** Дисциплина Б1.В.ОД.11 «Методы сжатия данных и защиты информации» относится к вариативной части блока Б1 (обязательные дисциплины).

**2.2.** Для изучения дисциплины «Методы сжатия данных и защиты информации» необходимы предшествующие дисциплины:

- «Информатика и программирование»
- «Объектно-ориентированные языки и системы»
- «Математический анализ»

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

- Производственная практики
- Итоговая государственная аттестация.

**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 общепрофессиональных (ОПК) и профессиональных (ПК) компетенций:**

№ п/п	Номер/индекс компетенции	Содержание компетенции (или ее части)	Перечень планируемых результатов обучения по дисциплине В результате изучения дисциплины обучающиеся должны:		
			Знать:	Уметь:	Владеть (навыками):
1	2	3	4	5	6
1	ОПК-2	способность применять в профессиональной деятельности знания математических основ информатики;	математические принципы сжатия данных; математические модели сжатия видео и аудиоинформации; математические принципы, лежащие в основе криптографических моделей	уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов сжатия и шифрования	владеть алгоритмическими языками для разработки прикладных алгоритмов сжатия данных владеть навыками решения задач криптоанализа и шифрования
2	ПК-2	готовность к использованию основных моделей информационных технологий и способов их применения для решения задач в предметных областях;	<ul style="list-style-type: none"> <li>• этапы решения задачи на компьютере;</li> <li>• терминологию из области криптологии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений;</li> <li>• основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики;</li> <li>• математические криптологические модели, включая средства описания;</li> <li>• современные системы сетевой безопасности;</li> <li>• антивирусные системы, их особенности и основные характеристики;</li> <li>• теоретические основы определения количества информации,</li> <li>• современные методы сжатия данных,</li> <li>• особенности сжатия различных видов информации,</li> <li>• современные стандарты сжатия данных, области их применения.</li> </ul>	<ul style="list-style-type: none"> <li>• уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач;</li> <li>• уметь использовать математические модели для построения криптологических систем;</li> <li>• уметь применять современные технологии создания брандмауэров и IDS-комплексов;</li> <li>• пользоваться современным инструментарием сжатия данных; разрабатывать алгоритмы сжатия данных, основанные на стандартных методах</li> </ul>	<ul style="list-style-type: none"> <li>• основными методами, способами и средствами шифрования и криптографии;</li> <li>• навыками проектирования, отладки и тестирования программ в средах, по крайней мере, трех императивных систем программирования</li> <li>• навыками работы с архиваторами различного типа</li> <li>• Навыками создания архиваторов на основе стандартных алгоритмов сжатия</li> <li>• Приемами обнаружения вирусных угроз</li> <li>• Приемами обнаружения сетевых проникновений</li> <li>• Навыками работы по обнаружению и защите от DDOS-атак</li> <li>• Навыками защиты информации с помощью криптосистем</li> </ul>

## 2.5 Матрица компетенций

КАРТА КОМПЕТЕНЦИЙ ДИСЦИПЛИНЫ					
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ: МЕТОДЫ СЖАТИЯ ДАННЫХ И ЗАЩИТЫ ИНФОРМАЦИИ					
Цель дисциплины	Целями освоения дисциплины «Методы сжатия данных и защиты информации» является формирование у обучающихся общепрофессиональных и профессиональных компетенций в процессе изучения информатики и программирования для последующего применения в учебной и практической деятельности				
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие					
Общепрофессиональные компетенции:					
КОМПЕТЕНЦИИ		Перечень компонентов	Технологии формирования	Форма оценочного средства	Уровни освоения компетенций
ИНДЕКС	ФОРМУЛИРОВКА				
1	2	3	4	5	6
ОПК-2	способность применять в профессиональной деятельности знания математических основ информатики;	<p>Знать:</p> <p>математические принципы сжатия данных; математические модели сжатия видео и аудиоинформации, математические принципы, лежащие в основе криптографических моделей</p> <p>Уметь:</p> <p>использовать алгоритмические модели и языки программирования для разработки алгоритмов сжатия.</p> <p>использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования</p> <p>Владеть:</p> <p>владеть алгоритмическими языками для разработки прикладных алгоритмов сжатия данных</p> <p>владеть навыками решения задач криптоанализа и шифрования</p>	<p>Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий, организации самостоятельной работы студентов</p>	Лабораторные работы, зачет	<p><b>Пороговый</b></p> <p>Способен решать стандартные задачи</p> <p><b>Повышенный</b></p> <p>Способен решать задачи криптографии и сжатия повышенной сложности</p>
ПК-2	готовность к использованию основных моделей информационных технологий и способов их применения для ре-	<p>Знать:</p> <p>терминологию из области криптологии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений; основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики; мате-</p>	<p>Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий, организации</p>	Лабораторные работы, зачет	<p><b>Пороговый</b></p> <p>Способен находить, анализировать и контекстно обрабатывать учебную научно-техническую информацию с помощью обучающего</p>

	<p>шения задач в предметных областях;</p>	<p>математические криптологические модели, включая их средства описания;  современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики;  теоретические основы определения количество информации, современные методы сжатия данных, особенности сжатия различных видов информации, современные стандарты сжатия данных, области их применения.  Уметь:  <ul style="list-style-type: none"> <li>• уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач;</li> <li>• уметь использовать математические модели для построения криптологических систем;</li> <li>• уметь применять современные технологии создания брандмауэров и IDS-комплексов;</li> <li>• пользоваться современным инструментарием сжатия данных; разрабатывать алгоритмы сжатия данных, основанные на стандартных методах</li> </ul> Владеть:  <ul style="list-style-type: none"> <li>• основными методами, способами и средствами шифрования и криптографии;</li> <li>• навыками проектирования, отладки и тестирования программ в средах, по крайней мере, трех императивных систем программирования</li> <li>• навыками работы с архиваторами различного типа</li> <li>• Навыками создания архиваторов на основе стандартных алгоритмов сжатия</li> <li>• Приемами обнаружения вирусных угроз</li> <li>• Приемами обнаружения сетевых проникновений</li> <li>• Навыками работы по обнаружению и защите от DDOS-атак</li> </ul> Навыками защиты информации с помощью криптосистем</p>	<p>самостоятельной работы студентов</p>		<p><b>Повышенный</b>  Способен самостоятельно находить, анализировать и контекстно обрабатывать научно-техническую информацию</p>
--	---	--	---	--	---

# ОСНОВНАЯ ЧАСТЬ

## 1. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестры
		№ 8 часов
		-
<b>Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)</b>	<b>108</b>	<b>108</b>
В том числе:		
Лекции (Л)	24	24
Лабораторные работы (ЛР)	24	24
<b>Самостоятельная работа студента (всего)</b>	<b>60</b>	<b>60</b>
В том числе:		
Изучение литературы и других источников	35	35
Подготовка к выполнению лабораторных работ	11	11
Подготовка к защите лабораторных работ	14	14
<b>Вид промежуточной аттестации</b>	<b>зачет (З)</b>	<b>+</b>
<b>ИТОГО: общая трудоемкость</b>	<b>часов</b>	<b>108</b>
	<b>зач. ед.</b>	<b>3</b>

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
8	1	<b>Основные составляющие информационной безопасности</b>	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	<b>Криптографические способы защиты информации</b>	<p>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</p>
8	3	<b>Антивирусная защита</b>	<p>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</p>
8	4	<b>Сетевая безопасность</b>	<p>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</p>

8	5	<b>Элементы теории информации</b>	Введение в статистическую теорию информации. Определение количества информации по Шеннону. Сжатие данных методом кодирования неравномерным кодом. Количество информации в автокоррелирующем сообщении. Основы статистической теории информации. Определение количества информации по Колмогорову. Тождественность информации, алгоритма, вычислимой функции. Обоснование словарных методов сжатия данных.
8	6	<b>Алгоритмы сжатия без потерь</b>	Статистические методы сжатия данных: Алгоритм Шеннона - Фано. Алгоритм Хаффмана. Арифметическое кодирование. Словарные методы сжатия данных: Кодирование длин серий. LZW. Алгоритм Барроуза-Вилье.
8	7	<b>Алгоритмы сжатия данных с потерями</b>	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.
8	8	<b>Современные стандарты сжатия данных</b>	Архиваторы Zip, gZip, Rar, 7-Zip. Форматы GIF, PNG, JPEG, TIFF. Форматы ALAC, FLAC, RAL, MPEG-4 ALS, WavPack, WMA, MP3. Форматы DivX, MPEG-1, MPEG-2, MPEG-4, RealMedia, Windows Media Video.

## 2.2. Разделы дисциплины, виды учебной деятельности и формы контроля

№ семестра	№ раздела	Наименование раздела дисциплины	Виды учебной деятельности, включая самостоятельную работу студентов (в часах)				Формы текущего контроля успеваемости (по неделям семестра)	
			Л	ЛР	СРС	всего		
8	1	<b>Основные составляющие информационной безопасности</b>	2	2	2	6	1 неделя:	
8	2	<b>Криптографические способы защиты информации</b>	4	6	14	24	2,3 неделя: ЛР №1 4 неделя: ЛР №2	
8	3	<b>Антивирусная защита</b>	2	4	5	11	5 неделя: ЛР №3 6 неделя: ЛР №4	
8	4	<b>Сетевая безопасность</b>	4	-	6	10	5, 6 неделя:	
8	5	<b>Элементы теории информации</b>	2	-	4	6	7 неделя:	
8	6	<b>Алгоритмы сжатия без потерь</b>	4	6	11	21	7 – 9 неделя: ЛР №5	
8	7	<b>Алгоритмы сжатия данных с потерями</b>	4	4	14	22	10, 11 неделя:  ЛР №6	
8	8	<b>Современные стандарты сжатия данных</b>	2	2	4	8	12 неделя: ЛР №7	
		<b>ИТОГО семестр</b>	<b>8</b>	<b>24</b>	<b>24</b>	<b>60</b>	<b>108</b>	<b>ПрАг - Зачет</b>

### 2.3. Лабораторный практикум

№ семестра	№ раздела	Наименование раздела дисциплины	Наименование лабораторных работ	Всего часов
8	1	<b>Основные составляющие информационной безопасности</b>	ЛР вводная. Знакомство с антивирусными программами, брандмауэрами, архиваторами	2
8	2	<b>Криптографические способы защиты информации</b>	ЛР №1. Написание, ввод, отладка и тестирование программ шифрования подстановкой	3
			ЛР №2. Написание, ввод, отладка и тестирование программ шифрования перестановкой, аналитическим и гаммированием	3
8	3	<b>Антивирусная защита</b>	ЛР №4. Диагностика антивирусной программы и создание тестовых вирусов	2
8	4	<b>Сетевая безопасность</b>	ЛР №4. Парольная аутентификация	2
8	5	<b>Элементы теории информации</b>	ЛР по данному разделу не предусмотрена	
8	6	<b>Алгоритмы сжатия без потерь</b>	ЛР №5. Написание, ввод, отладка и тестирование программ сжатия методом Шеннона-Фэнно, Хаффмана и арифметическим кодированием	6
8	7	<b>Алгоритмы сжатия данных с потерями</b>	ЛР №6. Написание, ввод, отладка и тестирование программ сжатия методом RLE-кодирования, BWT-кодирования	4
8	8	<b>Современные стандарты сжатия данных</b>	ЛР №7. Сравнительный анализ работы различных архиваторов с файлами разных форматов и вычисление степени сжатия для каждого архиватора	2
		<b>ИТОГО 8 семестр</b>		<b>24</b>

### 2.4. Примерная тематика курсовых работ

Курсовые работы не предусмотрены по учебному плану

### 3. Самостоятельная работа студента

#### 3.1. Виды СРС

№ семестра	№ раздела	Наименование раздела дисциплины	Виды СРС	Всего часов
1	2	3	4	5
8	1	<b>Основные составляющие информационной безопасности</b>	Изучение литературы и других источников	2
8	2	<b>Криптографические способы защиты информации</b>	Изучение литературы и других источников	4
			Подготовка к выполнению лабораторной работы №1 по теме "Шифрование подстановкой"	2
			Подготовка к защите лабораторной работы (ЛР №1)	3
			Подготовка к выполнению лабораторной работы №2 по теме "Шифрование перестановкой, аналитически и гаммированием"	2
			Подготовка к защите лабораторной работы (ЛР №2)	3
8	3	<b>Антивирусная защита</b>	Изучение литературы и других источников	3
			Подготовка к выполнению лабораторной работы №3 по теме "Диагностика работы антивируса и создание тестовых вирусов"	1
			Подготовка к защите лабораторной работы №3	1
8	4	<b>Сетевая безопасность</b>	Подготовка к выполнению лабораторной работы №4 по теме "Парольная аутентификация"	1
			Подготовка к защите лабораторной работы №4	1
			Изучение литературы и других источников	4
8	5	<b>Элементы теории информации</b>	Изучение литературы и других источников	4
8	6	<b>Алгоритмы сжатия без потерь</b>	Изучение литературы и других источников (основная и дополнительная литература)	5
			Изучение литературы и других источников (конспекты лекций и ресурсы компьютерных сетей)	3
			Подготовка к выполнению лабораторной работы № 5	1
			Подготовка к защите лабораторной работы №5	2
8	7	<b>Алгоритмы сжатия данных с потерями</b>	Изучение литературы и других источников (основная и дополнительная литература)	5
			Изучение литературы и других источников (конспекты лекций и ресурсы компьютерных сетей)	3
			Подготовка к выполнению лабораторной работы №6	3
			Подготовка к защите лабораторной работы №6	3
8	8	<b>Современные стандарты сжатия данных</b>	Изучение литературы и других источников (основная и дополнительная литература)	2
			Подготовка к выполнению лабораторной работы №7	1
			Подготовка к защите лабораторной работы №7	1
		<b>ИТОГО 8 семестр</b>		<b>60</b>
		<b>ИТОГО</b>		<b>60</b>

### 3.2. График работы студента

Семестр № 8

Форма оценочного средства	Усл. обозн.	НЕДЕЛЯ											
		1	2	3	4	5	6	7	8	9	10	11	12
Лабораторная работа	Сб			+	+	+	+		+	+		+	+
Зачет	ЗЛР												+

### 3.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Темы и разделы дисциплины	Учебно-методическое обеспечение для соответствующих тем и разделов
1.Основные составляющие информационной безопасности	http://www.intuit.ru/ Криптографические основы безопасности Автор: О.Р. Лапонина http://www.intuit.ru/ Математика криптографии и теория шифрования Автор: Б.А. Фороузан Переводчик: А.Н. Берлин
2.Криптографические способы защиты информации	
3.Антивирусная защита	Конеев И.Р. Информационная безопасность предприятия. [Текст]./ И.Р.Конеев, А.В.Беляев. - СПб.: БХВ-Петербург, 2003
4.Сетевая безопасность	
5.Элементы теории информации	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 – URL: Http// www.compression.ru/
6.Алгоритмы сжатия без потерь	
7.Алгоритмы сжатия данных с потерями	
8.Современные стандарты сжатия данных	

3.3.1. Контрольные работы/рефераты *не предусмотрены*

#### 4. Оценочные средства для контроля успеваемости и результатов освоения дисциплины (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	Используется при изучении разделов	семестр	Количество экземпляров	
				В библиотеке	На кафедре
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 : <a href="http://www.compression.ru/">Http//www.compression.ru/</a> (дата обращения 31.08.2020)	4-8	8	Электронный ресурс	
2	Конеев И.Р. Информационная безопасность предприятия. [Текст]./ И.Р.Конеев, А.В.Беляев. - СПб.: БХВ-Петербург, 2003 – 752 с.	1-4	8	14	1
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 : <a href="https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1">https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1</a> (дата обращения 31.08.2020)	4-8	8	ЭБС	
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 : <a href="https://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7">https://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7</a> (дата обращения 31.08.2020)	1-4	8	ЭБС	

### 5.2. Дополнительная литература

№	Наименование Авторы Год, место издания	Используется при изучении разделов	семестр	Количество экземпляров	
				В библиотеке	На кафедре
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>
1	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 : <a href="https://www.biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A">https://www.biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A</a> (дата обращения 31.08.2020)	1-8	8	ЭБС	1

1	2	3	4	5	6
2	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 : <a href="https://www.biblio-online.ru/book/B27D8A2B-F86C-4F18-9F21-3E0695C0A4C0">https://www.biblio-online.ru/book/B27D8A2B-F86C-4F18-9F21-3E0695C0A4C0</a> (дата обращения 31.08.2020)	1-8	8	ЭБС	-

### 5.3. Базы данных, информационно-справочные и поисковые системы

1. VOOR.ru [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: <http://www.book.ru> (дата обращения: 31.08.2020).

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: 31.08.2020).

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: 31.08.2020).

4. Znanium.com [Электронный ресурс] : [база данных]. – Доступ к полным текстам по паролю. – Режим доступа: <http://znanium.com> (дата обращения: 31.08.2020).

5. «Издательство «Лань» [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: <http://e-lanbook.com> (дата обращения: 31.08.2020).

6. Университетская библиотека ONLINE [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: <http://www.biblioclub.ru> (дата обращения: 31.08.2020).

7. Юрайт [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: <http://www.biblio-online.ru> (дата обращения: 31.08.2020).

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: 31.08.2020).

### 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: 31.08.2020).

2. Prezentacya.ru [Электронный ресурс] : образовательный портал. – Режим доступа: <http://prezentacya.ru/>, свободный (дата обращения: 31.08.2020).
3. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] : федеральный портал. – Режим доступа: <http://school-collection.edu.ru/>, свободный (дата обращения: 31.08.2020).
4. Единое окно доступа к образовательным ресурсам [Электронный ресурс] : федеральный портал. – Режим доступа: <http://window.edu.ru/>, свободный (дата обращения: 31.08.2020).
5. Интернет Университет Информационных технологий. [Электронный ресурс] : сайт. – Режим доступа: <http://www.intuit.ru/>, свободный (дата обращения 31.08.2020).
6. КиберЛенинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: <http://cyberleninka.ru>, свободный (дата обращения: 31.08.2020).
7. Российский общеобразовательный портал [Электронный ресурс] : образовательный портал. – Режим доступа: <http://www.school.edu.ru/>, свободный (дата обращения: 31.08.2020).
8. Российское образование [Электронный ресурс] : федеральный портал. – Режим доступа: <http://www.edu.ru/>, свободный (дата обращения: 31.08.2020).
9. Федеральный центр информационно-образовательных ресурсов [Электронный ресурс] : Единое окно доступа к образовательным ресурсам. – Режим доступа: <http://fcior.edu.ru>, свободный (дата обращения: 31.08.2020).

## **6. Материально-техническое обеспечение дисциплины**

### **6.1. Требования к аудиториям для проведения занятий:**

Класс персональных компьютеров под управлением MS Windows XP Pro, 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 XP Pro, Microsoft Office, системы программирования Turbo-Pascal и Turbo-C++, Delphi, 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	<p>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.</p> <p>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 удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям:</p> <p><i>Энтропия, кодирование, код Хаффмана, вероятность появления символа в блоке, поток, арифметическое кодирование, вэйвлет-сжатие, фрактал, словарное кодирование, BWT-преобразование, угрозы, атаки, целостность, аутентификация, конфиденциальность, доступность, хэш-функции, антивирусы, сигнатуры, эвристический анализ, брандмауэры, шифрование перестановкой, подстановкой, гаммирование</i></p>
Лабораторная работа	<p>Лабораторные работы, предложенные в данном курсе, выстраиваются в схему практического освоения базовых алгоритмов сжатия данных и криптографии, на изучение которых и нацелены.</p> <p>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 неременной 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.</p> <p>В соответствии с запланированным на самостоятельную работу временем (раздел 3.1) изучить соответствующий теоретический материал и практические рекомендации.</p> <p>В соответствии с запланированным на самостоятельную работу временем составить схемы алгоритмов и программы решения соответствующего варианта учебной задачи.</p> <p>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.</p> <p>Защитить оформленную лабораторную работу, продемонстрировав теоретические и практические знания, умения и навыки по соответствующей теме.</p>

Подготовка к зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, типовые практические задания и др.
---------------------	--

## 8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Для организации учебной и самостоятельной работы обучаемых используется технология удаленного доступа. Для каждой из учебных групп на сервере кафедры ИВТ и МПИ созданы каталоги с соответствующими правами доступа. В каталоге группы создан подкаталог для данной дисциплины, в котором по мере необходимости преподавателем размещаются рабочая программа дисциплины, электронные варианты лекций, электронные обучающие ресурсы, задания к лабораторным работам, графики выполнения лабораторных работ, материалы для самостоятельной работы, контрольные материалы, оценки текущих результатов учебной деятельности обучающихся и др. материалы для организации учебного процесса по данной дисциплине. Материалы, размещенные в каталоге группы доступны любому обучающемуся соответствующей группы посредством локальной компьютерной сети университета с любого рабочего места компьютерных классов кафедры ИВТ и МПИ.

В каталоге группы также для каждого обучающегося создан личный подкаталог, к которому разрешен доступ только обучающемуся и преподавателям кафедры. В личном подкаталоге обучающийся размещает результаты своей учебной деятельности: выполненные лабораторные работы, отчеты и другие результаты.

Для организации учебной работы может использоваться набор веб-сервисов MS office365, вебинарная платформа РГУ имени С.А. Есенина, университетская информационно-образовательная среда Moodle, облачные технологии. Координация учебной работы осуществляется через университетскую электронную почту.

## 9. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ УЧЕБНОГО ПРОЦЕССА

1. Операционная система Windows Pro (договор №65/2019 от 02.10.2019);
2. Антивирус Kaspersky Endpoint Security (договор №14-ЗК-2020 от 06.07.2020г.);
3. Офисное приложение LibreOffice (свободно распространяемое ПО);
4. Архиватор 7-zip (свободно распространяемое ПО);
5. Браузер изображений Fast Stone Image Viewer (свободно распространяемое ПО);
6. PDFридер Foxit Reader (свободно распространяемое ПО);
7. Медиа проигрыватель VLC media player (свободно распространяемое ПО);
8. Запись дисков ImageBurn (свободно распространяемое ПО);
9. DJVU браузер DjVu Browser Plug-in (свободно распространяемое ПО);
10. Набор веб-сервисов MS office365 (бесплатное ПО для учебных заведений <https://www.microsoft.com/ru-ru/education/products/office>);

11. Система электронного обучения Moodle (свободно распространяемое ПО).

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**  
**МЕТОДЫ СЖАТИЯ ДАННЫХ И ЗАЩИТЫ ИНФОРМАЦИИ**

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

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

Квалификация  
**Бакалавриат**

Форма обучения  
**Очная**

Рязань, 2020

### 1. Цель освоения дисциплины

Целью освоения дисциплины «Методы сжатия данных и защиты информации» является формирование у обучающихся общепрофессиональных и профессиональных компетенций в процессе изучения информатики и программирования для последующего применения в учебной и практической деятельности.

### 2. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.ОД.11 «Методы сжатия данных и защиты информации» относится к вариативной части блока Б1 (обязательные дисциплины).

Дисциплина изучается на 4 курсе 8 семестр)

**3. Трудоемкость дисциплины:** 3 зачетные единицы, 108 академических часов.

### 4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы.

№ п/п	Номер/индекс компетенции	Содержание компетенции (или ее части)	Перечень планируемых результатов обучения по дисциплине В результате изучения дисциплины обучающиеся должны:		
			Знать:	Уметь:	Владеть (навыками):
1	2	3	4	5	6
1	ОПК-2	способность применять в профессиональной деятельности знания математических основ информатики;	математические принципы сжатия данных; математические модели сжатия видео и аудиоинформации; математические принципы, лежащие в основе криптографических моделей	уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов сжатия и шифрования	владеть алгоритмическими языками для разработки прикладных алгоритмов сжатия данных владеть навыками решения задач криптоанализа и шифрования

1	2	3	4	5	6
2	ПК-2	готовность к использованию основных моделей информационных технологий и способов их применения для решения задач в предметных областях	<ul style="list-style-type: none"> <li>• этапы решения задачи на компьютере;</li> <li>• терминологию из области криптологии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений;</li> <li>• основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики;</li> <li>• математические криптологические модели, включая средства описания;</li> <li>• современные системы сетевой безопасности;</li> <li>• антивирусные системы, их особенности и основные характеристики;</li> <li>• теоретические основы определения количества информации,</li> <li>• современные методы сжатия данных,</li> <li>• особенности сжатия различных видов информации,</li> <li>• современные стандарты сжатия данных, области их применения.</li> </ul>	<ul style="list-style-type: none"> <li>• уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач;</li> <li>• уметь использовать математические модели для построения криптологических систем;</li> <li>• уметь применять современные технологии создания брандмауэров и IDS-комплексов;</li> <li>• пользоваться современным инструментарием сжатия данных; разрабатывать алгоритмы сжатия данных, основанные на стандартных методах</li> </ul>	<ul style="list-style-type: none"> <li>• основными методами, способами и средствами шифрования и криптографии;</li> <li>• навыками проектирования, отладки и тестирования программ в средах, по крайней мере, трех императивных систем программирования;</li> <li>• навыками работы с архиваторами различного типа;</li> <li>• навыками создания архиваторов на основе стандартных алгоритмов сжатия;</li> <li>• приемами обнаружения вирусных угроз;</li> <li>• приемами обнаружения сетевых проникновений;</li> <li>• навыками работы по обнаружению и защите от DDOS-атак;</li> <li>• навыками защиты информации с помощью криптосистем</li> </ul>

## 5. Форма промежуточной аттестации и семестр прохождения

Зачет (8 семестр).

Дисциплина реализуется частично с применением дистанционных образовательных технологий.