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 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ 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, 2018

Вводная часть

1. Цели освоения дисциплины

Целью освоения учебной 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 следующие знания, умения, навыки, формируемые предшествующими дисциплинами:
- «Информатика и программирование»
- «Объектно-ориентированные языки и системы»
- «Математический анализ»

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения, навыки, формируемые данной учебной 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 учебной дисциплины направлено на формирование у обучающих 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 учебной 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;	• 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; • теоретические основы определения количество информации, • современные методы сжатия данных, • особенности сжатия различных видов информации, • современные стандарты сжатия данных, области их применения.	• уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач; • уметь использовать математические модели для построения криптологических систем; • уметь применять современные технологии создания брандмауэров и IDS-комплексов; • пользоваться современным инструментарием сжатия данных; разрабатывать алгоритмы сжатия данных, основанные на стандартных методах	• основными методами, способами и средствами шифрования и криптографиии; • навыками проектирования, отладки и тестирования программ в средах, по крайней мере, трех императивных систем программирования • навыками работы с архиваторами различного типа • 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

2.5 Матрица компетенций

КАРТА КОМПЕТЕНЦИЙ ДИСЦИПЛИНЫ					
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ: МЕТОДЫ СЖАТИЯ ДАННЫХ И ЗАЩИТЫ ИНФОРМАЦИИ					
Цель дисциплины	Целями освоения учебной 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;	Знать: математические принципы сжатия данных; математические модели сжатия видео и аудио-информации, математические принципы, лежащие в основе криптографических моделей Уметь: использовать алгоритмические модели и языки программирования для разработки алгоритмов сжатия. использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования Владеть: владеть алгоритмическими языками для разработки прикладных алгоритмов сжатия данных владеть навыками решения задач криптоанализа и шифрования	Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий, организации самостоятельной работы студентов	Лабораторные работы, зачет	**Пороговый** Способен решать стандартные задачи **Повышенный** Способен решать задачи криптографии и сжатия повышенной сложности
ПК-2	готовность к использованию основных моделей информационных технологий и способов	Знать: терминологию из области криптологии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений; основные алгоритмы шифрования для решения задач предметной	Путем проведения лекционных, лабораторных занятий, применения новых образовательных	Лабораторные работы, зачет	**Пороговый** Способен находить, анализировать и контекстно обрабатывать учебную научно-техническую информацию с

	их применения для решения задач в предметных областях;	области, их особенности и характеристики; 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: • уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач; • уметь использовать математические модели для построения криптологических систем; • уметь применять современные технологии создания брандмауэров и IDS-комплексов; • пользоваться современным инструментарием сжатия данных; разрабатывать алгоритмы сжатия данных, основанные на стандартных методах Владеть: • основными методами, способами и средствами шифрования и криптографиии; • навыками проектирования, отладки и тестирования программ в средах, по крайней мере, трех императивных систем программирования • навыками работы с архиваторами различного типа • 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	технологий, организации самостоятельной работы студентов		помощи обучающего **Повышенный** Способен самостоятельно находить, анализировать и контекстно обрабатывать научно-техническую информацию

ОСНОВНАЯ ЧАСТЬ

1. Объем учебной дисциплины и виды учебной работы

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

2. Содержание учебной дисциплины

2.1. Содержание разделов учебной дисциплины

№ семестра	№ раздела	Наименование раздела учебной 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
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**.**
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.
8	8	**Современные стандарты сжатия данных**	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 учебной дисциплины, виды учебной деятельности и формы контроля

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

2.3. Лабораторный практикум

№ семестра	№ раздела	Наименование раздела учебной дисциплины	Наименование лабораторных работ	Всего часов
1	2	3	4	5
8	1	**Основные составляющие информационной безопасности**	ЛР вводная. *Знакомство с антивирусными программами, брандмауэрами, архиваторами*	2
8	2	**Криптографические способы защиты информации**	ЛР №1. *Написание, ввод, отладка и тестирование программ шифрования подстановкой*	3
			ЛР №2. *Написание, ввод, отладка и тестирование программ шифрования перестановкой, аналитически и гаммированием*	3
8	3	**Антивирусная защита**	ЛР №4. *Диагностика антивирусной программы и создание тестовых вирусов*	2
8	4	**Сетевая безопасность**	ЛР №4. *Парольная аутентификация*	2
8	5	**Элементы теории информации**	ЛР по данному разделу не предусмотрена	
8	6	**Алгоритмы сжатия без потерь**	ЛР №5. *Написание, ввод, отладка и тестирование программ сжатия методом Шеннона-Фэно, Хаффмана и арифметическим кодированием*	6
8	7	**Алгоритмы сжатия данных с потерями**	ЛР №6. *Написание, ввод, отладка и тестирование программ сжатия методом RLE-кодирования, BWT-кодирования*	4
8	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 8 семестр		**24**

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 учебной дисциплины	Виды СРС	Всего часов
1	2	3	4	5
8	1	**Основные составляющие информационной безопасности**	Изучение литературы и других источников	2
8	2	**Криптографические способы защиты информации**	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	**Антивирусная защита**	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	**Сетевая безопасность**	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	**Элементы теории информации**	Изучение литературы и других источников	4
8	6	**Алгоритмы сжатия без потерь**	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	**Алгоритмы сжатия данных с потерями**	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	**Современные стандарты сжатия данных**	Изучение литературы и других источников (основная и дополнительная литература)	2
			Подготовка к выполнению лабораторной работы №7	1
			Подготовка к защите лабораторной работы №7	1
		ИТОГО 8 семестр		**60**
		ИТОГО		**60**

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 «Методы сжатия данных и защиты информации»

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 учебной 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 : Http// www.compression.ru/ (дата обращения 12.06.18)	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 : https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1 (дата обращения 12.06.18)	4-8	8	ЭБС	
	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 12.06.18)	1-4	8	ЭБС	

5.2. Дополнительная литература

№	Наименование Авторы Год, место издания			Использ-зуется при изучении разделов	се-местр	Количество экземпляров	
						В библио-теке	На кафедре
1	2	3	4	5	6	7	8
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 12.06.18)			1-8	8	ЭБС	1
	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 12.06.18)			1-8	8	ЭБС	-

5.3. Базы данных, информационно-справочные и поисковые системы

1. BOOR.ru [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://www.book.ru (дата обращения: 15.04.2018).
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: 15.04.2018).
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: 15.04.2018).
4. Znanium.com [Электронный ресурс] : [база данных]. – Доступ к полным текстам по паролю. – Режим доступа: http://znanium.com (дата обращения: 15.04.2018).
5. «Издательство «Лань» [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://e-lanbook.com (дата обращения: 15.04.2018).
6. Университетская библиотека ONLINE [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://www.biblioclab.ru (дата обращения: 15.04.2018).
7. Юрайт [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://www.biblio-online.ru (дата обращения: 15.04.2018).
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: 15.04.2018).

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: 15.05.2018).
2. Prezentacya.ru [Электронный ресурс] : образовательный портал. – Режим доступа: http://prezentacya.ru/, свободный (дата обращения: 15.05.2018).
3. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] : федеральный портал. – Режим доступа: http://school-collection.edu.ru/, свободный (дата обращения: 15.05.2018).

4. Единое окно доступа к образовательным ресурсам [Электронный ресурс] : федеральный портал. – Режим доступа: http://window.edu.ru/, свободный (дата обращения: 15.05.2018).

5. Интернет Университет Информационных технологий. [Электронный ресурс] : сайт. – Режим доступа: http://www.intuit.ru/, свободный (дата обращения 10.06.2018).

6. КиберЛенинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://cyberleninka.ru, свободный (дата обращения: 15.05.2018).

7. Российский общеобразовательный портал [Электронный ресурс] : образовательный портал. – Режим доступа: http://www.school.edu.ru/, свободный (дата обращения: 15.05.2018).

8. Российское образование [Электронный ресурс] : федеральный портал. – Режим доступа: http://www.edu.ru/, свободный (дата обращения: 15.05.2018).

9. Федеральный центр информационно-образовательных ресурсов [Электронный ресурс] : Единое окно доступа к образовательным ресурсам. – Режим доступа: http://fcior.edu.ru, свободный (дата обращения: 15.05.2018).

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. Образовательные технологии *(Заполняется только для стандарта ФГОС ВПО)*

8. 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, целостность, 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.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

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 учебной 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.

10. Требования к программному обеспечению учебного процесса

№ п/п	Наименование раздела учебной дисциплины (модуля)	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	2	3
1	Все разделы дисциплины, для которых проводятся лабораторные работы	1. Программа DreamSpark, договор №Tr000043844 от 22.09.2015, срок действия до 21.09.2018 2. Kaspersky Endpoint Security, договор №14/032018-0142 от 30 марта 2018 г. длительностью 1 год, на 750 ПК. 3. Microsoft Office Professional Plus 2010, согласно Microsoft Open License 60049804 (от 05/03/2012, авторизационный номер лицензиата 90038163ZZE1403), бессрочно
2	Все разделы дисциплины, для которых проводится лекционный курс	1. Программа DreamSpark, договор №Tr000043844 от 22.09.2015, срок действия до 21.09.2018 2. Kaspersky Endpoint Security, договор №14/032018-0142 от 30 марта 2018 г. длительностью 1 год, на 750 ПК 3. Windows Vista, согласно Microsoft Open License* № 60049804 (от 05/03/2012, авторизационный номер лицензиата 90038163ZZE1403), срок действия бессрочно 4. Microsoft Office Professional Plus 2010, согласно Microsoft Open License* № 45472941 (от 18/05/2009, авторизационный номер лицензиата 65463391ZZE1105), срок действия бессрочно
3	Все разделы дисциплины, для которых проводится самостоятельная работа студента	1. Программа DreamSpark, договор №Tr000043844 от 22.09.2015, срок действия до 21.09.2018 2. Kaspersky Endpoint Security, договор №14/032018-0142 от 30 марта 2018 г. длительностью 1 год, на 750 ПК 3. Windows Vista, согласно Microsoft Open License* № 60049804 (от 05/03/2012, авторизационный номер лицензиата 90038163ZZE1403), срок действия бессрочно 4. Microsoft Office Professional Plus 2010, согласно Microsoft Open License* № 45472941 (от 18/05/2009, авторизационный номер лицензиата 65463391ZZE1105), срок действия бессрочно

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Паспорт фонда оценочных средств по дисциплине
для промежуточного контроля успеваемости

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции) или её части)	Наименование оценочного средства
1	**Основные составляющие информационной безопасности**	ОПК 2 ПК-2	Зачет
2	**Криптографические способы защиты информации**		
3	**Антивирусная защита**		
4	**Сетевая безопасность**		
5	**Элементы теории информации**		
6	**Алгоритмы сжатия без потерь**		
7	**Алгоритмы сжатия данных с потерями**		
8	**Современные стандарты сжатия данных**		

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОБУЧЕНИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Индекс компетенции	Содержание компетенции	Элементы компетенции	Индекс элемента
1	2	3	4
ОПК-2	способность применять в профессиональной деятельности знания математических основ информатики;	знать	
		З1 математические принципы сжатия данных;	ОПК-2 З1
		З2 математические принципы, лежащие в основе криптографических моделей	ОПК-2 З2
		З3 математические модели сжатия видео и аудио-информации,	ОПК-2 З3
		Уметь	
		У1 уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов сжатия.	ОПК-2 У1
		У2 уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования	ОПК-2 У2
		Владеть	
		В1 владеть алгоритмическими языками для разработки прикладных алгоритмов сжатия данных	ОПК-2 В1
		В2 владеть навыками решения задач криптоанализа и шифрования	ОПК-2 В2
ПК-2	готовность к использованию основных моделей информационных технологий и способов их применения для решения задач в предметных областях;	Знать	
		З1 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 их средства описания;	ПК-2 З1
		З2 современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики;	ПК-2 З2
		З3 теоретические основы определения количество информации, современные методы сжатия данных, особенности сжатия различных видов информации, современные стандарты сжатия данных, области их применения.	ПК-2 З3
		Уметь	
		У1 уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач; уметь использовать математические модели для построения криптологических систем;	ПК-2 У1
		У2 уметь применять современные технологии создания брандмауэров и IDS-комплексов;	ПК-2 У2
		У3 пользоваться современным инструментарием сжатия данных; разрабатывать алгоритмы сжатия данных, основанные на стандартных методах	ПК-2 У3
		Владеть	

		В1 основными методами, способами и средствами шифрования и криптографиии; навыками проектирования, отладки и тестирования программ в средах, по крайней мере, трех императивных систем программирования	ПК-2 В1
		В2 навыками работы с архиваторами различного типа; Навыками создания архиваторов на основе стандартных алгоритмов сжатия	ПК-2 В2
		В3 Приемами обнаружения вирусных угроз	ПК-2 В3
		В4 Приемами обнаружения сетевых проникновений; Навыками работы по обнаружению и защите от DDOS-атак	ПК-2 В4

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЗАЧЕТ)

Содержание оценочного средства	Индекс оцениваемой компетенции и ее элементов
1. Базовые понятия теории информации.	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ПК-2 З3 ПК-2 В2
2. Измерение дискретной информации. Энтропия Шеннона.	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ПК-2 З3 ПК-2 В2
3. Алгоритм Хаффмана.	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ОПК-2 В1 ПК-2 З3
4. Алгоритм арифметического кодирования.	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ОПК-2 В1 ПК-2 З3
5. Алгоритм адаптивного арифметического кодирования	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ОПК-2 В1 ПК-2 З3
6. Словарные методы сжатия данных. Алгоритм LZ77	ОПК-2 З1 ОПК-2 У1 ОПК-2 В1 ПК-2 З3
7. Словарные методы сжатия данных. Алгоритм LZSS	ОПК-2 З1 ОПК-2 У1 ОПК-2 В1 ПК-2 З3
8. Методы Лемпеля-Зива. Алгоритм LZW.	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ОПК-2 В1 ПК-2 З3
9. Преобразование Барроуза-Уилера (BWT)	ОПК-2 З1 ОПК-2 У1 ОПК-2 В1 ПК-2 З3
10. Алгоритмы сжатия изображений. Классы изображений. Требования к алгоритмам компрессии. Критерии сравнения алгоритмов.	ОПК-2 З1 ОПК-2 У1 ОПК-2 В1 ПК-2 З3 ПК-2 В2
11. Архивация изображений и сообщений без потерь. Общие понятия. Приведите требования к алгоритмам компрессии с потерями.	ОПК-2 З1 ОПК-2 З3ОПК-2 У1 ОПК-2 В1 ПК-2 У3 ПК-2 В2
12. RLE –алгоритм и примеры его использования	ОПК-2 З1 ОПК-2 У1 ОПК-2 В1 ПК-2 У3 ПК-2 В2
13. Алгоритмы сжатия изображений с потерями. Алгоритм JPEG.	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ОПК-2 В1 ПК-2 У3 ПК-2 В2
14. Wavelet-алгоритм (рекурсивный или волновой алгоритм).	ОПК-2 З1 ОПК-2 У1 ОПК-2 В1 ПК-2 У3 ПК-2 В2
15. Фрактальный алгоритм	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ОПК-2 В1
16. Контекстное моделирование	ОПК-2 З1 ОПК-2 З3 ОПК-2 У1 ПК-2 З3 ПК-2 У3
17. Базовые технологии сжатия видео.	ОПК-2 З1 ОПК-2 У1 ПК-2 З3 ПК-2 У3 ПК-2 В2
18. Основные понятия информационной безопасности. Классификация угроз. Целостность и конфиденциальность. Классификация средств защиты информации.	ОПК-2 З2 ПК-2 З2 ПК-2 В1 ПК-2 В2
19. Методы и средства организационно-правовой защиты информации. Методы и средства	ОПК-2 З2 ПК-2 З2 ПК-2 У1 ПК-2 В1 ПК-2 В2

инженерно-технической защиты. Криптографические методы защиты и шифрование.	
20. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.	ОПК-2 З2 ПК-2 З2 ПК-2 В1
21. Модель сетевой безопасности. Классификация сетевых атак.	ОПК-2 З2 ПК-2 З2 ПК-2 В1
22. Сервисы и механизмы безопасности	ОПК-2 З2 ПК-2 В1
23. Модель сетевого взаимодействия, модель безопасности информационной системы	ОПК-2 З2 ПК-2 В1
24. Простые криптосистемы. Шифрование методом замены (подстановки): Одноалфавитная подстановка; Многоалфавитная одноконтурная обыкновенная подстановка(Таблицы Вижинера)**.**	ОПК-2 З2 ОПК-2 У2 ОПК-2 В2 ПК-2 З1 ПК-2 У1
25. Шифрование многоалфавитной одноконтурной монофонической подстановкой. Многоалфавитная многоконтурная подстановка.	ОПК-2 З2 ОПК-2 У2 ОПК-2 В2 ПК-2 З1 ПК-2 У1
26. Шифрование методом перестановки: Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам	ОПК-2 З2 ОПК-2 У2 ОПК-2 В2 ПК-2 З1 ПК-2 У1
27. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.	ОПК-2 З2 ОПК-2 У2 ОПК-2 В2 ПК-2 З1 ПК-2 У1 ПК-2 В1 ПК-2 В1
28. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Алгоритм шифрования данных IDEA.	ОПК-2 З2 ОПК-2 У2 ОПК-2 В2 ПК-2 З1 ПК-2 У1 ПК-2 В1
29. Общие понятия антивирусной защиты. Уязвимости. Последствия заражений компьютерными вирусами.	ПК-2 З2 ПК-2 В3 ПК-2 В4
30. Классификация вредоносных программ.	ПК-2 З2 ПК-2 В3
31. Признаки присутствия на компьютере вредоносных программ. Явные и косвенные проявления.	ПК-2 З2 ПК-2 В3 ПК-2 В4
32. Признаки присутствия на компьютере вредоносных программ. Скрытые проявления.	ПК-2 З2 ПК-2 В3
33. Методы защиты от вредоносных программ.	ПК-2 З2 ПК-2 В3
34. Основы работы антивирусных программ: Сигнатурный анализ. Приведите примеры использования	ПК-2 З2 ПК-2 В3
35. Эвристический анализ при работе антивирусных программ	ПК-2 З2 ПК-2 В3
36. Основные модули антивирусной системы.	ПК-2 З2 ПК-2 В3
37. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы.	ПК-2 З2 ПК-2 В3
38. Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты сети.	ПК-2 З2 ПК-2 У2 ПК-2 В4
39. Принципы организации централизованного управления антивирусной защитой. Компоненты системы удаленного управления.	ПК-2 З2 ПК-2 У2 ПК-2 В4
40. Брандмауэры. Определение типов брандмауэров.	ПК-2 З2 ПК-2 У2 ПК-2 В4

41. Конфигурация межсетевого экрана. Построение набора правил межсетевого экрана для различных типов архитектуры	ПК-2 З2 ПК-2 У2 ПК-2 В4
42. Виртуальные частные сети.	ПК-2 З2 ПК-2 У2 ПК-2 В4

ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

(Шкалы оценивания)

Результаты выполнения обучающимся заданий на зачете оцениваются по шкале «зачтено» - «не зачтено»

В основе оценивания лежат критерии порогового и повышенного уровня характеристик компетенций или их составляющих частей, формируемых на учебных занятиях по дисциплине «Методы сжатия данных и защиты информации» (Таблица 2.5 рабочей программы дисциплины).

«Зачтено» – оценка соответствует повышенному и пороговому уровню и выставляется обучающемуся, если он

1) глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
2) твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос или выполнении заданий, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
3) оценка соответствует пороговому уровню и выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, демонстрирует недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

«Не зачтено» - оценка выставляется обучающемуся, который не достигает порогового уровня, демонстрирует непонимание проблемы, не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.