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

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень основной профессиональной образовательной программы:
бакалавриат

Направление подготовки: **38.03.05 Бизнес-информатика**

Направленность (профиль) подготовки: **Цифровая экономика**

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 учебной дисциплины «Информационная безопасность» является формирование у обучающихся общекультурных и профессиональных компетенций в процессе изучения различных аспектов защиты информации для последующего применения в учебной и практической деятельности.

Задачи дисциплины:

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

2.1. Дисциплина **Б1.В.15 «Информационная безопасность»** относится к вариативной части блока Б1.

2.2. Для изучения дисциплины необходимы следующие знания, умения, навыки, формируемые предшествующими дисциплинами:

- *Математический анализ;*
- *Теория вероятностей и математическая статистика;*
- *Программирование*

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

- *Цифровые ресурсы предприятия;*
- *Администрирование цифровой инфраструктуры предприятия.*
- *Государственная итоговая 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 обучающихся следующих общепрофессиональных (ОПК) и профессиональных (ПК) компетенций:

№ п/п	Номер/ индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны:		
			Знать:	Уметь:	Владеть (навыками):
1	ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	математические принципы, лежащие в основе криптографических моделей; теорию простых чисел и модульной арифметики	уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач	владеть алгоритмическими языками для разработки прикладных алгоритмов шифрования; владеть навыками решения задач криптоанализа и шифрования; Приемами обнаружения сетевых проникновений
2	ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	Основные принципы административно-правовой защиты информации	Быстро реагировать на различные угрозы информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов	Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; Навыками работы по обнаружению и защите от DDOS-атак

2.5. Карта компетенций дисциплины

КАРТА КОМПЕТЕНЦИЙ ДИСЦИПЛИНЫ					
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ: Информационная безопасность					
Цель дисциплины	формирование у обучающихся общепрофессиональных и профессиональных компетенций в процессе изучения бизнес-информатики и цифровой экономики для последующего применения в учебной и практической деятельности				
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие					
Общепрофессиональные компетенции					
ИНДЕКС	**ФОРМУЛИРОВКА**	**Перечень компонентов**	**Технологии формирования**	**Форма оценочного средства**	**Уровни освоения компетенций**
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать** математические принципы, лежащие в основе криптографических моделей; теорию простых чисел и модульной арифметики ; **уметь** использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач; **владеть** алгоритмическими языками для разработки прикладных алгоритмов шифрования; владеть навыками решения задач криптоанализа и шифрования; Приемами обнаружения сетевых проникновений;	Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий, организации самостоятельной работы студентов	Лабораторные работы, зачет	**Пороговый** Способен решать стандартные задачи информационной безопасности **Повышенный** Способен решать задачи криптографии повышенной сложности
Профессиональные компетенции					
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры пред-	**Знать** основные принципы административно-правовой защиты информации **Уметь** быстро реагировать на различные угрозы информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов; **Владеть навыками п**рименения, установ-	Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий, ор-	Лабораторные работы, зачет	**Пороговый** Способен решать стандартные задачи **Повышенный** Способен быстро решать задачи определения взлома

	приятия	ки и настройки антивирусных систем и систем распознавания угроз и атак; Навыками работы по обнаружению и защите от DDOS-атак	ганизации самостоятельной работы студентов		и атак злоумышленников повышенной сложности

ОСНОВНАЯ ЧАСТЬ

1. ОБЪЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы		**Всего часов**	**Семестры**
			№ 5
			часов
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)		**34**	**34**
В том числе:			
Лекции (Л)		16	16
Лабораторные работы (ЛР)		18	18
Самостоятельная работа студента (всего)		**38**	**38**
В том числе:			
Изучение литературы и других источников		18	18
Подготовка к выполнению лабораторных работ		10	10
Подготовка к защите лабораторных работ		10	10
Вид промежуточно аттестации	**зачет**		+
ИТОГО: общая трудоемкость	**часов**	**72**	**72**
	зач. ед.	**2**	**2**

2. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Содержание разделов учебной дисциплины

№ семестра	№ раздела	Наименование раздела учебной дисциплины	Содержание раздела в дидактических единицах
5	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. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности
	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. Перестанов-

			ка, 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
5	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
	4	**Сетевая безопасность**	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS

2.2. 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	
5	1	**Основные составляющие информационной безопасности**	2	2	5	9	*1 неделя:* Защита лабораторной работы №1
	2	**Криптографические способы защиты информации**	6	8	11	25	*2,3 неделя:* Защита лабораторной работы №2 4,5 неделя Защита лабораторной работы №3
	3	**Антивирусная защита**	4	2	11	17	*6 неделя:* Защита лабораторной работы №4
	4	**Сетевая безопасность**	4	6	11	21	*7,8 неделя:* Защита лабораторной работы №5 *9 неделя* Защита лабораторной работы №6
		ИТОГО	**16**	**18**	**38**	**72**	

2.3. Лабораторный практикум

№ семестра	№ раздела	Наименование раздела учебной дисциплины	Наименование лабораторных работ	Всего часов
5	1	**Основные составляющие информационной безопасности**	ЛР №1. Составление плана и основных положений политики безопасности для учреждения	2
	2	**Криптографические способы защиты информации**	ЛР №2. *Написание, ввод, отладка и тестирование программ шифрования подстановкой и перестановкой*	4
			ЛР №3. *Написание, ввод, отладка и тестирование программ шифрования RSA, аналитически и гаммированием*	4
	3	**Антивирусная защита**	ЛР №4. *Диагностика антивирусной программы и создание тестовых вирусов*	2
	4	**Сетевая безопасность**	ЛР №5 *Создание цифровой подписи*	4
			ЛР №6 *Парольный доступ и парольная аутентификация*	2
		ИТОГО 5 семестр		**18**

2.4. Курсовые работы *не предусмотрены*

3. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТА

3.1. Виды СРС

№ семестра	№ раздела	Наименование раздела учебной дисциплины	Виды СРС	Всего часов
5	1	**Основные составляющие информационной безопасности**	Изучение литературы и других источников	3
			Подготовка к выполнению ЛР №1	1
			Подготовка к защите лабораторной работы (ЛР №1)	1
	2	**Криптографические способы защиты информации**	Изучение литературы и других источников	5
			Подготовка к выполнению лабораторной работы №2 по теме "Шифрование подстановкой"	1,5
			Подготовка к защите лабораторной работы (ЛР №2)	1,5
			Подготовка к выполнению лабораторной работы №3 по теме "Шифрование перестановкой, аналитически и гаммированием"	1,5
			Подготовка к защите лабораторной работы (ЛР №3)	1,5
	3	**Антивирусная защита**	Изучение литературы и других источников	5
			Подготовка к выполнению лабораторной работы №4 по теме "Диагностика работы антивируса и создание тестового вируса"	3
			Подготовка к защите лабораторной работы №4	3
	4	**Сетевая безопасность**	Изучение литературы и других источников	5
			Подготовка к выполнению лабораторной работы №5 по теме "Создание цифровой подписи"	1,5
			Подготовка к защите лабораторной работы (ЛР №5)	1,5
			Подготовка к выполнению лабораторной работы №6 по теме «Парольный доступ и парольная аутентификация»	1,5
			Подготовка к защите лабораторной работы №6	1,5
		ИТОГО		**38**

3.2. График работы студента
Семестр №5

Форма оценочного средства	Усл. Обозн.	НЕДЕЛЯ																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Защита лабораторной работы	ЛР	+	+	+	+		+			+	+		+		+	+		+

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

1. Лапонина О.Р. Криптографические основы безопасности – [Электронный ресурс] – URL: http://www.intuit.ru/
2. Фороузан Б.А. Математика криптографии и теория шифрования. Пер. А.Н. Берлин. – [Электронный ресурс] – URL http://www.intuit.ru/
3. Конеев И.Р. Информационная безопасность предприятия. [Текст]./ И.Р.Конеев, А.В.Беляев. - СПб.: БХВ-Петербург, 2003/
4. Учебники, учебные пособия, ресурсы сети Интернет (см. раздел 5).

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

№	Автор (ы), наименование, место издания и издательство, год	Используется при изучении разделов	семестр	Количество экземпляров	
				В библиотеке	На кафедре
1	Конеев, И. Информационная безопасность предприятия [Текст] / И.Конеев, А.Беляев. – СПб. : БХВ-Петербург, 2003. – 752с.	1-4	5	10	
2	Штарьков, Ю. М. Универсальное кодирование: Теория и алгоритмы [Электронный ресурс] / Ю. М. Штарьков. – М. : Физматлит, 2013. – 280 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=275569 (дата обращения 30.08.2019).	1-4	5	ЭБС	

5.2. Дополнительная литература

№	Автор (ы), наименование, место издания и издательство, год	Используется при изучении разделов	семестр	Количество экземпляров	
				В библиотеке	На кафедре
1	Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://www.biblio-online.ru/bcode/434171 (дата обращения 30.08.2019)	1-4	5	ЭБС	
2	Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю.Н. Загинайлов. – М. ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения 30.08.2019)	1-4	5	ЭБС	
3	Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения 30.08.2019)	1-4	5	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: 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. Ватолин, Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео [Электронный ресурс] / Д. Ватолин [и др.]. – М.: ДИАЛОГ-МИФИ, 2002. – 384 с. – Режим доступа: http://www.compression.ru/book, свободный (дата обращения: 30.08.2019).

2. Сэломон, Д. Сжатие данных, изображения и звука [Электронный ресурс] / Д. Сэломон. – М.: Техносфера, 2004. – 367 с. – Режим доступа: http://da.kalinin.ru/books/salmon.pdf, свободный (дата обращения: 30.08.2019).

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://elibrary.ru/defaultx.asp, свободный (дата обращения: 30.08.2019).

4. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] : федеральный портал. – Режим доступа: http://school-collection.edu.ru/, свободный (дата обращения: 30.08.2019).

5. Единое окно доступа к образовательным ресурсам [Электронный ресурс] : федеральный портал. – Режим доступа: http://window.edu.ru/, свободный (дата обращения: 30.08.2019).

6. Интернет Университет Информационных технологий. [Электронный ресурс] : сайт. – Режим доступа: http://www.intuit.ru/, свободный (дата обращения 30.08.2019).

7. Портал естественных наук. [Электронный ресурс] : сайт. – Режим доступа: http://e-science11.ru, свободный (дата обращения 30.08.2019).

8. Российский общеобразовательный портал [Электронный ресурс] : образовательный портал. – Режим доступа: http://www.school.edu.ru/, свободный (дата обращения: 30.08.2019).

9. Сервер Информационных Технологий [Электронный ресурс] : сайт. – Режим доступа: http://citforum.ru/, 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 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*:* *Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Цифровая подпись. Установление подлинности объекта. Управление ключами. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. угрозы, атаки, целостность, аутентификация, 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 алгоритмов криптографии и

	изучения антивирусной защиты, на изучение которых и нацелены. В лекционной части курса описание работы в антивирусных системах не предусмотрено, поэтому рекомендуется преподавателям давать задание на самостоятельный поиск и изучение сетевого антивирусного ПО. Наилучшим вариантом может служить предоставление лабораторных работ в виде 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 экзамену	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

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

1. Операционная система Windows Pro (договор №Tr000043844 от 22.09.15г)
2. Антивирус Kaspersky Endpoint Security (договор №02-ЗК-2019 от 15.04.2019г.)
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. 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)

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 -1 ПК-9	зачет
2	**Криптографические способы защиты информации**		
3	**Антивирусная защита**		
4	**Сетевая безопасность**		

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОБУЧЕНИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Индекс компетенции	Содержание компетенции	Элементы компетенции	Индекс элемента
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знать	
		З1 математические принципы, лежащие в основе криптографических моделей;	ОПК-1 З1
		Уметь	
		У1 использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач;	ОПК-1 У1
		Владеть	
		В1 алгоритмическими языками для разработки прикладных алгоритмов шифрования;	ОПК-1 В1
		В2 владеть навыками решения задач криптоанализа и шифрования;	ОПК-1 В2
		В3 Приемами обнаружения сетевых проникновений;	ОПК-1 В3
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения за-	знать	
		З1 основные принципы административно-правовой защиты информации	ПК-9 З1
		Уметь	
		У1 быстро реагировать на различные угрозы информационной безопасности	ПК-9 У1

	дач управления информационной безопасностью ИТ-инфраструктуры предприятия	У2 применять современные технологии создания брандмауэров и IDS-комплексов;	ПК-9 У2
		Владеть	
		В1 навыками применения, установки и настройки антивирусных систем и систем распознавания угроз и атак;	ПК-9 В1
		В2 Навыками работы по обнаружению и защите от DDOS-атак	ПК-9 В2

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЗАЧЕТ)

№ п/п	Содержание оценочного средства	Индекс оцениваемой компетенции и ее элементов
1.	Основные понятия информационной безопасности. Классификация угроз.	ОПК-1 В3 ПК-9 З1 ПК-9 У1 ПК-9 В2
2.	Целостность и конфиденциальность. Классификация средств защиты информации.	ОПК-1 В3 ПК-9 З1 ПК-9 У1 ПК-9 В2
3.	Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.	ОПК-1 В1 ОПК-1 В3 ПК-9 У1 ПК-9 В2
4.	Базовые понятия теории информации.	ОПК-1 У1
5.	Измерение дискретной информации. Энтропия Шеннона.	ОПК-1 У1
6.	Методы и средства организационно-правовой защиты информации.	ОПК-1 В3 ПК-9 З1 ПК-9 У1
7.	Методы и средства инженерно-технической защиты.	ПК-9 З1 ПК-9 У1
8.	Формулы мультипликативных шифров. Аффинные шифры. Криптоанализ аффинного шифра.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В2
9.	Модель сетевой безопасности. Классификация сетевых атак.	ПК-9 З1 ПК-9 У1 ПК-9 В1 ПК-9 В2
10.	Сервисы и механизмы безопасности	ПК-9 З1 ПК-9 У1 ПК-9 В1
11.	Модель сетевого взаимодействия, модель безопасности информационной системы	ОПК-1 В3 ПК-9 З1 ПК-9 В1
12.	Простые криптосистемы. Шифрование методом замены (подстановки): Одноалфавитная подстановка;	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1
13.	Простые криптосистемы. Шифрование методом замены (подстановки): Многоалфавитная одноконтурная обыкновенная подстановка(Таблицы Вижинера).	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1
14.	Простые криптосистемы. Шифрование методом замены (подстановки): Шифрование многоалфавитной одноконтурной монофонической подстановкой.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1
15.	Простые криптосистемы. Шифрование методом замены (подстановки): Многоалфавитная многоконтурная подстановка.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1
16.	Арифметика целых чисел. НОД и алгоритм Евклида Бинарные операции.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В2
17.	Расширенный алгоритм Евклида . Линейные диофантовы уравнения.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В2

18.	Модульная арифметика. Операции по модулю. Система вычетов. Сравнения. Инверсии.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В2
19.	Шифрование методом перестановки: Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1
20.	Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1
21.	Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Алгоритм шифрования данных IDEA.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1 ПК-9 У2
22.	Стандарт шифрования данных RSA	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1
23.	Основы работы антивирусных программ: Сигнатурный анализ. Приведите примеры использования	ПК-9 У1 ПК-9 В1
24.	Эвристический анализ при работе антивирусных программ	ПК-9 У1 ПК-9 В1
25.	Основные приемы криптоанализа при симметричных ключах. Виды атак. Принцип Керкгоффса.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1 ОПК-1 В2
26.	Формулы аддитивных шифров. Криптоанализ.	ОПК-1 З1 ОПК-1 У1 ОПК-1 В1 ОПК-1 В2
27.	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты сети.	ОПК-1 В3 ПК-9 З1 ПК-9 У1 ПК-9 В1
28.	Принципы организации централизованного управления антивирусной защитой. Компоненты системы удаленного управления.	ОПК-1 В3 ПК-9 З1 ПК-9 У1 ПК-9 В1
29.	Брандмауэры. Определение типов брандмауэров.	ПК-9 У2 ПК-9 В2
30.	Конфигурация межсетевого экрана. Построение набора правил межсетевого экрана для различных типов архитектуры	ПК-9 У2 ПК-9 В2
31.	Одноразовый блокнот и роторные шифры. Устройство и принцип работы шифровальной машины «Энигма»	ОПК-1 З1
32.	Основные приемы криптоанализа при асимметричных ключах	ОПК-1 З1 ОПК-1 У1 ОПК-1 В2
33.	Базовые методы и алгоритмы стеганографии	ОПК-1 З1 ОПК-1 У1

ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ
(Шкалы оценивания)

Результаты выполнения обучающимся заданий на зачете оцениваются зачет – незачет.

В основе оценивания лежат критерии порогового и повышенного уровня характеристик компетенций или их составляющих частей, формируемых на учебных занятиях по дисциплине «Информационная безопасность» (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.