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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень основной профессиональной образовательной программы:
бакалавриат

Направление подготовки: **01.03.01 Математика**

Направленность (профиль) подготовки: **Математическое моделирование в цифровой экономике**

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

2.1. Дисциплина **Б1.В.01.07 «Информационная безопасность»** относится к обязательной части блока Б1.

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

- *Цифровая инфраструктура предприятия;*
- *Теория вероятностей и математическая статистика;*
- *Математический анализ*
- *Компьютерные технологии в математике*

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

- *Программные средства цифровой экономики;*
- *Государственная итоговая аттестация.*
- *Практики*

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 универсальных (УК), общепрофессиональных (ОПК) и профессиональных (ПК) компетенций:

№ п/п	Код и содержание компетенции	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения по дисциплине В результате изучения дисциплины обучающиеся должны:		
			Знать:	Уметь:	Владеть (навыками):
1	2	3	4	5	6
1	**УК-8.** Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	УК -8.1. Идентифицирует и анализирует вредные и опасные факторы среды обитания; оценивает факторы риска её элементов (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений).	Алгоритмы создания политики безопасности предприятия Механизмы защиты предприятия от угроз информационного проникновения и атак	уметь выбирать, адаптировать и применять необходимые алгоритмы и программное обеспечение при решении профессиональных задач Быстро реагировать на различные угрозы информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов	Приемами обнаружения сетевых проникновений Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; Навыками работы по созданию протоколов безопасности предприятия
		УК -8.2. Оценивает степень потенциальной опасности; выявляет проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает мероприятия по предотвращению чрезвычайных ситуаций; создает условия безопасной и комфортной среды и умеет обеспечивать личную безопасность и безопасность окружающих.	современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики; основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики; математические криптологические модели, включая средства описания	уметь применять современные технологии создания брандмауэров и IDS-комплексов; Основные принципы административно-правовой защиты информации	Приемами обнаружения вирусных угроз Приемами обнаружения нарушений протокола сетевой безопасности Навыками работы по администрированию и настройке производственных программных систем и локальных сетей с точки зрения информационной безопасности

2	**ОПК-4.** Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-4.2. Анализирует и обобщает результаты научно-исследовательских работ с учетом основных требований информационной безопасности	Алгоритмы создания политики безопасности предприятия Механизмы защиты предприятия от угроз информационного проникновения и атак	уметь выбирать, адаптировать и применять необходимые алгоритмы и программное обеспечение при решении профессиональных задач Быстро реагировать на различные угрозы информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов	Приемами обнаружения сетевых проникновений Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; Навыками работы по созданию протоколов безопасности предприятия
		ОПК-4.3. Применяет навыки информационно-коммуникационных технологий для создания и обработки информации с учетом основных требований информационной безопасности	современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики; основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики; математические криптологические модели, включая средства описания; современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики;	уметь применять современные технологии создания брандмауэров и IDS-комплексов; Основные принципы административно-правовой защиты информации	Приемами обнаружения вирусных угроз Приемами обнаружения нарушений протокола сетевой безопасности Навыками работы по администрированию и настройке производственных программных систем и локальных сетей с точки зрения информационной безопасности
3	**ПК-2.** Способен к анализу и моделированию бизнес-процессов в сфере цифровой экономики	ПК-2.3. Умеет осваивать аналитические платформы и специализированные пакеты прикладных программ	математические принципы, лежащие в основе криптографических моделей этапы решения задач сетевой безопасности на компьютере; терминологию из области криптологии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений;	пользоваться современным программным обеспечением для решения задач информационной безопасности. Настраивать сетевое программное обеспечение по протоколу политики информационной безопасности предприятия	владеть навыками решения задач криптоанализа и шифрования для поддержания протоколов информационной безопасности Навыками защиты информации с помощью криптосистем Навыками применения дублирующих брандмауэров и протоколов сетевой безопасности

ОСНОВНАЯ ЧАСТЬ

1. ОБЪЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы		**Всего часов**	**Семестры**
			№ 6
			часов
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)		**32**	**32**
В том числе:			
Лекции (Л)		16	16
Лабораторные работы (ЛР)		16	16
Самостоятельная работа студента (всего)		**40**	**40**
В том числе:			
Изучение литературы и других источников		16	16
Подготовка к выполнению лабораторных работ		12	12
Подготовка к защите лабораторных работ		12	12
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
6	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. Перестановка, усложненная по маршрутам. Шифрование методом гамми-

			рования. 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
6	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. Лабораторный практикум

№ семестра	№ раздела	Наименование раздела учебной дисциплины	Наименование лабораторных работ	Всего часов
6	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*	2
			ЛР №6 *Парольный доступ и парольная аутентификация*	2

		ИТОГО 6 семестр		**16**

Курсовые работы не предусмотрены по учебному плану

3. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТА

Самостоятельная работа осуществляется в объеме 40 часов.
Видами СРС являются:

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

Формами текущего контроля успеваемости являются:

- Защита лабораторных работ

4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (*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
1	Конеев, И. Информационная безопасность предприятия [Текст] / И.Конеев, А.Беляев. – СПб. : БХВ-Петербург, 2003. – 752с.
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 30.05.2020).

5.2. Дополнительная литература

№	Автор (ы), наименование, место издания и издательство, год
1	Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2020. — 321 с. — Режим доступа: https://www.biblio-online.ru/bcode/434171 (дата обращения 30.05.2020)
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 30.05.2020)
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 30.05.2020)

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: 30.05.2020).

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: 30.05.2020).

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: 30.05.2020).

4. Znanium.com [Электронный ресурс] : [база данных]. – Доступ к полным текстам по паролю. – Режим доступа: http://znanium.com (дата обращения: 30.05.2020).

5. «Издательство «Лань» [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://e-lanbook.com (дата обращения: 30.05.2020).

6. Университетская библиотека ONLINE [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://www.biblioclab.ru (дата обращения: 30.05.2020).

7. Юрайт [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://www.biblio-online.ru (дата обращения: 30.05.2020).

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: 30.05.2020).

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: 30.05.2020).

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: 30.05.2020).

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://elibrary.ru/defaultx.asp, свободный (дата обращения: 30.05.2020).

4. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] : федеральный портал. – Режим доступа: http://school-collection.edu.ru/, свободный (дата обращения: 30.05.2020).

5. Единое окно доступа к образовательным ресурсам [Электронный ресурс] : федеральный портал. – Режим доступа: http://window.edu.ru/, свободный (дата обращения: 30.05.2020).

6. Интернет Университет Информационных технологий. [Электронный ре-

сурс] : сайт. – Режим доступа: http://www.intuit.ru/, свободный (дата обращения 30.05.2020).

7. Портал естественных наук. [Электронный ресурс] : сайт. – Режим доступа: http://e-science11.ru, свободный (дата обращения 30.05.2020).

8. Российский общеобразовательный портал [Электронный ресурс] : образовательный портал. – Режим доступа: http://www.school.edu.ru/, свободный (дата обращения: 30.05.2020).

9. Сервер Информационных Технологий [Электронный ресурс] : сайт. – Режим доступа: http://citforum.ru/, свободный (дата обращения 30.05.2020).

5.5. Периодические издания

1. Компьютерные и информационные науки. Доступ: Киберленинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: https://cyberleninka.ru/article/c/computer-and-information-sciences, свободный (дата обращения: 30.08.2020).
2. Электротехника, электронная техника, информационные технологии. Доступ: Киберленинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: https://cyberleninka.ru/article/c/electrical-electronic-information-engineering, свободный (дата обращения: 30.08.2020).
3. Архив научных статей из журнала «Информационная безопасность» [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/articles, свободный (дата обращения: 30.08.2020).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Требования к аудиториям для проведения занятий:

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

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

6.2. Требования к оборудованию рабочих мест преподавателя и обучающихся:

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

6.3. Требования к специализированному оборудованию: *отсутствует*

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебных занятий	Организация деятельности студента
Лекция	Освоение дисциплины идет с помощью объектно-ориентированных сред языков программирования. Учитывая, что курс выстроен по разделам, большинство из которых охватывает теоретические вопросы, преподавателю необходимо соблюсти баланс между ко-

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

8. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ УЧЕБНОГО ПРОЦЕССА

Название ПО	№ лицензии
Операционная система Windows Pro	договор №Tr000043844 от 22.09.15г.
Антивирус Kaspersky Endpoint Security	договор №14/03/2020-0142 от 30/03/2020г.
Офисное приложение LibreOffice	свободно распространяемое ПО
Архиватор 7-zip	свободно распространяемое ПО
Браузер изображений Fast-StoneImageViewer	свободно распространяемое ПО
PDF ридер FoxitReader	свободно распространяемое ПО
PDF принтер doPdf	свободно распространяемое ПО
Медиа проигрыватель VLC media play-er	свободно распространяемое ПО
Запись дисков ImageBurn	свободно распространяемое ПО
DJVU браузер DjVu Browser Plug-in	свободно распространяемое ПО

Набор ПО для кафедральных ноутбуков	
Антивирус Kaspersky Endpoint Security	договор №14/03/2018-0142 от 30/03/2018г
Офисное приложение LibreOffice	свободно распространяемое ПО
Архиватор 7-zip	свободно распространяемое ПО
Браузер изображений FastStoneImageViewer	свободно распространяемое ПО
PDF ридер FoxitReader	свободно распространяемое ПО
Медиа проигрыватель VLC media player	свободно распространяемое ПО
Запись дисков ImageBurn	свободно распространяемое ПО
DJVU браузер DjVu Browser Plug-in	свободно распространяемое ПО

При реализации дисциплины с применением (частичным применением) дистанционных образовательных технологий используются:

- вебинарная платформа Zoom (договор б/н от 10.10.2020г.);
- набор веб-сервисов MS office365 (бесплатное ПО для учебных заведений https://www.microsoft.com/ru-ru/education/products/office);
- система электронного обучения Moodle (свободно распространяемое ПО).

9. ИНЫЕ СВЕДЕНИЯ

Не предусмотрены

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

«Информационная безопасность»

Направление подготовки
01.03.01 Математика

Направленность (профиль)
Математическое моделирование в цифровой экономике

Квалификация
бакалавр

Форма обучения
очная

Рязань 2020

1. Цель освоения дисциплины:

формирование у обучающихся компетенций в процессе изучения различных аспектов защиты информации для последующего применения в учебной и практической деятельности.

2. Место дисциплины в структуре ОПОП

Дисциплина относится к обязательной части Блока 1.

Дисциплина изучается на 3 курсе (6 семестр)

3. Трудоемкость дисциплины: 2 зачетные единицы, 72 академических часа

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

Код индикатора достижения компетенции	**Перечень планируемых результатов обучения по дисциплине** В результате изучения дисциплины обучающиеся должны:		
	Знать:	Уметь:	Владеть (навыками):
УК -8.1.	Алгоритмы создания политики безопасности предприятия Механизмы защиты предприятия от угроз информационного проникновения и атак	уметь выбирать, адаптировать и применять необходимые алгоритмы и программное обеспечение при решении профессиональных задач Быстро реагировать на различные угрозы информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов	Приемами обнаружения сетевых проникновений Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; Навыками работы по созданию протоколов безопасности предприятия
УК -8.2.	современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики; основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики; математические криптологические модели, включая средства описания; современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики;	уметь применять современные технологии создания брандмауэров и IDS-комплексов; Основные принципы административно-правовой защиты информации	Приемами обнаружения вирусных угроз Приемами обнаружения нарушений протокола сетевой безопасности Навыками работы по администрированию и настройке производственных программных систем и локальных сетей с точки зрения информационной безопасности
ОПК-4.2.	Алгоритмы создания политики безопасности предприятия Механизмы защиты предприятия от угроз информационного проникновения и атак	уметь выбирать, адаптировать и применять необходимые алгоритмы и программное обеспечение при решении профессиональных задач Быстро реагировать на различные угрозы информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов	Приемами обнаружения сетевых проникновений Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; Навыками работы по созданию протоколов безопасности предприятия

ОПК-4.3.	современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики; основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики; математические криптологические модели, включая средства описания; современные системы сетевой безопасности; антивирусные системы, их особенности и основные характеристики;	уметь применять современные технологии создания брандмауэров и IDS-комплексов; Основные принципы административно-правовой защиты информации	Приемами обнаружения вирусных угроз Приемами обнаружения нарушений протокола сетевой безопасности Навыками работы по администрированию и настройке производственных программных систем и локальных сетей с точки зрения информационной безопасности
ПК-2.3.	математические принципы, лежащие в основе криптографических моделей этапы решения задач сетевой безопасности на компьютере; терминологию из области криптологии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений;	пользоваться современным программным обеспечением для решения задач информационной безопасности. Настраивать сетевое программное обеспечение по протоколу политики информационной безопасности предприятия	владеть навыками решения задач криптоанализа и шифрования для поддержания протоколов информационной безопасности Навыками защиты информации с помощью криптосистем Навыками применения дублирующих брандмауэров и протоколов сетевой безопасности

5. Форма промежуточной аттестации и семестр прохождения

Зачёт (6 семестр)

Дисциплина реализуется частично с применением дистанционных образовательных технологий.