


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Кафедра «Вычислительной и прикладной математики»

«СОГЛАСОВАНО»

Декан факультета ВТ

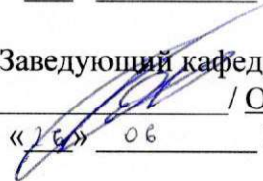
 / Перепелкин Д.А.
« 26 » 06 20 20 г

«УТВЕРЖДАЮ»

Проректор РОПиМД

 / Корячко А.В.
« 26 » 06 20 20 г

Заведующий кафедрой ВПМ

 / Овечкин Г.В.
« 26 » 06 20 20 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.01.25 «ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки
09.03.04 «Программная инженерия»

Направленность (профиль) подготовки
«Программная инженерия»

Уровень подготовки
Бакалавриат

Квалификация выпускника – бакалавр


Формы обучения – очная

Рязань 2020 г

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) 09.03.04 «Программная инженерия», утвержденного 19.09.2017 г. № 920

Разработчик
Доцент каф. ВПИМ

 Швечкова О.Г.

Программа рассмотрена и одобрена на заседании кафедры

«11» _06_ 2020 г., протокол № 11

Заведующий кафедрой
Вычислительной и прикладной математики
д.т.н., проф.

 Овечкин Г.В.

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является приобретение базовых знаний и умений в соответствии с Федеральным государственным образовательным стандартом в сфере обеспечения безопасности информации и информационных систем на базе современных информационных технологий, посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.

Задачи:

- Изучение проблем защиты информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.
- Изучение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам.
- Изучение механизмов и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;
- Освоение основных методов и приемов построения защищенных информационных систем, использования программных методов защиты информации. Использование современных алгоритмов криптографической защиты и механизмов цифровой подписи для реализации защищенного электронного документооборота.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.О.01.25 относится к дисциплинам обязательной части Блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы (далее – образовательной программы) бакалавриата «Программная инженерия» направления 09.03.04 Программная инженерия.

Дисциплина базируется на знаниях, полученных в ходе изучения дисциплин: «Математический анализ», «Математическая логика и теория алгоритмов», «Вычислительная математика», «Основы информационных технологий», «Теория вероятностей и математическая статистика», «Объектно-ориентированное программирование», «Интернет-технологии».

Для освоения дисциплины обучающиеся должны

- *знать:*
 - основные понятия базовых разделов высшей математики, дискретной математики, информатики, теории вероятностей;
 - принципы, приемы, методы объектно-ориентированного программирования, основы современных информационных технологий;
- *уметь:*
 - применять свои знания при решении различных предметных задач;
 - работать в средах программирования, ориентированных на соответствующие предметные области, разрабатывать и использовать специализированные программные средства;
- *владеть:*
 - навыками применения математических методов и проектирования алгоритмов, знаниями в области архитектуры информационных систем;
 - методами и приемами разработки и использования специализированных программных средств.

Результаты обучения, полученные при освоении дисциплины, необходимы далее для выполнения НИР и при подготовке выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ПООП (при наличии) по данному направлению подготовки, а также компетенций (при наличии), установленных университетом.

Общепрофессиональные компетенции выпускников и индикаторы и достижения

Категория (группа) общепрофессиональных компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК-3	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p>ОПК-3.1. Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p> <p>ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p> <p>ОПК-3.3. Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры, с учетом соблюдения авторского права и требований информационной безопасности данных с помощью средств вычислительной техники.</p>

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3зачетных единицы (ЗЕ), 108 часов.

Объем дисциплины	Всего часов	Семестр 7
Общая трудоемкость дисциплины, в том числе:	108	108
1. Контактная работа обучающихся с преподавателем (всего), в том числе:	48,25	48,25
Лекции	16	16
лабораторные работы	16	16
практические занятия	16	16
иная контактная работа (ИКР)	0,25	0,25
консультация	-	-
2. Самостоятельная работа	51	51
3. Курсовой проект	-	-
4. Контроль	8,75	8,75
Вид промежуточной аттестации		Зачет

4.2 Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№	Раздел дисциплины	Общая трудоемкость, всего часов	Контактная работа обучающихся с преподавателем				Самостоятельная работа обучающихся
			всего	лекции	Лабораторные занятия	Практические занятия	
Семестр 7							
	Всего	108	48	16	16	16	51
1	<i>1 раздел</i> Базовые понятия области защиты информации и безопасности информационных систем.	10	4	2		2	6
2	<i>2 раздел</i> Угрозы информационной безопасности	10	4	2		2	6
3	<i>3 раздел</i> Общие подходы к	12	6	2	2	2	6

	проблеме защиты информации. Основные методы и средства защиты безопасности						
4	<i>4 раздел</i> Основные понятия теории защиты информации	10	4	2		2	6
5	<i>5 раздел</i> Понятие информационного сервиса безопасности	10	4	2	2		6
6	<i>браздел</i> Защита интернет-подключений.	8	6	2	4		2
7	<i>7 раздел</i> Разрушающие программные средства. Вирусы, троянские программы	16	8	2	2	4	8
8	<i>8 раздел</i> Криптографические методы защиты информации. Электронная цифровая подпись	23	12	2	6	4	11
9	Зачет	9					

4.3. Содержание разделов дисциплины, структурированное по темам

4.3.1 Лекционные занятия

7 семестр

№ п/п	Темы лекционных занятий	Трудоемкость (час)	Формируемые компетенции	Форма контроля
1	Проблема информационной безопасности общества. Основные термины и определения данной предметной области. Задачи по защите информации и информационных систем. Уровни формирования режима информационной безопасности. Обзор нормативно-правовых документов в области защиты	2	ОПК-3	Зачет

	информации. Государственные стандарты РФ – руководящие документы Гостехкомиссии России по защите информации.			
2	Исследование причин нарушения безопасности. Понятие угрозы информационной безопасности. Классификация угроз по различным классификационным признакам. Понятие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации. Каналы несанкционированного доступа к информации.	2	ОПК-3	Зачет
3	Оценка рисков в сфере информационной безопасности. Основные методы средства, механизмы защиты информации.	2	ОПК-3	Зачет
4	Теоретические основы информационной безопасности. Понятия «объект», «субъект», «сущность», «процесс». Понятие модели безопасности. Виды моделей безопасности в зависимости от реализуемых функций защиты. Понятие политики безопасности. Мандатная, дискреционная, ролевая политики безопасности.	2	ОПК-3	Зачет
5	Обзор проблем безопасности наиболее популярных Internet-сервисов. Задачи обеспечения информационной безопасности сетей. Комплексный подход к реализации основных функциональных компонентов безопасности сетевых систем обработки информации с использованием методов и средств криптографии, механизмов аутентификации и авторизации, анти-вирусных средств, межсетевого экранирования.	2	ОПК-3	Зачет
6	Функции и назначение межсетевых экранов. Требования к межсетевым экранам. Классификация межсетевых экранов.	4	ОПК-3	Зачет

	Механизмы построения виртуальных защищенных сетей (VPN-технологии).			
7	Вредоносные программы как угроза информационной безопасности. Хронология и классификация вредоносного программного обеспечения. Анти-вирусные программы, особенности, качество их работы. Методы защиты от вредоносных программ.	2	ОПК-3	Зачет
8	Понятие криптографических методов защиты информации. Классификация криптографических методов. Простейшие шифры и их свойства. Оценка криптостойкости шифров. Системы шифрования с симметричным и открытым ключом. Современные алгоритмы шифрования. Понятие электронной цифровой подписи. Законодательные акты, регламентирующие использование электронной цифровой подписи при реализации электронного документооборота. Процедуры постановки и проверки электронной цифровой подписи. Понятие и свойства хэш-функции. Современные алгоритмы электронной цифровой подписи	2	ОПК-3	Зачет

4.3.2 Лабораторные занятия

7 семестр

№ п/п	Наименование лабораторных работ	Трудоемкость (час)	Формируемые компетенции	Форма контроля
1	Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Защита от разрушающих программных средств..	2	ОПК-3	Зачет

2	Шифры перестановки, замены, гаммирования	2	ОПК-3	Зачет
3	Системы с открытым ключом. Алгоритм RSA.	2	ОПК-3	Зачет
4	Схема шифрования Полига – Хеллмана.	2	ОПК-3	Зачет
5	Схема шифрования Эль-Гамала.	2	ОПК-3	Зачет
6	Потоковый шифр RC4.	2	ОПК-3	Зачет
7	Алгоритмы электронной цифровой подписи. Схема DSA.	2	ОПК-3	Зачет
8	Алгоритмы электронной цифровой подписи. Схема ГОСТ, алгоритм Шнорра.	2	ОПК-3	Зачет

4.3.3 Практические занятия (семинары)

7 семестр

№ п/п	Наименование лабораторных работ	Трудоемкость (час)	Формируемые компетенции	Форма контроля
1	Изучение понятия «информационная безопасность» в различных контекстах. Закон РФ «Об участии в международном информационном обмене». Доктрина информационной безопасности Российской Федерации. Понятие защиты информации как комплекса мероприятий, направленных на обеспечение информационной безопасности..	2	ОПК-3	Зачет
2	Построение сценария функционирования компьютерной системы в среде реально существующих угроз с учетом ролей всех участников процесса обработки и потребления информации позволяет определить механизмы построения защищенной системы обработки информации и свести к минимуму ущерб от возможных нарушений.	2	ОПК-3	Зачет

3	Изучение законодательных актов РФ в области защиты информации и информационных систем от разрушающих программных средств. Изучение различных видов разрушающих программных средств.	2	ОПК-3	Зачет
4	Системно-концептуальный подход при решении задачи защиты информации в КС. Сущность концептуального подхода. Обеспечение безопасности данных означает гарантией конфиденциальности, целостности и доступности. Критерии безопасности данных. Три основные функции обеспечения безопасности данных. Принципы создания систем информационной безопасности.	2	ОПК-3	Зачет
5	Понятие компьютерного вируса. Классификация вирусов по различным признакам. Изучение алгоритмов работы резидентных вирусов, вирусов, использующих стелс-алгоритмы, полиморфичность. Анализ деструктивных, разрушительных возможностей разрушающих программных средств. Основной механизм заражения вирусом, макровирусом. Методы обнаружения макровируса. Методы обезвреживания макровируса	2	ОПК-3	Зачет
6	Основные понятия и определения электронной цифровой подписи. Основные алгоритмы электронной цифровой подписи. Виды атак на электронную цифровую подпись. Математическая и программная реализация алгоритмов электронной цифровой подписи.	2	ОПК-3	Зачет

4.3.4 Самостоятельная работа

7семестр

№ п/п	Тематика самостоятельной работы	Трудоемкость (час)	Формируемые компетенции	Форма контроля
-------	---------------------------------	--------------------	-------------------------	----------------

1	Проблемы защиты информации для открытых информационных систем. Характеристики, влияющие на безопасность информации.	6	ОПК-3	Зачет
2	Возможности сети Интернет и проблемы безопасности. Угрозы и уязвимости корпоративных сетей и систем.	6	ОПК-3	Зачет
3	Политика безопасности в сетях. Технологии безопасности данных.	6	ОПК-3	Зачет
4	Типовые решения по применению межсетевых экранов для защиты информационных ресурсов.	6	ОПК-3	Зачет
5	Методы управления средствами сетевой безопасности.	6	ОПК-3	Зачет
6	Типовые решения по применению межсетевых экранов для защиты информационных ресурсов.	2	ОПК-3	Зачет
7	Освоение приемов противодействия разрушающим программным средствам.	8	ОПК-3	Зачет
8	Основные принципы работы алгоритма отечественной цифровой подписи «Нотариус».	11	ОПК-3	Зачет

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Защита информации»»).

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Основная учебная литература

1. Защита информации с использованием механизмов электронной цифровой подписи: учебно-метод. пособие / Д.Г. Демидов, О.Г. Швечкова, О.А. Москвитина, А.Н. Пылькин, К.А. Майков, К.Г. Смирнова; Моск. гос. ун-т печати имени Ивана Федорова. – М.: МГУП имени Ивана Федорова, 2014. – 53 с.
2. Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS: учеб. пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. – М.: КУРС, 2017. – 296 с.
Данное издание представлено в библиотеке РГРТУ в количестве 40 экземпляров.
3. Базовые криптографические алгоритмы защиты информации : Учебное пособие/ О.Г. Швечкова, А.Н. Пылькин, Д.В. Марчев.- М: Курс, 2018.- с.

- Данное издание представлено в библиотеке РГРТУ в количестве 40 экземпляров.
4. Криптографические методы защиты информации: учеб. пособие / С. Б. Гашков, Э. А. Применко, М. А. Черепнев – М.: Академия, 2010. – 304 с.
Данное издание представлено в библиотеке РГРТУ в количестве 16 экземпляров.
 5. Башлы, П. Н. Информационная безопасность и защита информации: учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — М. : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/10677.html>
 6. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — Самара : Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — ISBN 978-5-9585-0603-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/43183.html>
 7. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — Саратов : Профобразование, 2017. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/63594.html>
 8. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов: Вузовское образование, 2018. — 218 с. — ISBN 978-5-4487-0297-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/77317.html>
 9. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/87995.html>
 10. Программно-аппаратные средства защиты информации : учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.] ; под редакцией В. К. Головати. — СПб. : Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/73644.html>
 11. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю. Н. Сычев. — Саратов : Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/72345.html>
 12. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере / А. Е. Фаронов. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/52160.html>
 13. Скрипник, Д. А. Общие вопросы технической защиты информации / Д. А. Скрипник. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —
Режим доступа: URL: <http://www.iprbookshop.ru/52161.html>

6.2 Дополнительная учебная литература:

14. Пржегорлинский В.Н. Объекты защиты информации : учеб. пособие. Ч.1: Элементарные объекты защиты информации / В. Н. Пржегорлинский; РГРТУ. – Рязань, 2012. –

131с.

Данное издание представлено в библиотеке РГРТУ в количестве 19 экземпляров.

15. Пржегорлинский В.Н. Защита информации : учеб. пособие. Ч.2: Комплексные объекты защиты информации. Условия защиты информации / В. Н. Пржегорлинский; РГРТУ. – Рязань, 2013. – 87с.

Данное издание представлено в библиотеке РГРТУ в количестве 47 экземпляров.

16. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — ISBN 978-5-94774-821-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —

Режим доступа: URL: <http://www.iprbookshop.ru/52209.html>

17. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 с. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —

Режим доступа: URL: <http://www.iprbookshop.ru/72341.html>

18. Технологии защиты информации в компьютерных сетях / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. — 2-е изд. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 368 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —

Режим доступа: URL: <http://www.iprbookshop.ru/73732.html>

6.3 Нормативно правовые акты

6.4 Периодические издания

6.5 Методические указания к практическим занятиям/ лабораторным занятиям

1. Современные алгоритмы криптографической защиты информации: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т; сост.: О.Г. Швечкова, О.А. Москвитина, Н.С. Курдюков. – Рязань, 2012. – 40 с. – № 4605.

Данное издание размещено в электронной библиотеке РГРТУ.

– URL: <http://elib.rsreu.ru/ebs>, а также представлено в библиотеке РГРТУ в количестве **40** экземпляров.

2. Основы теории и практики реализации криптографических алгоритмов защиты информации: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т; сост.: О.Г. Швечкова, О.А. Москвитина, Н.С. Курдюков. – Рязань, 2012. – 48 с. – № 4606.

Данное издание размещено в электронной библиотеке РГРТУ.

– URL: <http://elib.rsreu.ru/ebs>, а также представлено в библиотеке РГРТУ в количестве **40** экземпляров.

3. Алгоритмы электронной цифровой подписи. Схема ГОСТ Р 34.10-2001: методические указания к лабораторным работам/ Рязан. гос. радиотехн. ун-т; сост.: О.Г. Швечкова, О.А. Москвитина. – Рязань, 2013. – 16 с. – № 4721.

Данное издание размещено в электронной библиотеке РГРТУ.

– URL: <http://elib.rsreu.ru/ebs>,

а также представлено в библиотеке РГРТУ в количестве **20** экземпляров.

4. Алгоритмы электронной цифровой подписи. Схема Эль-Гамала: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т; сост.: О.Г. Швечкова, О.А. Москвитина. – Рязань, 2013. – 16 с. – № 4722.

Данное издание размещено в электронной библиотеке РГРТУ.

– URL: <http://elib.rsreu.ru/ebs>,

а также представлено в библиотеке РГРТУ в количестве **20** экземпляров.

5. Алгоритмы электронной цифровой подписи. Схема DSA: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т; сост.: О.Г. Швечкова, О.А. Москвитина. – Рязань, 2013. – 16 с. – № 4723.

Данное издание размещено в электронной библиотеке РГРТУ.

– URL: <http://elib.rsreu.ru/ebs>,

а также представлено в библиотеке РГРТУ в количестве **20** экземпляров.

6. Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Схемы электронной цифровой подписи. Алгоритм Шнорра: методические указания к лабораторной работе / Рязан. гос. радиотехн. ун-т; сост.: В.А. Швечков, О.Г. Швечкова. – Рязань, 2014. – 20 с. – № 4780.

Данное издание размещено в электронной библиотеке РГРТУ.

– URL: <http://elib.rsreu.ru/ebs>,

а также представлено в библиотеке РГРТУ в количестве **20** экземпляров.

7. Методы контроля, обеспечения достоверности и защиты информационного и программного обеспечения. Защита от разрушающих программных средств: методические указания к лабораторной работе / Рязан. гос. радиотехн. ун-т; сост.: В.А. Швечков, О.Г. Швечкова. – Рязань, 2014. – 16 с. – № 4789.

Данное издание размещено в электронной библиотеке РГРТУ.

– URL: <http://elib.rsreu.ru/ebs>, а

также представлено в библиотеке РГРТУ в количестве **20** экземпляров.

8. Алгоритмы стеганографической защиты информации: методические указания к лабораторным работам/ Рязан. гос. радиотехн. ун-т; сост.: О.Г. Швечкова. - Рязань, 2017.- 32 с.- № 5121

Данное издание размещено в электронной библиотеке РГРТУ.

– URL: <http://elib.rsreu.ru/ebs>, а

также представлено в библиотеке РГРТУ в количестве **20** экземпляров

6.6 Методические указания к курсовому проектированию (курсовой работе) и другим видам самостоятельной работы

Изучение дисциплины «Защита информации» проходит в течение 1 семестра. Основные темы дисциплины осваиваются в ходе аудиторных занятий, однако важная роль отводится и самостоятельной работе студентов.

Самостоятельная работа включает в себя следующие этапы:

- изучение теоретического материала (работа над конспектом лекции);
- самостоятельное изучение дополнительных информационных ресурсов (доработка конспекта лекции);
- выполнение заданий текущего контроля успеваемости (подготовка к практическому занятию);
- итоговая аттестация по дисциплине (подготовка к зачету и экзамену).

Работа над конспектом лекции: лекции – основной источник информации по предмету, позволяющий не только изучить материал, но и получить представление о наличии других источников, сопоставить разные способы решения задач и практического применения получаемых знаний. Лекции предоставляют возможность «интерактивного» обучения, когда есть возможность задавать преподавателю вопросы и получать на них ответы. Поэтому рекомендуется в день, предшествующий очередной лекции, прочитать конспекты двух предшествующих лекций, обратив особое внимание на содержимое последней лекции.

Подготовка к практическому занятию: состоит в теоретической подготовке (изучение конспекта лекций и дополнительной литературы) и выполнении практических заданий (решение задач, ответы на вопросы и т.д.). Во время самостоятельных занятий студенты выполняют задания, выданные им на предыдущем практическом занятии, готовятся к контрольным работам, выполняют задания типовых расчетов.

Доработка конспекта лекции с применением учебника, методической литературы,

дополнительной литературы, интернет-ресурсов: этот вид самостоятельной работы студентов особенно важен в том случае, когда одну и ту же задачу можно решать различными способами, а на лекции изложен только один из них. Кроме того, рабочая программа по математике предполагает рассмотрение некоторых относительно несложных тем только во время самостоятельных занятий, без чтения лектором.

Подготовка к зачету, экзамену: основной вид подготовки – «свертывание» большого объема информации в компактный вид, а также тренировка в ее «развертывании» (примеры к теории, выведение одних закономерностей из других и т.д.). Надо также правильно распределить силы, не только готовясь к самому экзамену, но и позаботившись о допуске к нему (это хорошее посещение занятий, выполнение в назначенный срок типовых расчетов, активность на практических занятиях).

7. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Система дистанционного обучения ФГБОУ ВО «РГРТУ», режим доступа. - <http://cdo.rsreu.ru/>
2. Единое окно доступа к образовательным ресурсам: <http://window.edu.ru/>
3. Интернет Университет Информационных Технологий: <http://www.intuit.ru/>
4. Электронно-библиотечная система «IPRbooks» [Электронный ресурс]. – Режим доступа: доступ из корпоративной сети РГРТУ – свободный, доступ из сети Интернет – по паролю. – URL: <https://iprbookshop.ru/>.
5. Электронно-библиотечная система издательства «Лань» [Электронный ресурс]. – Режим доступа: доступ из корпоративной сети РГРТУ – свободный, доступ из сети Интернет – по паролю. – URL: <https://www.e.lanbook.com>
6. Электронная библиотека РГРТУ [Электронный ресурс]. – Режим доступа: из корпоративной сети РГРТУ – по паролю. – URL: <http://elib.rsreu.ru/ebs>.

8. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. Операционная система Windows XP (Microsoft Imagine, номер подписки 700102019, бессрочно);
2. Microsoft Visual Studio (Microsoft Imagine: Номер подписки 700102019, бессрочно)
3. Свободно распространяемое программное обеспечение под лицензиями GNU, Apache, Oracle, Mozilla, CeCILL2.
4. Свободно распространяемая версия языка Питон 3.7.4. <https://python.org/downloads/windows/>, "latest python release", python 3.
5. Kaspersky Endpoint Security (Коммерческая лицензия на 1000 компьютеров №2304-180222-115814-600-1595, срок действия с 25.02.2018 по 05.03.2019);
6. LibreOffice

7. Adobe acrobat reader
8. Справочная правовая система «Консультант Плюс» [Электронный ресурс]. – Режим доступа: доступ из корпоративной сети РГРТУ – свободный.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для освоения дисциплины необходимы следующие материально-технические ресурсы:

- 1) аудитория для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации, оборудованная маркерной (меловой) доской;
- 2) аудитория для самостоятельной работы, оснащенная индивидуальной компьютерной техникой с подключением к локальной вычислительной сети и сети Интернет.

№	Наименование специальных помещений и помещений для самостоятельной работы	Перечень специализированного оборудования
1	Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №206-1 главный учебный корпус	42 посадочных места, 1 ПК: ЦП: Intel Pentium 4 class 3200 ОЗУ: 1 Гб ПЗУ: 80 Гб Телевизор: PHILIPS U7PEL4606H/60 документ-камера: AVER Media POB3 (AverVision 330)
2	Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации; Аудитория для самостоятельной работы №206-2 главный учебный корпус	18 посадочных мест, Телевизор PHILIPS 46PFL3208T/60; документ-камера: AverVisionF33 POE7D; 20 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel Pentium II/III class 2327 ОЗУ: 2 Гб ПЗУ: 80 Гб (1 шт.) ЦП: Intel Pentium III 2992 ОЗУ: 1,5 Гб ПЗУ: 150 Гб (1 шт.) ЦП: Intel Pentium III 2660 ОЗУ: 2 Гб ПЗУ: 80 Гб (9 шт.) ЦП: Intel Pentium III 2793 ОЗУ: 2 Гб ПЗУ: 100 Гб (1 шт.) ЦП: Intel Pentium II/III class 2660 ОЗУ: 1 Гб

		ПЗУ: 50 Гб (1 шт.) ЦП: Intel Pentium III 2527 ОЗУ: 2 Гб ПЗУ: 100 Гб (1 шт.) ЦП: Intel Pentium III 3158 ОЗУ: 2 Гб ПЗУ: 50 Гб (3 шт.) ЦП: Intel Pentium III 2826 ОЗУ: 2 Гб ПЗУ: 100 Гб (2 шт.) ЦП: Intel Pentium III 2693 ОЗУ: 1,5 Гб ПЗУ: 100 Гб (1 шт.)
3	Учебная аудитория для проведения практических занятий, лабораторных работ и самостоятельной работы №206-3 главный учебный корпус	Проектор: InFocus LP640 18 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel Pentium 4 class 2800 ОЗУ: 1 Гб ПЗУ: 50 Гб (11 шт.) ЦП: Intel Pentium 4 class 3200 ОЗУ: 1 Гб ПЗУ: 50 Гб (5 шт.) ЦП: Intel Pentium 4 class 2800 ОЗУ: 500 Мб ПЗУ: 50 Гб (1 шт.) ЦП: Intel Pentium 4 class 2800 ОЗУ: 2 Гб ПЗУ: 50 Гб (1 шт.)
4	Учебная аудитория для проведения практических занятий, лабораторных работ и самостоятельной работы №206-4 главный учебный корпус	18 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Pentium 4 class 2800 ОЗУ: 1 Гб ПЗУ: 50 Гб (8 шт.) ЦП: Intel Pentium II/III class 2327 ОЗУ: 2 Гб ПЗУ: 50 Гб (10 шт.)
5	Учебная аудитория для проведения практических занятий, лабораторных работ и самостоятельной работы №206-5 главный учебный корпус	24 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel Pentium II/III class 2394

		ОЗУ: 2 Гб ПЗУ: 70 Гб (17 шт.) ЦП: Intel Pentium II/III class 2327 ОЗУ: 2 Гб ПЗУ: 100 Гб (1 шт.) ЦП: Intel Pentium III Xeon 3093 ОЗУ: 4 Гб ПЗУ: 300 Гб (6 шт.)
--	--	--