

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
"РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ  
ИМЕНИ В.Ф. УТКИНА"**

СОГЛАСОВАНО  
Зав. выпускающей кафедры

УТВЕРЖДАЮ

## **Основы информационной безопасности** рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Автоматики и информационных технологий в управлении**  
Учебный план 27.03.04\_24\_00.plx  
27.03.04 Управление в технических системах  
Квалификация **бакалавр**  
Форма обучения **очная**  
Общая трудоемкость **3 ЗЕТ**

### **Распределение часов дисциплины по семестрам**

Семестр (<Курс>. <Семестр на курсе>)	<b>6 (3.2)</b>		Итого	
	16			
Неделя	16			
Вид занятий	уп	рп	уп	рп
Лекции	32	32	32	32
Практические	16	16	16	16
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	48,25	48,25	48,25	48,25
Контактная работа	48,25	48,25	48,25	48,25
Сам. работа	51	51	51	51
Часы на контроль	8,75	8,75	8,75	8,75
Итого	108	108	108	108

г. Рязань

Программу составил(и):

*к.т.н., доц., Смирнов Сергей Александрович*

Рабочая программа дисциплины

**Основы информационной безопасности**

разработана в соответствии с ФГОС ВО:

ФГОС ВО - бакалавриат по направлению подготовки 27.03.04 Управление в технических системах (приказ Минобрнауки России от 31.07.2020 г. № 871)

составлена на основании учебного плана:

27.03.04 Управление в технических системах

утвержденного учёным советом вуза от 26.01.2024 протокол № 8.

Рабочая программа одобрена на заседании кафедры

**Автоматики и информационных технологий в управлении**

Протокол от 22.03.2024 г. № 7

Срок действия программы: 20242028 уч.г.

Зав. кафедрой Бабаян Павел Варганович

---

---

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры  
**Автоматики и информационных технологий в управлении**

Протокол от \_\_\_\_\_ 2025 г. № \_\_\_\_

Зав. кафедрой \_\_\_\_\_

---

---

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры  
**Автоматики и информационных технологий в управлении**

Протокол от \_\_\_\_\_ 2026 г. № \_\_\_\_

Зав. кафедрой \_\_\_\_\_

---

---

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры  
**Автоматики и информационных технологий в управлении**

Протокол от \_\_\_\_\_ 2027 г. № \_\_\_\_

Зав. кафедрой \_\_\_\_\_

---

---

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры

**Автоматики и информационных технологий в управлении**

Протокол от \_\_\_\_\_ 2028 г. № \_\_\_\_

Зав. кафедрой \_\_\_\_\_

<b>1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>	
1.1	Целью освоения дисциплины «Основы информационной безопасности» является изучение основных принципов информационной безопасности.
1.2	Задачи дисциплины: изучение базовых вопросов информационной безопасности; изучение законодательных, административных, организационных и технических мер защиты информации.

<b>2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ</b>	
Цикл (раздел) ОП:	
<b>2.1</b>	<b>Требования к предварительной подготовке обучающегося:</b>
2.1.1	Информатика
2.1.2	Ознакомительная практика
2.1.3	Учебная практика
2.1.4	Научно-исследовательская практика
2.1.5	Компьютерная графика
<b>2.2</b>	<b>Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>
2.2.1	Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.2	Научно-исследовательская работа
2.2.3	Преддипломная практика

<b>3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>	
<b>ОПК-5: Способен решать задачи развития науки, техники и технологии в области управления в технических системах с учетом нормативно-правового регулирования в сфере интеллектуальной собственности</b>	
<b>ОПК-5.1. Проводит патентные исследования</b>	
<b>Знать</b> алгоритмы и порядок проведения патентных исследований	
<b>Уметь</b> проводить патентные исследования	
<b>Владеть</b> алгоритмами проведения патентных исследований	
<b>ОПК-5.2. Определяет формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности</b>	
<b>Знать</b> формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности	
<b>Уметь</b> определять формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности	
<b>Владеть</b> знаниями о формах и методах правовой охраны и защиты прав на результаты интеллектуальной деятельности	
<b>ОПК-5.3. Распоряжается правами на результаты интеллектуальной деятельности для решения задач в развитии науки, техники и технологии</b>	
<b>Знать</b> права на результаты интеллектуальной деятельности для решения задач в развитии науки, техники и технологии	
<b>Уметь</b> распоряжаться правами на результаты интеллектуальной деятельности для решения задач в развитии науки, техники и технологии	
<b>Владеть</b> знаниями о правах на результаты интеллектуальной деятельности для решения задач в развитии науки, техники и технологии	
<b>ОПК-11: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности</b>	
<b>ОПК-11.1. Понимает принципы работы современных информационных технологий</b>	
<b>Знать</b> принципы работы современных информационных технологий	
<b>Уметь</b> понимать принципы работы современных информационных технологий	
<b>Владеть</b> принципами работы современных информационных технологий	
<b>ОПК-11.2. Использует современные информационные технологии для решения задач профессиональной деятельности</b>	

<b>Знать</b> современные информационные технологии для решения задач профессиональной деятельности
<b>Уметь</b> использовать современные информационные технологии для решения задач профессиональной деятельности
<b>Владеть</b> современными информационными технологиями для решения задач профессиональной деятельности

**В результате освоения дисциплины (модуля) обучающийся должен**

<b>3.1</b>	<b>Знать:</b>
3.1.1	тенденции развития угроз информационной безопасности, перспективные методы противодействия вредоносным программам
<b>3.2</b>	<b>Уметь:</b>
3.2.1	эффективно организовать свою практическую деятельность с учетом потенциальных угроз несанкционированного доступа третьих лиц, обеспечить целостность, аутентичность и избежание утечек информации
<b>3.3</b>	<b>Владеть:</b>
3.3.1	навыками настройки операционной системы для разграничения доступа и настройки программного антивирусного обеспечения.

**4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Форма контроля
	<b>Раздел 1. Основы информационной безопасности</b>					
1.1	Информационная безопасность (ИБ). Введение /Тема/	6	0			Зачет
1.2	Информационная безопасность (ИБ). Введение /Лек/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.3	Информационная безопасность (ИБ). Введение /Ср/	6	11	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.4	ИБ автоматизированных систем /Тема/	6	0			Зачет
1.5	Угрозы ИБ. Общие требования к ИБ АС. Концепция обеспечения ИБ. Нарушители безопасности информации. Модель угроз /Лек/	6	12	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет

1.6	Угрозы ИБ. Общие требования к ИБ АС. Концепция обеспечения ИБ. Нарушители безопасности информации. Модель угроз /Ср/	6	24	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.7	Меры обеспечения защиты информации /Тема/	6	0			Зачет
1.8	Законодательные, административные и организационные меры /Лек/	6	6	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.9	Технические меры защиты информации /Лек/	6	6	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	
1.10	Криптографические и стеганографические методы защиты /Лек/	6	4	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	
1.11	Защита интеллектуальной собственности /Лек/	6	2	ОПК-5.1-3 ОПК-5.1-У ОПК-5.1-В ОПК-5.2-3 ОПК-5.2-У ОПК-5.2-В ОПК-5.3-3 ОПК-5.3-У ОПК-5.3-В ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	

1.12	Организационные меры защита информации /Пр/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.13	Управление доступом. Учётные записи пользователей /Пр/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.14	Управление доступом. Разграничение доступа к ресурсам в операционной системе /Пр/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.15	Управление доступом. Стойкость парольной защиты /Пр/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.16	Настройки параметров аудита в операционной системе. /Пр/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет

1.17	Обеспечение целостности и доступности данных /Пр/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.18	Криптография /Пр/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.19	Стеганография /Пр/	6	2	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.20	Меры обеспечения защиты информации /Ср/	6	16	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
<b>Раздел 2. Промежуточная аттестация</b>						
2.1	Подготовка и сдача зачета /Тема/	6	0			
2.2	Сдача зачета /ИКР/	6	0,25	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет

2.3	Подготовка к зачету /Зачёт/	6	8,75	ОПК-11.1-3 ОПК-11.1-У ОПК-11.1-В ОПК-11.2-3 ОПК-11.2-У ОПК-11.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.8 Л1.9Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
-----	-----------------------------	---	------	--	--	-------

### 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ "Оценочные материалы по дисциплине "Основы информационной безопасности")

### 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

#### 6.1. Рекомендуемая литература

##### 6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л1.1	Новиков С. Н., Солонская О. И.	Методы защиты информации : учебное пособие	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2009, 121 с.	2227-8397, <a href="http://www.iprbookshop.ru/54767.html">http://www.iprbookshop.ru/54767.html</a>
Л1.2	Астайкин А. И., Мартынов А. П., Николаев Д. Б., Фомченко В. Н.	Методы и средства обеспечения программно-аппаратной защиты информации : научно-техническое издание	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015, 224 с.	978-5-9515-0305-3, <a href="http://www.iprbookshop.ru/60959.html">http://www.iprbookshop.ru/60959.html</a>
Л1.3	Бехроуз А., Берлин А. Н.	Криптография и безопасность сетей : учебное пособие	Москва, Саратов: Интернет- Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017, 782 с.	978-5-4487-0143-6, <a href="http://www.iprbookshop.ru/72337.html">http://www.iprbookshop.ru/72337.html</a>
Л1.4	Джонс К. Д., Шема М., Джонсон Б. С.	Инструментальные средства обеспечения безопасности	Москва: Интернет- Университет Информационных Технологий (ИНТУИТ), 2016, 914 с.	2227-8397, <a href="http://www.iprbookshop.ru/73679.html">http://www.iprbookshop.ru/73679.html</a>
Л1.5	Суворова Г. М.	Информационная безопасность : учебное пособие	Саратов: Вузовское образование, 2019, 214 с.	978-5-4487-0585-4, <a href="http://www.iprbookshop.ru/86938.html">http://www.iprbookshop.ru/86938.html</a>

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л1.6	Петров А. А.	Компьютерная безопасность. Криптографические методы защиты	Саратов: Профобразование, 2019, 446 с.	978-5-4488-0091-7, <a href="http://www.iprbookshop.ru/87998.html">http://www.iprbookshop.ru/87998.html</a>
Л1.7	Тюльпинова Н. В.	Защита интеллектуальной собственности и компьютерной информации : учебное пособие для магистров	Саратов: Вузовское образование, 2020, 341 с.	978-5-4487-0611-0, <a href="http://www.iprbookshop.ru/88755.html">http://www.iprbookshop.ru/88755.html</a>
Л1.8	Сергиенко Е. Н.	Математические методы кодирования и шифрования : учебное пособие	Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2017, 101 с.	2227-8397, <a href="http://www.iprbookshop.ru/92262.html">http://www.iprbookshop.ru/92262.html</a>
Л1.9	Червяков Н. И., Бабенко М. Г., Гладков А. В.	Вероятностные методы оценки состояния информационной безопасности : учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2017, 182 с.	2227-8397, <a href="http://www.iprbookshop.ru/92536.html">http://www.iprbookshop.ru/92536.html</a>
<b>6.1.2. Дополнительная литература</b>				
№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л2.1	Симонян А. Г.	Учебно-методическое пособие по дисциплине Методы и средства защиты компьютерной информации	Москва: Московский технический университет связи и информатики, 2016, 32 с.	2227-8397, <a href="http://www.iprbookshop.ru/61498.html">http://www.iprbookshop.ru/61498.html</a>
Л2.2	Котов Ю. А.	Криптографические методы защиты информации. Шифры : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2016, 59 с.	978-5-7782-2959-4, <a href="http://www.iprbookshop.ru/91377.html">http://www.iprbookshop.ru/91377.html</a>
Л2.3	Смирнов А. Э., Пономарёва Ю. А.	Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации	Москва: Московский технический университет связи и информатики, 2015, 67 с.	2227-8397, <a href="http://www.iprbookshop.ru/61738.html">http://www.iprbookshop.ru/61738.html</a>
Л2.4	Симонян А. Г., Режеб Т. Б. К.	Практикум по выполнению лабораторных работ по дисциплине Методы и средства защиты компьютерной информации	Москва: Московский технический университет связи и информатики, 2015, 58 с.	2227-8397, <a href="http://www.iprbookshop.ru/61743.html">http://www.iprbookshop.ru/61743.html</a>

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л2.5	Пашинцев В. П., Ляхов А. В.	Нестандартные методы защиты информации : лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2016, 196 с.	2227-8397, <a href="http://www.iprbookshop.ru/63217.html">http://www.iprbookshop.ru/63217.html</a>
Л2.6	Котова Л. В.	Сборник задач по дисциплине «Методы и средства защиты информации» : учебное пособие	Москва: Московский педагогический государственный университет, 2015, 44 с.	978-5-4263-0221-1, <a href="http://www.iprbookshop.ru/70020.html">http://www.iprbookshop.ru/70020.html</a>
Л2.7	Тебуева Ф. Б., Антонов В. О.	Теоретико-числовые методы в криптографии : учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2017, 107 с.	2227-8397, <a href="http://www.iprbookshop.ru/75601.html">http://www.iprbookshop.ru/75601.html</a>
Л2.8	Кирпичников А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации : учебное пособие	Казань: Казанский национальный исследовательский технологический университет, 2016, 100 с.	978-5-7882-2052-9, <a href="http://www.iprbookshop.ru/79313.html">http://www.iprbookshop.ru/79313.html</a>
Л2.9	Бондаренко И. С., Демчишин Ю. В.	Методы и средства защиты информации : лабораторный практикум	Москва: Издательский Дом МИСиС, 2018, 32 с.	2227-8397, <a href="http://www.iprbookshop.ru/84413.html">http://www.iprbookshop.ru/84413.html</a>
Л2.10	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, <a href="http://www.iprbookshop.ru/87995.html">http://www.iprbookshop.ru/87995.html</a>

### 6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Официальный интернет портал РГРТУ [электронный ресурс] <a href="http://www.rsreu.ru">http://www.rsreu.ru</a>
Э2	Образовательный портал РГРТУ [электронный ресурс]. - Режим доступа: по паролю.- <a href="https://edu.rsreu.ru">https://edu.rsreu.ru</a>
Э3	Электронная библиотека РГРТУ [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - по паролю. - <a href="http://elib.rsreu.ru/">http://elib.rsreu.ru/</a>
Э4	Электронно-библиотечная система IRPbooks [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - свободный, доступ из сети интернет- по паролю. - <a href="https://www.iprbookshop.ru/">https://www.iprbookshop.ru/</a>
Э5	Электронно-библиотечная система «Лань» [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - свободный, доступ из сети интернет- по паролю. - <a href="https://e.lanbook.com">https://e.lanbook.com</a>
Э6	

### 6.3 Перечень программного обеспечения и информационных справочных систем

#### 6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование	Описание
Операционная система Windows	Коммерческая лицензия
Kaspersky Endpoint Security	Коммерческая лицензия
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
Firefox	Свободное ПО

7 Zip	Свободное ПО
<b>6.3.2 Перечень информационных справочных систем</b>	
6.3.2.1	Информационно-правовой портал ГАРАНТ.РУ <a href="http://www.garant.ru">http://www.garant.ru</a>
6.3.2.2	Система КонсультантПлюс <a href="http://www.consultant.ru">http://www.consultant.ru</a>
6.3.2.3	Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.)

### 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	445 учебно-административный корпус. Учебная аудитория для проведения учебных занятий лекционного и семинарского типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Специальная мебель (54 посадочных места), компьютер с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, мультимедиа проектор, экран, доска, колонки звуковые.
2	449 учебно-административный корпус. Учебная аудитория для проведения учебных занятий семинарского типа, лабораторных работ, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 15 компьютеров с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, проектор, экран, доска, магнитный усилитель, фазовращатель, асинхронные приводы, осциллограф, электронный микроскоп, учебный роботизированный стенд, учебный комплект роботизированного оборудования Mindstorms, видеокамера
3	447 учебно-административный корпус. Помещение для самостоятельной работы обучающихся 10 компьютеров с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, учебный роботизированный стенд, видеокамеры, сервер данных

### 8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ "Методические указания дисциплины "Основы информационной безопасности")

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ	<b>ФГБОУ ВО "РГРТУ", РГРТУ</b> , Бабаян Павел Вартанович, Заведующий кафедрой АИТУ	<b>20.06.24</b> 13:11 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	<b>ФГБОУ ВО "РГРТУ", РГРТУ</b> , Бабаян Павел Вартанович, Заведующий кафедрой АИТУ	<b>20.06.24</b> 16:38 (MSK)	Простая подпись
ПОДПИСАНО НАЧАЛЬНИКОМ УРОП	<b>ФГБОУ ВО "РГРТУ", РГРТУ</b> , Ерзылёва Анна Александровна, Начальник УРОП	<b>20.06.24</b> 16:38 (MSK)	Простая подпись