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 **Автоматизированных систем управления**

Учебный план 27.03.04_26_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>)	**6 (3.2)**		Итого	
Недель	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., Челебаев Сергей Валерьевич

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 24.04.2026 протокол № 10.

Рабочая программа одобрена на заседании кафедры
Автоматизированных систем управления

Протокол от 27.06.2026 г. № 10
Срок действия программы: 2026-2030 уч.г.
Зав. кафедрой Холопов Сергей Иванович

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Автоматизированных систем управления

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
Автоматизированных систем управления

Протокол от __ _____ 2028 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры
Автоматизированных систем управления

Протокол от __ _____ 2029 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2030-2031 учебном году на заседании кафедры

Автоматизированных систем управления

Протокол от __ _____ 2030 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
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.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
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
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.2	Научно-исследовательская работа
2.2.3	Преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

ОПК-5.1. Проводит патентные исследования

Знать
алгоритмы и порядок проведения патентных исследований
Уметь
проводить патентные исследования
Владеть
алгоритмами проведения патентных исследований

ОПК-5.2. Определяет формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности

Знать
формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности
Уметь
определять формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности
Владеть
знаниями о формах и методах правовой охраны и защиты прав на результаты интеллектуальной деятельности

ОПК-5.3. Распоряжается правами на результаты интеллектуальной деятельности для решения задач в развитии науки, техники и технологии

Знать
права на результаты интеллектуальной деятельности для решения задач в развитии науки, техники и технологии
Уметь
распоряжаться правами на результаты интеллектуальной деятельности для решения задач в развитии науки, техники и технологии
Владеть
знаниями о правах на результаты интеллектуальной деятельности для решения задач в развитии науки, техники и технологии

ОПК-11: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ОПК-11.1. Понимает принципы работы современных информационных технологий

Знать
принципы работы современных информационных технологий
Уметь
понимать принципы работы современных информационных технологий
Владеть
принципами работы современных информационных технологий

ОПК-11.2. Использует современные информационные технологии для решения задач профессиональной деятельности

Знать
современные информационные технологии для решения задач профессиональной деятельности
Уметь
использовать современные информационные технологии для решения задач профессиональной деятельности
Владеть
современными информационными технологиями для решения задач профессиональной деятельности

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	тенденции развития угроз информационной безопасности, перспективные методы противодействия вредоносным программам
3.2	**Уметь:**
3.2.1	эффективно организовать свою практическую деятельность с учетом потенциальных угроз несанкционированного доступа третьих лиц, обеспечить целостность, аутентичность и избежание утечек информации
3.3	**Владеть:**
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	Компетен-ции	Литература	Форма контроля
	Раздел 1. Основы информационной безовасности					
1.1	Информационная безопасность (ИБ). Введение /Тема/	6	0			Зачет
1.2	Информационная безопасность (ИБ). Введение /Лек/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.3	Информационная безопасность (ИБ). Введение /Ср/	6	11	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 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-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 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-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 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-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.9	Технические меры защиты информации /Лек/	6	6	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.10	Криптографические и стеганографические методы защиты /Лек/	6	4	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.11	Защита интеллектуальной собственности /Лек/	6	2	ОПК-5.1-З ОПК-5.1-У ОПК-5.1-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.3-З ОПК-5.3-У ОПК-5.3-В ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.6 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет

1.12	Организационные меры защита информации /Пр/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.13	Управление доступом. Учётные записи пользователей /Пр/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.14	Управление доступом. Разграничение доступа к ресурсам в операционной системе /Пр/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.15	Управление доступом. Стойкость парольной защиты /Пр/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.16	Настройки параметров аудита в операционной системе. /Пр/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет

1.17	Обеспечение целостности и доступности данных /Пр/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.18	Криптография /Пр/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.19	Стеганография /Пр/	6	2	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
1.20	Меры обеспечения защиты информации /Ср/	6	16	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет
	Раздел 2. Промежуточная аттестация					
2.1	Подготовка и сдача зачета /Тема/	6	0			
2.2	Сдача зачета /ИКР/	6	0,25	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Зачет

2.3	Подготовка к зачету /Зачёт/	6	8,75	ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В	Л1.4 Л1.7 Л1.3 Л1.8 Л1.5 Л1.9 Л1.1 Л1.2Л2.1 Л2.7 Л2.2 Л2.8 Л2.9 Л2.3 Л2.4 Л2.10 Л2.5 Л2.6Л3.1 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	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, http://www.iprbookshop.ru/92262.html
Л1.2	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, http://www.iprbookshop.ru/92536.html
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, http://www.iprbookshop.ru/72337.html
Л1.4	Новиков С. Н., Солонская О. И.	Методы защиты информации : учебное пособие	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2009, 121 с.	2227-8397, http://www.iprbookshop.ru/54767.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.5	Суворова Г. М.	Информационная безопасность : учебное пособие	Саратов: Вузовское образование, 2023, 214 с.	978-5-4487-0585-4, http://www.iprbookshop.ru/86938.html
Л1.6	Тюльпинова Н. В.	Защита интеллектуальной собственности и компьютерной информации : учебное пособие для магистров	Саратов: Вузовское образование, 2020, 341 с.	978-5-4487-0611-0, http://www.iprbookshop.ru/88755.html
Л1.7	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, http://www.iprbookshop.ru/60959.html
Л1.8	Джонс К. Д., Шема М., Джонсон Б. С.	Инструментальные средства обеспечения безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 914 с.	2227-8397, http://www.iprbookshop.ru/73679.html
Л1.9	Петров А. А.	Компьютерная безопасность. Криптографические методы защиты	Саратов: Профобразование, 2019, 446 с.	978-5-4488-0091-7, http://www.iprbookshop.ru/87998.html

6.1.2. Дополнительная литература

№	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, http://www.iprbookshop.ru/61498.html
Л2.2	Бондаренко И. С., Демчишин Ю. В.	Методы и средства защиты информации : лабораторный практикум	Москва: Издательский Дом МИСиС, 2018, 32 с.	2227-8397, http://www.iprbookshop.ru/84413.html
Л2.3	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, http://www.iprbookshop.ru/61743.html
Л2.4	Тебуева Ф. Б., Антонов В. О.	Теоретико-числовые методы в криптографии : учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2017, 107 с.	2227-8397, http://www.iprbookshop.ru/75601.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.5	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, http://www.iprbookshop.ru/79313.html
Л2.6	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html
Л2.7	Котов Ю. А.	Криптографические методы защиты информации. Шифры : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2016, 59 с.	978-5-7782-2959-4, http://www.iprbookshop.ru/91377.html
Л2.8	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, http://www.iprbookshop.ru/61738.html
Л2.9	Пашинцев В. П., Ляхов А. В.	Нестандартные методы защиты информации : лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2016, 196 с.	2227-8397, http://www.iprbookshop.ru/63217.html
Л2.10	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, http://www.iprbookshop.ru/70020.html
6.1.3. Методические разработки				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Паротькин Н. Ю., Селигеев С. С., Кустов Н. Д.	Информационная безопасность сред виртуализации: Лабораторный практикум	Красноярск: СибГУ им. академика М. Ф. Решетнёва, 2025, 80 с.	https://e.lanbook.com/book/513704
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	Официальный интернет портал РГРТУ [электронный ресурс] http://www.rsreu.ru			
Э2	Образовательный портал РГРТУ [электронный ресурс]. - Режим доступа: по паролю.- https://edu.rsreu.ru			
Э3	Электронная библиотека РГРТУ [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - по паролю. - http://elib.rsreu.ru/			
Э4	Электронно-библиотечная система IRPbooks [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - свободный, доступ из сети интернет- по паролю. - https://www.iprbookshop.ru/			

Э5	Электронно-библиотечная система «Лань» [электронный ресурс]. - Режим доступа: доступ из корпоративной сети РГРТУ - свободный, доступ из сети интернет- по паролю. - https://e.lanbook.com
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

6.3.2 Перечень информационных справочных систем

6.3.2.1	Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.)
6.3.2.2	Система КонсультантПлюс http://www.consultant.ru
6.3.2.3	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	254 учебно-административный корпус . Учебная аудитория кафедры АСУ для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 64 места, 1 проектор, 1 экран, 1 компьютер, специализированная мебель, маркерная доска
2	127 учебно-административный корпус. Учебная аудитория для проведения практических занятий, лабораторных работ 25 ПК Intel Pentium CPU G620, 2.6GHz, 4Gb ОЗУ, HDD 500Gb
3	118 учебно-административный корпус. Учебная аудитория для проведения практических занятий, лабораторных работ 21 ПК Intel Pentium CPU G620, 2.6GHz, 4Gb ОЗУ, HDD 500Gb

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	**ФГБОУ ВО "РГРТУ", РГРТУ,** Холопов Сергей Иванович, Заведующий кафедрой АСУ	**03.09.26** 13:47 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Бабаян Павел Вартанович, Заведующий кафедрой АИТУ	**04.09.26** 13:22 (MSK)	Простая подпись