

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

Защита информации в СПР
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Телекоммуникаций и основ радиотехники**

Учебный план 11.03.02_26_00.plx
11.03.02 Инфокоммуникационные технологии и системы связи

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
Неделя	16			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
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., *Никишкин Павел Борисович*

Рабочая программа дисциплины

Защита информации в СПР

разработана в соответствии с ФГОС ВО:

ФГОС ВО - бакалавриат по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
(приказ Минобрнауки России от 19.09.2017 г. № 930)

составлена на основании учебного плана:

11.03.02 Инфокоммуникационные технологии и системы связи

утвержденного учёным советом вуза от 24.04.2026 протокол № 10.

Рабочая программа одобрена на заседании кафедры

Телекоммуникаций и основ радиотехники

Протокол от 02.04.2026 г. № 3

Срок действия программы: 2026-2030 уч.г.

Зав. кафедрой Витязев Владимир Викторович

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2027-2028 учебном году на заседании кафедры
Телекоммуникаций и основ радиотехники

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
Телекоммуникаций и основ радиотехники

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
Телекоммуникаций и основ радиотехники

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

Телекоммуникаций и основ радиотехники

Протокол от ____ 2030 г. № ____

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Целью освоения дисциплины являются формирование у студентов знаний по основам инженерно-технической защиты информации в системах подвижной радиосвязи, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учётом требований системного подхода.
1.2	Основные задачи освоения учебной дисциплины:
1.3	1. ознакомление студентов с информационной безопасностью;
1.4	2. обучение теоретическим и физическим основам инженерно-технической защиты применительно к системам подвижной радиосвязи, принципам и основам построения мобильных систем телекоммуникаций, методам и техническим средствам преобразования, обработки и защиты информации в современных системах телекоммуникаций;
1.5	3. ознакомление с основами правового регулирования и стандартизации вопросов обеспечения информационной безопасности телекоммуникационных систем, с основными существующими в настоящее время средствами и механизмами защиты, которые могут быть использованы при создании систем обеспечения информационной безопасности систем подвижной радиосвязи;
1.6	4. обучение основным методам, способам и принципам оценки эффективности средств обеспечения информационной безопасности систем подвижной радиосвязи.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:		Б1.В.ДВ.01
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	Основы цифровой модуляции и кодирования	
2.1.2	Технологическая (проектно-технологическая) практика	
2.1.3	Современные методы кодирования и модуляции	
2.1.4	Цифровая обработка сигналов	
2.1.5	Электромагнитные поля и волны	
2.1.6	Основы программирования микропроцессорной техники	
2.1.7	Вычислительная техника и информационные технологии	
2.1.8	Интеллектуальные сети	
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Выполнение и защита выпускной квалификационной работы	
2.2.2	Преддипломная практика	
2.2.3	УИР	
2.2.4	Преддипломный курс	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**ПК-2: Способен разрабатывать схемы организации связи телекоммуникационной системы****ПК-2.3. Обосновывает выбор информационных технологий, предварительных технических решений по цифровой системе связи, компонентам, оборудования и программного обеспечения****Знать**

Требования ЭМС

Уметь

Оптимизировать использование ресурсов сети радиодоступа с учётом требований ЭМС

Владеть

Методами и средствами оптимизации использования ресурсов сети радиодоступа с учётом требований ЭМС

В результате освоения дисциплины (модуля) обучающийся должен

3.1	Знать:
3.1.1	- виды ресурсов и ограничений для решения профессиональных задач;
3.1.2	- основные методы оценки разных способов решения задач;
3.1.3	- действующее законодательство и правовые нормы, регулирующие профессиональную деятельность;
3.1.4	- принципы построения и работы сетей связи и протоколов сигнализации, стандарты качества передачи данных, голоса и видео, применяемых в организации сети организации связи, Законодательство Российской Федерации в области связи, принципы работы и архитектура различных геоинформационных систем
3.2	Уметь:

3.2.1	- проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения;
3.2.2	- анализировать альтернативные варианты для достижения намеченных результатов;
3.2.3	- использовать нормативно-правовую документацию в сфере профессиональной деятельности;
3.2.4	- анализировать статистические параметры трафика, проводить расчет интерфейсов внутренних направлений сети, вырабатывать решения по оперативному переконфигурированию сети, изменению параметров коммутационной подсистемы, сетевых платформ и оборудования новых технологий; изменять параметры коммутационной подсистемы, маршрутизации трафика, прописки кодов маршрутизации, организации новых и расширении имеющихся направлений связи
3.2.5	- анализировать статистику основных показателей эффективности радиосистем и систем передачи данных, разрабатывать мероприятия по их поддержанию на требуемом уровне, выполнять расчет пропускной способности сетей телекоммуникаций
3.3	Владеть:
3.3.1	- методиками разработки цели и задач проекта;
3.3.2	- методами оценки потребности в ресурсах, продолжительности и стоимости проекта;
3.3.3	- навыками работы с нормативно-правовой документацией;
3.3.4	- навыками разработки схемы организации связи и интеграции новых сетевых элементов, построения и расширения коммутационной подсистемы и сетевых платформ, работой на коммутационном оборудовании по обеспечению реализации услуг, развертыванию оборудования сервисных платформ, оборудования новых технологий на сети, выполнению планов по расширению существующего оборудования сетевых платформ и новых технологий;
3.3.5	- навыками сопровождения геоинформационных баз данных по сети радиодоступа, информационной поддержки расчетов радиопокрытия, радиорелейных и спутниковых трасс и частотно-территориального планирования в части использования картографической информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Форма контроля
	Раздел 1. Защита информации в СПР					
1.1	Проблема защиты информации в телекоммуникационных системах. Анализ основных угроз /Тема/	7	0			
1.2	Проблема защиты информации в телекоммуникационных системах. Анализ основных угроз /Лек/	7	2	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.3	Проблема защиты информации в телекоммуникационных системах. Анализ основных угроз /Пр/	7	2	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы

1.4	Проблема защиты информации в телекоммуникационных системах. Анализ основных угроз /Ср/	7	6	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.5	Криптографические методы защиты информации /Тема/	7	0			
1.6	Криптографические методы защиты информации /Лек/	7	6	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.7	Криптографические методы защиты информации /Пр/	7	6	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.8	Криптографические методы защиты информации /Лаб/	7	8	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.9	Криптографические методы защиты информации /Ср/	7	13	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.10	Методы обеспечения подлинности пользователей и сообщений /Тема/	7	0			

1.11	Методы обеспечения подлинности пользователей и сообщений. /Лек/	7	3	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.12	Методы обеспечения подлинности пользователей и сообщений. /Пр/	7	3	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.13	Методы обеспечения подлинности пользователей и сообщений. /Лаб/	7	8	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.14	Методы обеспечения подлинности пользователей и сообщений. /Ср/	7	13	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.15	Обеспечение безопасности информации в мобильных системах телекоммуникаций /Тема/	7	0			
1.16	Обеспечение безопасности информации в мобильных системах телекоммуникаций /Лек/	7	3	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы

1.17	Обеспечение безопасности информации в мобильных системах телекоммуникаций /Пр/	7	3	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.18	Обеспечение безопасности информации в мобильных системах телекоммуникаций /Ср/	7	13	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.19	Практика сетевой защиты /Тема/	7	0			
1.20	Практика сетевой защиты /Лек/	7	2	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.21	Практика сетевой защиты. /Пр/	7	2	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.22	Практика сетевой защиты /Ср/	7	6	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.23	Зачёт с оценкой /Тема/	7	0			

1.24	Зачёт с оценкой /ИКР/	7	0,25	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы
1.25	Зачёт с оценкой /ЗаО/	7	8,75	ПК-2.3-3 ПК-2.3-У ПК-2.3-В	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Л3.6 Э1 Э2 Э3	Контрольные вопросы

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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

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	Басалова Г. В.	Основы криптографии : учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 282 с.	978-5-4497-0340-8, http://www.iprbookshop.ru/89455.html
Л1.2	Дмитриев В.Т.	Защита информации в инфокоммуникационных системах : учеб. пособие	Рязань, 2023, 148с.	978-5-7722-0371-2, 1
Л1.3	Дмитриев В.Т.	Защита информации в инфокоммуникационных системах : учеб. пособие	Рязань, 2023, 160с.	978-5-7722-0370-5, 1

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
---	---------------------	----------	-------------------	-----------------------------

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л2.1	Лапони́на О. Р.	Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016, 242 с.	5-9556-00020-5, http://www.iprbookshop.ru/52217.html
Л2.2	Макоева М.М., Шинаков Ю.С.	Системы связи с подвижными объектами : Учеб.пособие для вузов	М.:Радио и связь, 2002, 440с.	5-256-01562-1, 1
Л2.3	Сердюков П.Н., Бельчиков А.В., Дронов А.Е., Григорьев А.С., Волков С.С.	Защищенные радиосистемы цифровой передачи информации	М.:АСТ, 2006,	5-17-033739-6, 1
Л2.4	Шахнович И.В.	Современные технологии беспроводной связи	М.:Техносфера , 2006, 287с.	5-94836-070-9, 1
Л2.5	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019, 702 с.	978-5-4488-0070-2, http://www.iprbookshop.ru/87995.html
Л2.6	Петров А. А.	Компьютерная безопасность. Криптографические методы защиты	Саратов: Профобразование, 2019, 446 с.	978-5-4488-0091-7, http://www.iprbookshop.ru/87998.html
Л2.7	Герасименко В.А., Малюк А.А.	Основы защиты информации : Учебник для вузов	М., 1997, 539с.	5-88852-010-1, 1
Л2.8	Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.	Защита информации в компьютерных системах и сетях	М.:Радио и связь, 1999, 328с.	5-256-01436-6, 1
Л2.9	Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю.	Теоретические основы компьютерной безопасности : Учеб.пособие для вузов	М.:Радио и связь, 2000, 192с.	5-256-01413-7, 1
Л2.10	Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.	Основы криптографии : Учеб.пособие	М.:Гелиос АРВ, 2001, 479с.	5-85438-019-6, 1
Л2.11	Петраков А.В.	Основы практической защиты информации : Учеб.пособие	М.:Радио и связь, 2001, 361с.	5-256-01598-2, 1
Л2.12	Петраков А.В., Лагутин В.С.	Защита абонентского телетрафика	М.:Радио и связь, 2002, 499с.	5-256-01625-3, 1

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
ЛЗ.1	Швечкова О.Г., Москвитина О.А.	Алгоритмы электронной цифровой подписи. Схема Эль-Гамала : Методические указания	Рязань: РИЦ РГРТУ, 2013,	, https://elib.rsre.ru/ebs/download/1031
ЛЗ.2	Кащеев А.А., Дмитриев В.Т.	Основы криптографии : Методические указания	Рязань: РИЦ РГРТУ, 2010,	, https://elib.rsre.ru/ebs/download/1749
ЛЗ.3	Гусинская Г.В., Гусинская Е.И., Власенков В.В., Саутина А.Ю., Кащеев А.А.	Защита информации в системах подвижной радиосвязи : Методические указания	Рязань: РИЦ РГРТУ, 2010,	, https://elib.rsre.ru/ebs/download/2193
ЛЗ.4	Гусинская Г.В., Гусинская Е.И., Власенков В.В., Саутина А.Ю., Кащеев А.А.	Защита информации в системах подвижной радиосвязи : метод. указ. к лаб. работам	Рязань, 2010, 88с.	, 1
ЛЗ.5	Швечкова О.Г., Москвитина О.А.	Алгоритмы электронной цифровой подписи. Схема ГОСТ Р 34.10-2001 : метод. указ. к лаб. работам	Рязань, 2013, 16с.	, 1
ЛЗ.6	Швечкова О.Г., Москвитина О.А.	Алгоритмы электронной цифровой подписи. Схема DSA : метод. указ. к лаб. работам	Рязань, 2013, 16с.	, 1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронно-библиотечная система (ЭБС) РГРТУ(вход с сайта РГРТУ).
Э2	Электронно-библиотечная система (ЭБС) "Лань"(вход с сайта РГРТУ).
Э3	Электронно-библиотечная система IPRbooks.

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
MATLAB	Коммерческая лицензия
Simulink	Коммерческая лицензия
Communications Blockset (Transitioned)	Коммерческая лицензия
Communications System Toolbox	Коммерческая лицензия
DSP System Toolbox	Коммерческая лицензия
Filter Design Toolbox (Transitioned)	Коммерческая лицензия
Fixed-Point Designer	Коммерческая лицензия
Signal Processing Toolbox	Коммерческая лицензия

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	423 учебно-административный корпус. Учебная аудитория для проведения учебных занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Специализированная мебель (80 мест), 1 мультимедиа проектор, 1 экран, 1 компьютер, доска
2	422 учебно-административный корпус. Учебная аудитория для проведения учебных занятий лекционного и семинарского типа, лабораторных работ, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Специализированная мебель (30 посадочных мест), стенды для проведения лабораторных работ, магнитно-маркерная доска, экран. Мультимедиа проектор (Epson), 1 экран. ПК: Intel Core i5 8400/8Gb – 1 шт. ПК: Core i5 3470/4Gb – 10 шт. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ «Методические указания дисциплины «Защита информации в СПР»»).

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО
ЗАВЕДУЮЩИМ
КАФЕДРЫ**ФГБОУ ВО "РГРТУ", РГРТУ**, Витязев Владимир
Викторович, Заведующий кафедрой ТОР**19.06.26** 16:02 (MSK)

Простая подпись

ПОДПИСАНО
ЗАВЕДУЮЩИМ
ВЫПУСКАЮЩЕЙ
КАФЕДРЫ**ФГБОУ ВО "РГРТУ", РГРТУ**, Витязев Владимир
Викторович, Заведующий кафедрой ТОР**19.06.26** 16:02 (MSK)

Простая подпись