

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

Управление информационной безопасностью
рабочая программа дисциплины (модуля)

Закреплена за кафедрой

Информационной безопасности

Учебный план

10.05.01_25_00.plx

10.05.01_Информационная безопасность

Квалификация

специалист по защите информации

Форма обучения

очная

Общая трудоемкость

2 ЗЕТ

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	5 (3.1)		Итого	
Неделя	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	32,25	32,25	32,25	32,25
Контактная работа	32,25	32,25	32,25	32,25
Сам. работа	31	31	31	31
Часы на контроль	8,75	8,75	8,75	8,75
Итого	72	72	72	72

г. Рязань

Программу составил(и):

к.т.н., доцент, Кузьмин Юрий Михайлович

Рабочая программа дисциплины

Управление информационной безопасностью

разработана в соответствии с ФГОС ВО:

ФГОС ВО - специалитет по специальности 10.05.01 Компьютерная безопасность (приказ Минобрнауки России от 26.11.2020 г. № 1459)

составлена на основании учебного плана:

10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

утвержденного учёным советом вуза от 28.02.2025 протокол № 8.

Рабочая программа одобрена на заседании кафедры

Информационной безопасности

Протокол от 17.06.2025 г. № 12

Срок действия программы: 2025-2031 уч.г.

Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2026-2027 учебном году на заседании кафедры
Информационной безопасности

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
Информационной безопасности

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
Информационной безопасности

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
Информационной безопасности

Протокол от ____ 2029 г. № ____

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью дисциплины является получение обучающимися знаний, формирование у них умений и навыков, необходимых при разработке политик безопасности организации и администрирования систем обеспечения информационной безопасности для решения задач в профессиональной деятельности..
1.2	Задачами дисциплины являются:
1.3	– получение знаний об основных уязвимостях и угрозах безопасности информации, моделях угроз и нарушителя в автоматизированных системах, принципах формирования политики информационной безопасности в автоматизированных системах; рисках информационной безопасности в автоматизированных системах; методах и мерах по управлению информационной безопасностью в автоматизированных системах и оценке эффективности принятых мер;
1.4	– приобретение умения выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; проводить мониторинг угроз безопасности автоматизированных систем; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать корпоративную и частные политики информационной безопасности автоматизированных систем; оценивать информационные риски в автоматизированных системах; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
1.5	– приобретение практических навыков управления информационной безопасностью автоматизированных систем; разработки политик информационной безопасности, анализа информационной инфраструктуры автоматизированной системы и степени ее текущей безопасности, участия в экспертизе состояния защищенности информации на объекте защиты; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	ФТД.О
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Правовое регулирование в сфере информационно-коммуникационных технологий
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Государственные стандарты по защите информации
2.2.2	Нормативное обеспечение информационной безопасности компьютерных систем
2.2.3	Спецдисциплина 3
2.2.4	Информационная безопасность компьютерных систем объектов информатизации
2.2.5	Проектирование защищенных компьютерных сетей
2.2.6	Защита государственной тайны в Российской Федерации
2.2.7	Практика по получению профессиональных умений и опыта профессиональной деятельности
2.2.8	Производственная практика
2.2.9	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.10	Преддипломная практика
3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	
ОПК-5.5. Контролирует работы по выполнению режима защиты информации, в том числе ограниченного доступа	
Знать Содержание работ по выполнению режима защиты информации, в том числе ограниченного доступа	
Уметь Контролировать работы по выполнению режима защиты информации, в том числе ограниченного доступа	
Владеть Навыками контроля работ по выполнению режима защиты информации, в том числе ограниченного доступа	
В результате освоения дисциплины (модуля) обучающийся должен	
3.1	Знать:
3.1.1	Содержание работ по выполнению режима защиты информации, в том числе ограниченного доступа

3.2	Уметь:					
3.2.1	Контролировать работы по выполнению режима защиты информации, в том числе ограниченного доступа					
3.3	Владеть:					
3.3.1	Навыками контроля работ по выполнению режима защиты информации, в том числе ограниченного доступа					
4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Форма контроля
	Раздел 1. Введение в дисциплину. Базовая терминология					
1.1	/Тема/	5	0			
1.2	Цели, задачи, содержание дисциплины, планируемые результаты обучения по дисциплине. Система. Системный подход. Процесс. Процессный подход. Управление. Циклическая модель улучшения процессов. Системный подход к управлению организацией. Процессный подход к управлению организацией. Информационная безопасность. /Лек/	5	4	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
1.3	Изучение литературы и конспекта лекций. /Ср/	5	3	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 2. Стандартизация систем и процессов УИБ					
2.1	/Тема/	5	0			

2.2	Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ: ISO/IEC 13335 - методы и средства обеспечения безопасности информационных технологий, ISO/IEC 15408 и ISO/IEC 18045 - Общие критерии и методология оценки безопасности информационных технологий, ISO 19011:2018 и ГОСТ Р ИСО 19011-2012 - Рекомендации по аудиту систем менеджмента, BS 25999 и ГОСТ Р 53647 - Управление непрерывностью бизнеса. Законы о Банке России - Федеральный закон от 10 июля 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" и Федеральный закон от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе». ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (уровни защиты). ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия (оценка соответствия уровней защиты). Отраслевые стандарты в области управления ИБ - стандарты Банка России, рекомендации Банка России и положения Банка России по защите информации. /Лек/	5	4	ОПК-5.5-3 ОПК-5.5-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
2.3	Изучение литературы и конспекта лекций. /Ср/	5	4	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 3. Политика информационной безопасности					
3.1	/Тема/	5	0			
3.2	Понятия политики обеспечения ИБ и политики ИБ организации. Причины выработки политики ИБ. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ. Содержание политики ИБ: содержание корпоративной политики ИБ, содержание частных политик ИБ, примеры частных политик ИБ. Жизненный цикл политики ИБ: разработка политики ИБ, внедрение политики ИБ, применение политики ИБ, аннулирование политики ИБ, ответственность за исполнение политики ИБ. /Лек/	5	4	ОПК-5.5-3 ОПК-5.5-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

3.3	Изучение литературы и конспекта лекций. /Ср/	5	4	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 4. Управление и система управления информационной безопасностью					
4.1	/Тема/	5	0			
4.2	Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ организации как процесс. Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации. Система управления ИБ организации: область действия СУИБ, документальное обеспечение СУИБ, политика СУИБ, поддержка СУИБ со стороны руководства организации. Процессный подход в рамках управления ИБ: планирование СУИБ, реализация СУИБ, проверка СУИБ, совершенствование СУИБ. Работа с процессами СУИБ организации: задание процесса СУИБ, идентификация процессов СУИБ организации, документирование и описание процесса СУИБ, мониторинг и измерение параметров процесса СУИБ. Стратегии построения и внедрения СУИБ: построение и внедрение СУИБ в целом, построение и внедрение процессов СУИБ по отдельности. /Лек/	5	5	ОПК-5.5-3 ОПК-5.5-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
4.3	Изучение литературы и конспекта лекций. /Ср/	5	5	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 5. Оценка и управление рисками информационной безопасности					
5.1	/Тема/	5	0			
5.2	Основные определения. Нормативное обеспечение управления рисками информационной безопасности. Оценка рисков информационной безопасности. Обработка рисков информационной безопасности. Принятие и мониторинг рисков информационной безопасности. Обеспечение управления рисками информационной безопасности. /Лек/	5	5	ОПК-5.5-3 ОПК-5.5-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

5.3	Изучение литературы и конспекта лекций. /Ср/	5	5	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 6. Управление инцидентами ИБ и обеспечение непрерывности бизнеса					
6.1	/Тема/	5	0			
6.2	Нормативная база управления инцидентами ИБ и обеспечение непрерывности бизнеса. Стандарт ISO 27035. Идентификация, протоколирование, реагирование на инциденты ИБ. Влияние инцидентов ИБ на бизнес-процессы. Средства управления событиями ИБ. SOC-центры ИБ, SIEM-системы управления информацией о безопасности и событиями информационной безопасности, IRP-системы автоматизации реагирования на инциденты информационной безопасности. Управление непрерывностью бизнеса организации. /Лек/	5	5	ОПК-5.5-3 ОПК-5.5-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
6.3	Изучение литературы и конспекта лекций. /Ср/	5	5	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 7. Процессы проверки системы управления ИБ и оценка деятельности по управлению ИБ					
7.1	/Тема/	5	0			
7.2	Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью. Аудит СУИБ. Процесс аудита. Внутренний и внешний аудит. Аудит первой, второй и третьей сторонами. Подготовка к выполнению аудита. Подготовка и представление отчетов в устной и письменной форме о результатах аудита. Принятие решений о необходимости соответствующих последующих аудиторских проверок. Оценка деятельности по управлению информационной безопасностью. /Лек/	5	5	ОПК-5.5-3 ОПК-5.5-У	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
7.3	Изучение литературы и конспекта лекций. /Ср/	5	5	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).

7.4	Сдача (прием) зачета /ИКР/	5	0,25	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Ответы на Контрольные вопросы Результаты решения задач. Ответы на дополнительны е вопросы. Результаты тестирования.
7.5	Подготовка к зачету /Зачёт/	5	8,75	ОПК-5.5-3 ОПК-5.5-У ОПК-5.5-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	Задачи к зачету. Билеты к зачету. Тесты к зачету.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы по данной дисциплине приведены в Приложении 1 к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Управление информационной безопасностью»)

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	Пелешенко В. С., Говорова С. В., Лапина М. А.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие	Ставрополь: Северо-Кавказ ский федеральный университет, 2017, 86 с.	2227-8397, http://www.iprbookshop.ru/69405.html
Л1.2	Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью». Выпуск 1	Москва: Горячая линия-Телеком , 2012, 244 с.	978-5-9912-0271-8, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5178
Л1.3	Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Серия «Вопросы управление информационной безопасностью». Выпуск 2	Москва: Горячая линия-Телеком , 2012, 130 с.	978-5-9912-0272-5, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5179
Л1.4	Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Серия «Вопросы управление информационной безопасностью». Выпуск 3	Москва: Горячая линия-Телеком , 2013, 170 с.	978-5-9912-0273-2, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5180
Л1.5	Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Серия «Вопросы управление информационной безопасностью». Выпуск 4	Москва: Горячая линия-Телеком , 2012, 214 с.	978-5-9912-0274-9, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5181

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л1.6	Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Серия «Вопросы управление информационной безопасностью». Выпуск 5	Москва: Горячая линия-Телеком, 2012, 166 с.	978-5-9912-0275-6, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5182
Л1.7	Капгер И. В., Шабуров А. С.	Управление информационной безопасностью : учебное пособие	Пермь: ПНИПУ, 2023, 91 с.	978-5-398-02866-9, https://e.lanbook.com/book/328889

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л2.1	Сычев Ю. Н.	Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие	Саратов: Вузовское образование, 2018, 195 с.	978-5-4487-0128-3, http://www.iprbookshop.ru/72345.html

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/название ЭБС
Л3.1	Лапина М. А., Марков Д. М., Гиш Т. А., Песков М. В., Меденец В. В.	Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2016, 242 с.	2227-8397, http://www.iprbookshop.ru/62945.html

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	1. Электронно-библиотечная система «Лань». – Режим доступа: доступ из корпоративной сети РГПТУ – свободный (без пароля). URL: https://e.lanbook.com/
Э2	2. Электронно-библиотечная система «IPRbooks». – Режим доступа: доступ из корпоративной сети РГПТУ – свободный (без пароля), доступ из сети Интернет - по паролю. URL: https://iprbookshop.ru/
Э3	3. Электронная библиотека РГПТУ. URL: http://elib.rsreu.ru/ . Режим доступа: из корпоративной сети РГПТУ – по паролю
Э4	4. Научная электронная библиотека eLibrary. URL: http://e.lib/vlsu.ru/www.uisrussia.msu.ru/elibrary.ru
Э5	5. Библиотека и форум по программированию. URL: http://www.cyberforum.ru
Э6	6. Национальный открытый университет ИНТУИТ. URL: http://www.intuit.ru/

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
VMware Player	Свободное ПО

6.3.2 Перечень информационных справочных систем

6.3.2.1	Система КонсультантПлюс http://www.consultant.ru
---------	---

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	270 учебно-административный корпус. учебная аудитория для проведения учебных занятий. Специализированная мебель (42 посадочных места), магнитно-маркерная доска. Мультимедиа проектор, 1 экран. Рабочее место (2 стола), 1 персональный компьютер, 1 ноутбук.
---	---

2	268 учебно-административный корпус. компьютерный класс для проведения учебных занятий Специализированная мебель (20 компьютерных столов), 20 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.
8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)	
Методические материалы по данной дисциплине приведены в Приложении 2 к рабочей программе дисциплины (см. документ «Методическое обеспечение дисциплины «Управление информационной безопасностью»).	

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО
ЗАВЕДУЮЩИМ
КАФЕДРЫ**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор
Николаевич, Преподаватель**18.06.25** 20:52 (MSK)

Простая подпись

ПОДПИСАНО
ЗАВЕДУЮЩИМ
ВЫПУСКАЮЩЕЙ
КАФЕДРЫ**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор
Николаевич, Преподаватель**18.06.25** 20:52 (MSK)

Простая подпись