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 кафедрой

УТВЕРЖДАЮ

ПРОИЗВОДСТВЕННАЯ ПРАКТИКАПрактика по получению профессиональных умений и опыта профессиональной деятельности

рабочая программа

Закреплена за кафедрой **Информационной безопасности**
Учебный план 10.05.03_24_00.plx
10.05.03 - ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ

Квалификация **специалист по защите информации**
Форма обучения **очная**
Общая трудоемкость **6 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель				
Вид занятий	УП	РП	УП	РП
Контактная внеаудиторная работа	120	120	120	120
Иная контактная работа	0,25	0,25	0,25	0,25
Консультирование перед экзаменом и практикой	2	2	2	2
В том числе в форме практ.подготовки	207	207	207	207
Итого ауд.	2,25	2,25	2,25	2,25
Контактная работа	122,25	122,25	122,25	122,25
Часы на контроль	8,75	8,75	8,75	8,75
Иные формы работы	85	85	85	85
Итого	216	216	216	216

г. Рязань

Программу составил(и):
к.т.н., доц., Кузьмин Ю.М.

Рабочая программа
Практика по получению профессиональных умений и опыта профессиональной деятельности
разработана в соответствии с ФГОС ВО:
ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)
составлена на основании учебного плана:
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
утвержденного учёным советом вуза от 26.01.2024 протокол № 8.

Рабочая программа одобрена на заседании кафедры
Информационной безопасности
Протокол от 17.06.2024 г. № 12
Срок действия программы: 2024-2030 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Информационной безопасности

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
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 _____

1. ЦЕЛИ ОСВОЕНИЯ ПРАКТИКИ	
1.1	Цель дисциплины:
1.2	Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)проводится с целью получения обучающимися профессиональных умений и опыта профессиональной деятельности через непосредственное участие обучающихся в деятельности научно-производственного предприятия или с использованием материально-технической базы кафедры «Информационная безопасность» ФГБОУ ВО «РГРТУ».
1.3	
1.4	Задачи дисицплины:
1.5	- закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин общепрофессионального цикла и дисциплин специализации;
1.6	- практическое изучение и анализ нормативно-правовых документов, регламентирующих деятельность по защите информации в организации - месте проведения практики;
1.7	- закрепление навыков владения методами сбора и анализа исходных данных, необходимых для оценки уровня защищенности объектов защиты;
1.8	- закрепление у обучающихся умений и навыков разработки политики информационной безопасности организации;
1.9	- закрепление и расширение практических умений и навыков по выбору инструментальных средств, применяемых для построения системы защиты информации;
1.10	- получение и закрепление обучающимися практических умений и навыков работы с различными средства защиты информации, применяемыми для построения системы защиты информации объектов различной категории;
1.11	- формирование и закрепление умений и навыков комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;
1.12	- закрепление навыков использования различных источников информации и систем аудита для оценки эффективности применяемых мер обеспечения защиты информации;
1.13	- приобретение обучающимися профессиональных умений и навыков работы в рамках будущей профессиональной деятельности;
1.14	- развитие способностей обучающихся к самостоятельной деятельности в профессиональной сфере, самоорганизации и самоконтролю.
2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.О.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Разработка и эксплуатация автоматизированных систем в защищенном исполнении
2.1.2	Управление информационной безопасностью
2.1.3	Информационная безопасность автоматизированных систем
2.1.4	Компьютерные сети
2.1.5	Методы и средства криптографической защиты информации
2.1.6	Модели безопасности компьютерных систем
2.1.7	Спецдисциплина 1
2.1.8	Модели безопасности автоматизированных систем
2.1.9	Моделирование
2.1.10	Спецдисциплина 3
2.1.11	Государственные стандарты по защите информации
2.1.12	Нормативное обеспечение информационной безопасности компьютерных систем
2.1.13	Средства криптографической защиты информации
2.1.14	Правовое регулирование в сфере информационно-коммуникационных технологий
2.1.15	Информатика
2.1.16	Нормативное обеспечение информационной безопасности компьютерных систем
2.1.17	Нормативное обеспечение информационной безопасности компьютерных систем
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.2	Преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ

ОПК-2: Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-2.1. Анализирует информационную инфраструктуру объектов профессиональной деятельности

Знать
современные информационные технологии (операционные системы, базы данных, вычислительные сети)
виды и категории защищаемой информации
Уметь
проводить анализ угроз безопасности информации на объекте информатизации
Владеть
навыками работы с документацией на предприятии
навыками анализа технической документации объектов профессиональной деятельности

ОПК-2.2. Выбирает основные защитные механизмы и средства обеспечения информационной безопасности объектов профессиональной деятельности

Знать
технические возможности систем защиты информации
Уметь
проводить сравнение и подбор систем защиты инфор-мации
определять требования по защите информации в компьютерных системах
Владеть
навыками работы с научно-технической литературой в области информационных технологий и защиты информации

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ОПК-5.2. Использует нормативные и методические документы для определения требований о защите информации в компьютерных системах

Знать
руководящие и методические документы по разработке моделей угроз и нарушителей информационной безопасности
Уметь
разрабатывать и представлять модели (в том числе формальные) политик безопасности
Владеть
навыками использования современных информационных технологий в деятельности по ЗИ
методикой оценки требований по защите информации в компьютерных системах

ОПК-5.4. Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Знать
локальные нормативные правовые акты, действующие в организации
Уметь
классифицировать и категорировать защищаемую информацию
Владеть
навыками применения нормативных правовых актов в деятельность по защите информации
навыками категорирования защищаемой информации

ОПК-8: Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;

ОПК-8.5. Разрабатывает проектные решения по защите информации в автоматизированных системах, используя методы научных исследований

Знать
методогогию и методы научных исследований
организацию и порядок проведения научно – исследовательских работ
Уметь
прменять методы научных исследований
определять цель научного исследования, задачи, решения которых необходимо для достижения цели, результаты решения этих формулировать выводы по результатам исследования
Владеть
навыками применения методов научных исследований

ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-10.3. Использует методы и средства криптографической защиты информации при решении задач профессиональной деятельности

Знать
общие принципы функционирования средств криптографической защиты информации
Уметь
использовать средства криптографической защиты при решении задач информационной безопасности
Владеть
навыками конфигурирования программно-аппаратных средств защиты информации в компьютерных сетях

ОПК-15: Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

ОПК-15.2. Выявляет угрозы безопасности автоматизированных систем в защищенном исполнении

Знать
источники угроз информационной безопасности в ком-пьютерных сетях и меры по их предотвращению
Уметь
анализировать угрозы безопасности информации в ком-пьютерных сетях
Владеть
навыками работы со сканерами уязвимостей
навыками анализа угроз безопасности информации на объекте информатизации

ОПК-8.1.: Способен обосновывать целесообразность создания автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации;

ОПК-8.1..1. Проводит анализ угроз информационной безопасности при создании и эксплуатации автоматизированной системы в защищенном исполнении

Знать
источники угроз информационной безопасности в ком-пьютерных сетях и меры по их предотвращению
Уметь
формировать перечень угроз безопасности информации, возникающим при эксплуатации объектов информатизации
Владеть
навыками реализации мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения

ОПК-8.2.: Способен обеспечивать и осуществлять разработку проектных и организационных решений, документирование системы защиты информации автоматизированной системы в защищенном исполнении;

ОПК-8.2..1. Готовит исходные данные и формирует требования к системе защиты информации автоматизированных систем в защищенном исполнении

Знать
содержание основных работ по созданию АСЗИ, проводимых на стадиях проектирования
Уметь
готовить исходные данные и формулировать требования к системе защиты информации автоматизированных систем в защищенном сиполнении
Владеть
навыками подготовки исходных данных и формулирования требований к системе защиты информации автоматизированных систем в защищенном сиполнении

ОПК-8.2..2. Осуществляет разработку проектных и организационных решений по системе защиты информации автоматизированных систем в защищенном исполнении

Знать
содержание основных работ по созданию АСЗИ, проводимых на стадиях проектирования
Уметь
разрабатывать типовые нормативные документы по оценке угроз информационной безопасности автоматизированных систем и их формальному представлению
разрабатывать АСЗИ на проектных стадиях, в том числе разрабатывать технические задания на составные части АСЗИ
Владеть
навыками работы с научно-технической литературой, нормативными и методическими документами в области создания объектов информатизации

В результате освоения практики обучающийся должен

3.1	**Знать:**
3.1.1	современные информационные технологии (операционные системы, базы данных, вычислительные сети)
3.1.2	технические возможности систем защиты информации
3.1.3	локальные нормативные правовые акты, действующие в организации
3.1.4	нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

3.1.5	основные документы, регламентирующие требования к системе защиты информации автоматизированных систем в защищенном исполнении
3.1.6	руководящие и методические документы по разработке моделей угроз и нарушителей информационной безопасности
3.1.7	виды и категории защищаемой информации
3.1.8	методогогию и методы научных исследований
3.1.9	организацию и порядок проведения научно – исследовательских работ
3.1.10	общие принципы функционирования средств криптографической защиты информации
3.1.11	источники угроз информационной безопасности в ком-пьютерных сетях и меры по их предотвращению
3.1.12	содержание основных работ по созданию АСЗИ, проводимых на стадиях проектирования
3.2	**Уметь:**
3.2.1	проводить анализ угроз безопасности информации на объекте информатизации
3.2.2	проводить сравнение и подбор систем защиты инфор-мации
3.2.3	определять требования по защите информации в компьютерных системах
3.2.4	разрабатывать и представлять модели (в том числе формальные) политик безопасности
3.2.5	классифицировать и категорировать защищаемую информацию
3.2.6	прменять методы научных исследований
3.2.7	определять цель научного исследования, задачи, решения которых необходимо для достижения цели, результаты решения этих формулировать выводы по результатам исследования
3.2.8	использовать средства криптографической защиты при решении задач информационной безопасности
3.2.9	анализировать угрозы безопасности информации в ком-пьютерных сетях
3.2.10	формировать перечень угроз безопасности информации, возникающим при эксплуатации объектов информатизации
3.2.11	готовить исходные данные и формулировать требования к системе защиты информации автоматизированных систем в защищенном сиполнении
3.2.12	разрабатывать типовые нормативные документы по оценке угроз информационной безопасности автоматизированных систем и их формальному представлению
3.2.13	разрабатывать АСЗИ на проектных стадиях, в том числе разрабатывать технические задания на составные части АСЗИ
3.3	**Владеть:**
3.3.1	навыками анализа угроз безопасности информации на объекте информатизации
3.3.2	навыками анализа технической документации объектов профессиональной деятельности
3.3.3	методикой оценки требований по защите информации в компьютерных системах
3.3.4	навыками работы с документацией на предприятии
3.3.5	навыками использования современных информационных технологий в деятельности по ЗИ
3.3.6	навыками применения нормативных правовых актов в деятельность по защите информации
3.3.7	навыками категорирования защищаемой информации
3.3.8	навыками применения методов научных исследований
3.3.9	навыками работы с научно-технической литературой в области информационных технологий и защиты информации
3.3.10	навыками конфигурирования программно-аппаратных средств защиты информации в компьютерных сетях
3.3.11	навыками работы со сканерами уязвимостей
3.3.12	навыками реализации мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения
3.3.13	навыками подготовки исходных данных и формулирования требований к системе защиты информации автоматизированных систем в защищенном сиполнении
3.3.14	навыками работы с научно-технической литературой, нормативными и методическими документами в области создания объектов информатизации

4. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1.					
1.1	Основной этап /Тема/	10	0			

1.2	1.1. Определение и закрепление за обучающимися профильных организаций для прохождения практики. 1.2. Заключение договоров (оформление заявок) на прохождение практики с профильными организациями. 1.3. Утверждение приказа на прохождение практики. 1.4. Общее собрание по вопросам организации практики, ознакомление их с программой практики. 1.5. Инструктаж обучающихся руководителем практики от выпускающей кафедры по содержанию, требованиям и порядку проведения практики. 1.6. Составление и согласование с профильной организацией рабочего графика (плана) и индивидуального задания на практику. 1.7. Выдача обучающимся индивидуальных заданий. /КВР/	10	20	ОПК-2.1-У ОПК-2.1-В ОПК-2.2-З ОПК-2.2-У ОПК-2.2-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-8.1..1-З ОПК-8.1..1-У ОПК-8.1..1-В ОПК-8.2..1-З ОПК-8.2..1-У ОПК-8.2..1-В ОПК-8.2..2-З ОПК-8.2..2-У ОПК-8.2..2-	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18 Л1.19 Л1.20 Л1.21 Л1.22 Л1.23 Л1.24 Л1.25Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11Л3.1 Л3.2 Э5	Опрос
	Раздел 2.					
2.1	Основной этап. Выполнение ин-дивидуального задания /Тема/	10	0			

2.2	2.1. Инструктаж в месте прохождения практики по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка и режиму безопасности. Обязательство выполнения требований студенты подтверждают росписью в соответствующих журналах. 2.2. Получение пропусков в профильную организацию. 2.3. Общее знакомство с организацией - местом проведения практики. /КВР/	10	100	ОПК-2.1-З ОПК-2.1-У ОПК-2.1-В ОПК-2.2-З ОПК-2.2-У ОПК-2.2-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-8.1..1-З ОПК-8.1..1-У ОПК-8.1..1-В ОПК-8.2..1-З ОПК-8.2..1-У ОПК-8.2..1-В ОПК-8.2..2-З ОПК-8.2..2-У ОПК-8.2..2-	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18 Л1.19 Л1.20 Л1.21 Л1.22 Л1.23 Л1.24 Л1.25Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11Л3.1 Л3.2 Э5	Опрос

2.3	2.4. Знакомство с нормативно-правовыми документами, регламентирующими деятельность в области защиты информации, в том числе в организации - месте проведения практики. 2.5. Изучение работы конкретных средств защиты информации, методов и способов организации систем защиты информации в организации - месте проведения практики. 2.6. Определение перечня защищаемой информации и потоков этой информации в организации - месте проведения практики. 2.7. Определение угроз информационной безопасности в организации - месте проведения практики. 2.8. Оценка уровня соответствия защитных мер и средств, используемых в организации - месте проведения практики, требованиям руководящих документов по защите информации. 2.9. Разработка выводов и рекомендаций по результатам оценки. /ИФР/	10	60	ОПК-2.1-З ОПК-2.1-У ОПК-2.1-В ОПК-2.2-З ОПК-2.2-У ОПК-2.2-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-8.1..1-З ОПК-8.1..1-У ОПК-8.1..1-В ОПК-8.2..1-З ОПК-8.2..1-У ОПК-8.2..1-В ОПК-8.2..2-З ОПК-8.2..2-У ОПК-8.2..2-	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18 Л1.19 Л1.20 Л1.21 Л1.22 Л1.23 Л1.24 Л1.25Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Отчет о выполнении задания
	Раздел 3.					
3.1	Заключительный этап /Тема/	10	0			

3.2	3.1 Оформление результатов практики в виде отчетной документации по практике, содержащей следующую информацию: - индивидуальное задание студенту руководителя практики от предприятия; - пояснительная записка (отчет по практике) по заданной теме; - общий отзыв руководителя практикой от предприятия о работе студента (с оценкой); - отзыв о качестве выполнения студентом программы практики со стороны руководителя практики от университета (с оценкой). 3.2 Подготовка презентационного материала и доклада по итогам практики. /ИФР/	10	25	ОПК-2.1-З ОПК-2.1-У ОПК-2.1-В ОПК-2.2-З ОПК-2.2-У ОПК-2.2-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-8.1..1-З ОПК-8.1..1-У ОПК-8.1..1-В ОПК-8.2..1-З ОПК-8.2..1-У ОПК-8.2..1-В ОПК-8.2..2-З ОПК-8.2..2-У ОПК-8.2..2-	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18 Л1.19 Л1.20 Л1.21 Л1.22 Л1.23 Л1.24 Л1.25Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11Л3.1 Л3.2 Э5	Отчет и презентация по итогам практики
	Раздел 4.					
4.1	Промежуточная аттестация /Тема/	10	0			

4.2	Прием зачета /ИКР/	10	0,25	ОПК-2.1-З ОПК-2.1-У ОПК-2.1-В ОПК-2.2-З ОПК-2.2-У ОПК-2.2-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-8.1..1-З ОПК-8.1..1-У ОПК-8.1..1-В ОПК-8.2..1-З ОПК-8.2..1-У ОПК-8.2..1-В ОПК-8.2..2-З ОПК-8.2..2-У ОПК-8.2..2-	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18 Л1.19 Л1.20 Л1.21 Л1.22 Л1.23 Л1.24 Л1.25Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11Л3.1 Л3.2 Э5	Опрос по отчетам и отзывам.

4.3	Консультация перед зачетом /Кнс/	10	2	ОПК-2.1-З ОПК-2.1-У ОПК-2.1-В ОПК-2.2-З ОПК-2.2-У ОПК-2.2-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-8.1..1-З ОПК-8.1..1-У ОПК-8.1..1-В ОПК-8.2..1-З ОПК-8.2..1-У ОПК-8.2..1-В ОПК-8.2..2-З ОПК-8.2..2-У ОПК-8.2..2-	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18 Л1.19 Л1.20 Л1.21 Л1.22 Л1.23 Л1.24 Л1.25Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11Л3.1 Л3.2 Э5	Опрос по результатам.

4.4	Подготовка к зачету /ЗаО/	10	8,75	ОПК-2.1-З ОПК-2.1-У ОПК-2.1-В ОПК-2.2-З ОПК-2.2-У ОПК-2.2-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-8.1..1-З ОПК-8.1..1-У ОПК-8.1..1-В ОПК-8.2..1-З ОПК-8.2..1-У ОПК-8.2..1-В ОПК-8.2..2-З ОПК-8.2..2-У ОПК-8.2..2-	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л1.14 Л1.15 Л1.16 Л1.17 Л1.18 Л1.19 Л1.20 Л1.21 Л1.22 Л1.23 Л1.24 Л1.25Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11Л3.1 Л3.2 Э5	Опрос. Сбор отчетов и отзывов. Анализ результатов.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРАКТИКИ

Оценочные материалы приведены в Приложении 1 к рабочей программе дисциплины (см. докумет "Оценочные материалы по дисциплине "Производственная практика").

Оценочные материалы приведены в Приложении 1 к рабочей программе дисциплины (см. докумет "Оценочные материалы по дисциплине "Производственная практика").

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

6.1. Рекомендуемая литература

6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.1	Громов Ю. Ю., Стародубов О. Г., Кадыков К. В.	Программно-аппаратные средства защиты информационных систем : учебное пособие	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2017, 193 с.	978-5-8265-1737-6, http://www.iprbookshop.ru/85968.html
Л1.2	Фомина К.Ю., Кураксин В.А.	Методы и средства обнаружения вторжений в компьютерные сети : метод. указ. к лаб. работам	Рязань, 2018, 48с.; прил.	60
Л1.3	Фомина К.Ю., Кураксин В.А.	Методы и средства защиты информации : метод. указ. к лаб. работам	Рязань, 2018, 48с.; прил.	60

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.4	Гулак, М. Л., Рытов, М. Ю., Голембиовская, О. М.	Аудит информационной безопасности. Прикладная статистика : учебное пособие	Москва: Ай Пи Ар Медиа, 2020, 121 с.	978-5-4497-0713-0, http://www.iprbookshop.ru/97630.html
Л1.5	Калинкина Т.И., Пржегорлинский В.Н.	Вычислительные сети : метод. указ. к курс. проекту	Рязань, 2012, 31с.	30
Л1.6	Пржегорлинский В.Н.	Элементарные объекты защиты информации : учеб. пособие	Рязань, 2012, 131с.	60
Л1.7	Пржегорлинский В.Н.	Комплексные объекты защиты информации. Условия защиты информации : учеб. пособие	Рязань, 2013, 87с.	60
Л1.8	Пржегорлинский В.Н., Бабаев С.И., Калинкина Т.И.	Основы сетевых технологий : учеб. пособие	Рязань, 2016, 95с.	60
Л1.9	Засорин С.В., Кузьмин Ю.М., Пржегорлинский В.Н.	Защита в операционных системах : метод. указ. к лаб.работам	Рязань, 2016, 76с.	60
Л1.10	Засорин С.В., Кузьмин Ю.М., Пржегорлинский В.Н.	Защита в операционных системах : метод. указ. к лаб. работам	Рязань, 2016, 44с.	60
Л1.11	Фомина К.Ю., Кураксин В.А.	Методы и средства обнаружения вторжений в компьютерные сети : метод. указ. к лаб. работам	Рязань, 2018, 48с.; прил.	60
Л1.12	Белоус А. И., Солодуха В. А., Шведов С. В., Белоуса А. И.	Программные и аппаратные трояны – способы внедрения и методы противодействия. Первая техническая энциклопедия. В 2-х книгах. К.1	Москва: Техносфера, 2019, 688 с.	978-5-94836-524-4, http://www.iprbookshop.ru/93378.html
Л1.13	Фомина К.Ю., Кураксин В.А.	Методы и средства защиты информации : метод. указ. к лаб. работам	Рязань, 2018, 48с.; прил.	60
Л1.14	Кузьмин Ю.М., Кураксин В.А., Пржегорлинский В.Н.	Программно-аппаратные средства обеспечения информационной безопасности : метод. указ. к лаб. работам	Рязань, 2018, 48с.	60
Л1.15	Калинкина Т.И., Кузьмин Ю.М., Пржегорлинский В.Н.	Основы построения защищенных баз данных : метод. указ. к лаб. работам	Рязань, 2019, 80с.	30
Л1.16	Конкин Ю.В., Кузьмин Ю.М., Пржегорлинский В.Н.	Основы информационной безопасности : учеб. пособие	Рязань, 2021, 96с.	30
Л1.17	Булычёв Г. Г.	Программно-аппаратные средства защиты информации. Часть 1	Москва: РТУ МИРЭА, 2022, 203 с.	978-5-7339-1652-1, https://e.lanbook.com/book/310781
Л1.18	Булычёв Г. Г.	Программно-аппаратные средства защиты информации. Часть 2	Москва: РТУ МИРЭА, 2022, 177 с.	978-5-7339-1653-8, https://e.lanbook.com/book/310784
Л1.19	Душкин А. В., Барсуков О. М., Кравцов Е. В., Славнов К. В.	Программно-аппаратные средства обеспечения информационной безопасности	Москва: Горячая линия-Телеком, 2018, 248 с.	978-5-9912-0470-5, https://e.lanbook.com/book/111053

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.20	Зайцев А. П., Мещеряков Р. В., Шелупанов А. А.	Технические средства и методы защиты информации	Москва: Горячая линия-Телеком, 2018, 442 с.	978-5-9912-0233-6, https://e.lanbook.com/book/111057
Л1.21	Калинкина Т.И., Пржегорлинский В.Н.	Криптографические методы защиты информации : Методические указания	Рязань: РИЦ РГРТУ, 2014,	, https://elib.rsreu.ru/ebs/download/787
Л1.22	Пржегорлинский В.Н.	Объекты защиты информации. Ч.2 Комплексные объекты защиты информации : Учебное пособие	Рязань: РИЦ РГРТУ, 2014,	, https://elib.rsreu.ru/ebs/download/937
Л1.23	Пржегорлинский В.Н.	Объекты защиты информации. Ч.1. Элементарные объекты защиты информации : Учебное пособие	Рязань: РИЦ РГРТУ, 2012,	, https://elib.rsreu.ru/ebs/download/938
Л1.24	Кузьмин Ю.М., Кураксин В.А., Пржегорлинский В.Н.	Программно-аппаратные средства обеспечения информационной безопасности : Методические указания	Рязань: РИЦ РГРТУ, 2018,	, https://elib.rsreu.ru/ebs/download/1883
Л1.25	Фомина К.Ю., Кураксин В.А.	Методы и средства обнаружения вторжений в компьютерные сети : Методические указания	Рязань: РИЦ РГРТУ, 2018,	, https://elib.rsreu.ru/ebs/download/1896

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В.	Аудит информационной безопасности органов исполнительной власти : учебное пособие	Брянск: Брянский государственный технический университет, 2012, 100 с.	978-89838-491-3, http://www.iprbookshop.ru/6992.html
Л2.2	Бубнов А.А., Бубнов С.А., Майков К.А.	Разработка и анализ требований к программному обеспечению: учебник : Учебник	Рязань: КУРС, 2020,	, https://elib.rsreu.ru/ebs/download/2678
Л2.3	Бубнов С.А., Бубнов А.А.	Работа с файловой системой LINUX : метод. указ. к лаб. работам	Рязань, 2019, 28с.	50
Л2.4	Назаров С. В., Белоусова С. Н., Бессонова И. А., Гиляревский Р. С., Гудыно Л. П., Егоров В. С., Исаев Д. В., Кириченко А. А., Кишкович Ю. П., Кравченко Т. К., Куприянов Д. В., Меликян А. В., Пятибратов А. П., Кирсанов А. П.	Введение в программные системы и их разработку : учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 649 с.	978-5-4497-0312-5, http://www.iprbookshop.ru/89429.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.5	Назаров С. В., Белоусова С. Н., Бессонова И. А., Гиляревский Р. С., Гудыно Л. П., Егоров В. С., Исаев Д. В., Кириченко А. А., Кирсанов А. П., Кишкович Ю. П., Кравченко Т. К., Куприянов Д. В., Меликян А. В., Пятибратов А. П.	Основы информационных технологий : учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, 530 с.	978-5-4497-0339-2, http://www.iprbookshop.ru/89454.html
Л2.6	Бубнов С.А., Бубнов А.А., Коротаев А.Н.	Основы работы в ОС семейства Linux : Методические указания	Рязань: РИЦ РГРТУ, 2018,	, https://elib.rsreu.ru/ebs/download/1836
Л2.7	Кузьмин Ю.М., Калинкина Т.И.	Защита программ и данных : метод. указ. к лаб. работам	Рязань, 2019, 65с.	60
Л2.8	Кузьмин Ю.М., Калинкина Т.И.	Защита программ и данных. Часть 2. Исследование программ динамическим методом: метод. указ. к лаб. работам : Методические указания	Рязань: РИЦ РГРТУ, 2020,	, https://elib.rsreu.ru/ebs/download/2638
Л2.9	Булычев Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности. Часть 2	Москва: РТУ МИРЭА, 2020, 46 с.	, https://e.lanbook.com/book/163812
Л2.10	Булычев Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности.Часть 1: Методические рекомендации	Москва: РТУ МИРЭА, 2020, 23 с.	, https://e.lanbook.com/book/163932
Л2.11	Бубнов А.А., Реутский К.А., Тишкина В.В.	Тестирование программного обеспечения: учебник : Учебник	Рязань: КУРС, 2019,	, https://elib.rsreu.ru/ebs/download/2679

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Костров Б.В., Саблина В.А., Ефимов А.И.	Методология научных исследований: методические указания к практическим занятиям : Методические указания	Рязань: РИЦ РГРТУ, 2020,	, https://elib.rsreu.ru/ebs/download/2449
Л3.2	Костров Б.В., Ефимов А.И., Громов А.Ю., Гринченко Н.Н.	Прохождение практики бакалаврами и специалистами: метод. указ. к прохождению учебной и производственной практик : Методические указания	Рязань: , 2020,	, https://elib.rsreu.ru/ebs/download/2877

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Информационные технологии в науке и образовании: Учебное пособие [Электронный ресурс] / Е.Л. Федотова, А.А. Федотов. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013
Э2	ГОСТ 7.32–2001. Отчёт о научно-исследовательской работе. Структура и правила оформления [Электронный ресурс]. – Введ. 2002-07-01.
Э3	Интернет-портал правовой информации, справочно-правовая система [Электронный ресурс].
Э4	Научная электронная библиотека eLIBRARY.RU
Э5	Интернет-портал ФСТЭК России

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

Kaspersky Endpoint Security	Коммерческая лицензия
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
VirtualBox	Свободное ПО
VMware Player	Свободное ПО
6.3.2 Перечень информационных справочных систем	
6.3.2.1	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru
6.3.2.2	Система КонсультантПлюс http://www.consultant.ru
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ	
1	218 учебно-административный корпус. лаборатория средств защиты информации для проведения учебных занятий Специализированная мебель (12 посадочных мест), 12 рабочих мест (7 компьютерных столов, 2 стола), 12 персональных компьютеров, магнитно-маркерная доска
2	266 учебно-административный корпус. лаборатория средств защиты информации для проведения учебных занятий Специализированная мебель (12 посадочных мест), 4 рабочих места (стол), магнитно-маркерная доска
3	266 а учебно-административный корпус. компьютерный класс для проведения учебных занятий, самостоятельной работы обучающихся Специализированная мебель (14 компьютерных столов), 14 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.
4	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.
5	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.
8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПРАКТИКЕ	
Методическое обеспечение дисциплины приведено в Приложении 2 к рабочей программе дисциплины (см. докумет "Методические указания дисциплины "Производственая практика").	