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 10.05.01 _24_00.plx
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):
ст. преп., Павлунин М.А.

Рабочая программа
Практика по получению профессиональных умений и опыта профессиональной деятельности
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 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	Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности) (далее - практика) проводится с целью получения обучающимися профессиональных умений и опыта профессиональной деятельности.
1.2	Для достижения указанной цели в процессе практики решаются следующие задачи:
1.3	- закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин общепрофессионального цикла и дисциплин специализации;
1.4	- практическое изучение и анализ нормативно-правовых документов, регламентирующих деятельность по защите информации в организации - месте проведения практики.
1.5	- закрепление навыков владения методами сбора и анализа исходных данных, необходимых для оценки уровня защищенности объектов защиты;
1.6	- закрепление у обучающихся умений и навыков разработки политики информационной безопасности организации;
1.7	- закрепление и расширение практических умений и навыков по выбору инструментальных средств, применяемых для построения системы защиты информации;
1.8	- получение и закрепление обучающимися практических умений и навыков работы с различными средства защиты информации, применяемыми для построения системы защиты информации объектов различной категории;
1.9	- формирование и закрепление умений и навыков комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;
1.10	- закрепление навыков использования различных источников информации и систем аудита для оценки эффективности применяемых мер обеспечения защиты информации;
1.11	- приобретение обучающимися профессиональных умений и навыков работы в рамках будущей профессиональной деятельности;
1.12	- развитие способностей обучающихся к самостоятельной деятельности в профессиональной сфере, самоорганизации и самоконтролю.
1.13	
1.14	
2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.О.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Криптографические протоколы
2.1.2	Проектирование защищенных компьютерных сетей
2.1.3	Информационная безопасность компьютерных систем объектов информатизации
2.1.4	Методы и средства криптографической защиты информации
2.1.5	Модели безопасности компьютерных систем
2.1.6	Спецдисциплина 1
2.1.7	Криптографические средства защиты информации
2.1.8	Моделирование
2.1.9	Спецдисциплина 3
2.1.10	Государственные стандарты по защите информации
2.1.11	Нормативное обеспечение информационной безопасности компьютерных систем
2.1.12	Управление информационной безопасностью
2.1.13	Правовое регулирование в сфере информационно-коммуникационных технологий
2.1.14	Информатика
2.1.15	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 (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- современные информационные технологии (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- современные информационные технологии (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- современные информационные технологии (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- современные информационные технологии (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- современные информационные технологии (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- современные информационные технологии (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- современные информационные технологии (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- современные информационные технологии (операци-онные системы, базы данных, вычислительные сети).
Уметь
- проводить анализ угроз безопасности информации на объекте информатизации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

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.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

Знать
- технические возможности систем защиты информации.
Уметь
- проводить сравнение и подбор систем защиты инфор-мации.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

Знать
- технические возможности систем защиты информации.
Уметь
- проводить сравнение и подбор систем защиты инфор-мации.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

Знать
- технические возможности систем защиты информации.
Уметь
- проводить сравнение и подбор систем защиты инфор-мации.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

Знать
- технические возможности систем защиты информации.
Уметь
- проводить сравнение и подбор систем защиты инфор-мации.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

Знать
- технические возможности систем защиты информации.
Уметь
- проводить сравнение и подбор систем защиты инфор-мации.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

Знать
- технические возможности систем защиты информации.
Уметь
- проводить сравнение и подбор систем защиты инфор-мации.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

Знать
- технические возможности систем защиты информации.
Уметь
- проводить сравнение и подбор систем защиты инфор-мации.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

Знать
- технические возможности систем защиты информации.
Уметь
- проводить сравнение и подбор систем защиты инфор-мации.
Владеть
- навыками анализа технической документации объектов профессиональной деятельности.

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
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- локальные нормативные правовые акты, действующие в организации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

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

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

Знать
- нормативные правовые акты, нормативные и методиче-ские документы, регламентирующие деятельность по за-щите информации.
Уметь
- определять требования по защите информации в ком-пьютерных системах.
Владеть

ОПК-8: Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ОПК-8.6. Разрабатывает и оценивает модели объектов исследования

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

Знать
- категории защищаемой информации.
Уметь
- разрабатывать модель объекта защиты информации.
Владеть
- навыками анализа угроз безопасности информации на объекте информатизации.

ОПК-10: Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-10.5. Использует методы и средства криптографической защиты информации при решении задач профессиональной деятельности

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

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

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

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

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

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

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

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

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

ОПК-16: Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

ОПК-16.2. Выявляет угрозы безопасности компьютерных систем и сетей

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.

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.

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.

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.

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.

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.

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.

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.

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.

В результате освоения практики обучающийся должен

3.1	**Знать:**
3.1.1	- современные информационные технологии (операци-онные 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 методиче-ские документы, регламентирующие деятельность по за-щите информации.
3.1.5	- категории защищаемой информации.
3.1.6	- общие принципы функционирования средств крипто-графической защиты информации.
3.1.7	- источники угроз информационной безопасности в ком-пьютерных сетях и меры по их предотвращению.
3.1.8	- источники угроз информационной безопасности в ком-пьютерных сетях и меры по их предотвращению.
3.1.9	- категории защищаемой информации;
3.1.10	- требования по защите информации, обрабатываемой в компьютерных системах объектов информатизации.
3.1.11	- программные (программно-технические) средства за-щиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее.
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 ком-пьютерных системах.
3.2.4	- определять требования по защите информации в ком-пьютерных системах.
3.2.5	- разрабатывать модель объекта защиты информации.
3.2.6	- использовать средства криптографической защиты при решении задач информационной безопасности.
3.2.7	- анализировать угрозы безопасности информации в ком-пьютерных сетях.
3.2.8	- формировать перечень угроз безопасности информации, возникающим при эксплуатации объектов информатизации.
3.2.9	- реализовывать требования по защите информации, об-рабатываемой в компьютерных системах объектов ин-форматизации

3.2.10	- разрабатывать проектные и организационные решения систем защиты информации компьютерных систем объ-ектов информатизации.
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 анализа угроз безопасности информации на объекте информатизации.
3.3.5	- навыками конфигурирования программно-аппаратных средств защиты информации в компьютерных сетях.
3.3.6	- навыками работы со сканерами уязвимостей.
3.3.7	- навыками реализации мероприятия по противодейст-вию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения.
3.3.8	- навыками разработки проектной документации защиты информации компьютерных систем 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. Организационный этап					
1.1	Организационный 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. Приказ о проведении производственной практики с распределением обучающихся по профильным организациям с закреплением руководителей от кафедры утверждается не позднее 10 дней до ее начала. Обучающиеся перед началом практики получают формы документов отчета по практике. При необходимости обучающиеся должны подготовить фотографии (формат по требованию предприятия-базы практики) и паспортные данные (ксерокопии разворотов с фотографией и регистрацией места жительства) для оформления пропусков на предприятия. 1.3.Инструктаж обучающихся руководителем практики от выпускающей кафедры по содержанию, требованиям и порядку проведения практики. На инструктаже проводится ознакомление обучающихся со следующими вопросами: - цели и задачи производственной практики; - разделы (этапы) и формы проведения практики; - информация о базовом предприятии, на котором будет прохождение практики; - информация о темах практики для получения профессиональных умений и опыта профессиональной деятельности; - структура и содержание отчёта по производственной практике; - требованиями, которые предъявляются к местам практики; - необходимая документация для заключения договора с предприятием о прохождении производственной практики; - используемая нормативно-техническая документация; - порядок оформления пропусков для допуска в профильную организацию. 1.4. Составление и согласование с профильной организацией рабочего графика (плана) и индивидуального задания на практику. /КВР/	10	20		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 Л1.19Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3	Опрос
	Раздел 2. Основной этап. Выполнение индивидуального задания.					
2.1	Основной этап. Выполнение индивидуального 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		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 Л1.19Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3	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		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 Л1.19Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3	Отчет о выполнении задания
	Раздел 3. Заключительный этап					
3.1	Заключительный этап /Тема/	10	0			
3.2	3.1 Оформление результатов практики в виде отчета по практике, содержащего следующие разделы: - место и время прохождения практики; - общие положения о прохождения практики; - дневник практики, содержащий: - календарный план работы студента, - дневник выполнения работ, - теоретические занятия на практике, - производственные экскурсии; - индивидуальное задание студенту руководителя практики от предприятия; - пояснительная записка 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		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 Л1.19Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3	Отчет и презентация по итогам практики
	Раздел 4. Промежуточная аттестация					
4.1	Промежуточная аттестация. /Тема/	10	0			

4.2	Прием зачета /ИКР/	10	0,25		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 Л1.19Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3	Опрос по отчетам и отзывам.
4.3	Консультация перед зачетом. /Кнс/	10	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 Л1.19Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3	Опрос по результатам.
4.4	Подготовка к зачету. /ЗаО/	10	8,75		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 Л1.19Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3	Опрос. Сбор отчетов и отзывов. Анализ результатов.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРАКТИКИ

Оценочные материалы приведены в приложении к рабочей программе практики (см. документ «Оценочные материалы по практике «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	Сычев Ю. Н.	Основы информационной безопасности : учебное пособие	Москва: Евразийский открытый институт, 2010, 328 с.	978-5-374-00381-9, http://www.iprbookshop.ru/10746.html
Л1.2	Пржегорлинский В.Н.	Защита информации как деятельность. Центральный и обеспечивающие объекты защиты информации : учеб. пособие	Рязань, 2012, 63с.	, 1
Л1.3	Засорин С.В., Кузьмин Ю.М., Пржегорлинский В.Н.	Защита в операционных системах. Лабораторный практикум : учеб. пособие	М.: КУРС, 2018, 189с.	978-5-907064-04-1, 1

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.4	Фомина К.Ю., Кураксин В.А.	Методы и средства обнаружения вторжений в компьютерные сети : метод. указ. к лаб. работам	Рязань, 2018, 48с.; прил.	, 1
Л1.5	Кузьмин Ю.М., Кураксин В.А., Пржегорлинский В.Н.	Программно-аппаратные средства обеспечения информационной безопасности : метод. указ. к лаб. работам	Рязань, 2018, 48с.	, 1
Л1.6	Калинкина Т.И., Кузьмин Ю.М., Пржегорлинский В.Н.	Основы построения защищенных баз данных : метод. указ. к лаб. работам	Рязань, 2019, 80с.	, 1
Л1.7	Булычев Г. Г.	Программно-аппаратные средства обеспечения информационной безопасности. Часть 2	Москва: РТУ МИРЭА, 2020, 46 с.	, https://e.lanbook.com/book/163812
Л1.8	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
Л1.9	Белкин П.Ю., Михальский О.В., Першаков А.С., Правиков Д.И., Проскурин В.Г., Фоменков Г.В., Щербаков А.Ю.	Программно-аппаратные средства обеспечения информационной безопасности.Защита программ и данных : Учеб.пособие для вузов	М.:Радио и связь, 1999, 169с.	5-256-01416-1, 1
Л1.10	под ред. А.А.Стрельцова	Организационно-правовое обеспечение информационной безопасности : учеб. пособие для вузов	М.: Академия, 2008, 249с.	978-5-7695-4240-4, 1
Л1.11	Бабаев С.И., Засорин С.В.	Операционные системы. Лабораторный практикум : учеб. пособие	М.: КУРС, 2018, 240с.	978-5-906923-87-5, 1
Л1.12	Голиков А. М.	Основы информационной безопасности : учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2007, 288 с.	978-5-868889-467-1, http://www.iprbookshop.ru/13957.html
Л1.13	Сычев Ю. Н.	Основы информационной безопасности : учебно-методический комплекс	Москва: Евразийский открытый институт, 2012, 342 с.	978-5-374-00602-5, http://www.iprbookshop.ru/14642.html
Л1.14	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
Л1.15	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
Л1.16	Фомина К.Ю., Кураксин В.А.	Методы и средства защиты информации. Ч.1 : Методические указания	Рязань: РИЦ РГРТУ, 2018,	, https://elib.rsreu.ru/ebs/download/1897
Л1.17	Колесенков Н.А., Степашкин В.А.	Угрозы информационной безопасности АС : Методические указания	Рязань: РИЦ РГРТУ, 2019,	, https://elib.rsreu.ru/ebs/download/2078

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.18	Белкин П.Ю., Михальский О.В., Першаков А.С., Правиков Д.И., Проскурин В.Г., Фоменков Г.В., Щербаков А.Ю.	Программно-аппаратные средства обеспечения информационной безопасности.Защита программ и данных : Учеб.пособие для вузов	М.:Радио и связь, 1999, 169с.	5-256-01416-1, 1
Л1.19	под ред. А.А.Стрельцова	Организационно-правовое обеспечение информационной безопасности : учеб. пособие для вузов	М.: Академия, 2008, 249с.	978-5-7695-4240-4, 1

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	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
Л2.2	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.2	Москва: Техносфера, 2019, 630 с.	978-5-94836-524-4, http://www.iprbookshop.ru/93379.html
Л2.3	Пржегорлинский В.Н., Бабаев С.И., Калинкина Т.И.	Компьютерные сети. Ч.1. Основы сетевых технологий : Учебное пособие	Рязань: РИЦ РГРТУ, 2016,	, https://elib.rsreu.ru/ebs/download/936
Л2.4	Кузьмин Ю.М., Калинкина Т.И.	Защита программ и данных. Ч.1 : Методические указания	Рязань: РИЦ РГРТУ, 2019,	, https://elib.rsreu.ru/ebs/download/2119

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Интернет-портал правовой информации, справочно-правовая система [Электронный ресурс]. – URL
Э2	Научная электронная библиотека eLIBRARY.RU. URL
Э3	Интернет-портал ФСТЭК России. URL

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
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
VMware Player	Свободное ПО
Kaspersky Endpoint Security	Коммерческая лицензия
Справочно-правовая система «КонсультантПлюс»	Коммерческая лицензия

6.3.2 Перечень информационных справочных систем

6.3.2.1	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. документ "Методические указания дисциплины "Производственая практика").

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**04.07.24** 21:06 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**04.07.24** 21:06 (MSK)	Простая подпись
ПОДПИСАНО НАЧАЛЬНИКОМ УРОП	**ФГБОУ ВО "РГРТУ", РГРТУ,** Ерзылёва Анна Александровна, Начальник УРОП	**05.07.24** 09:24 (MSK)	Простая подпись

Проверьте содержание РП, информация дублируется несколько раз