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
Проректор по УР
А.В. Корячко

Преддипломная практика

рабочая программа

Закреплена за кафедрой **Информационной безопасности**
Учебный план 10.05.03_23_00.plx

Квалификация **специалист по защите информации**

Форма обучения **очная**
Общая трудоемкость **21 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**11 (6.1)**		Итого	
Недель				
Вид занятий	УП	РП	УП	РП
Контактная внеаудиторная работа	14	14	14	14
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	747	747	747	747
Итого ауд.	2,25	2,25	2,25	2,25
Контактная работа	16,25	16,25	16,25	16,25
Часы на контроль	8,75	8,75	8,75	8,75
Иные формы работы	731	731	731	731
Итого	756	756	756	756

г. Рязань

Программу составил(и):
ст. преп., Фомина Ксения Юрьевна

Рабочая программа
Преддипломная практика
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 28.04.2023 протокол № 11.

Рабочая программа одобрена на заседании кафедры
Информационной безопасности
Протокол от 05.07.2023 г. № 12
Срок действия программы: 2023-2029 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2024 г. № __

Зав. кафедрой _____

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 _____

1. ЦЕЛИ ОСВОЕНИЯ ПРАКТИКИ	
1.1	Выполнение теоретических и практических задач, отвечающих всем требованиям утвержденного задания на ВКР в соответствии с Федеральным государственным образовательным стандартом и формирование у студентов способности к комплексному применению полученных на момент прохождения преддипломной практики знаний, умений и навыков при выполнении задач в рамках работ над ВКР, посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.
2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.О.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Защита государственной тайны в Российской Федерации
2.1.2	Методы и средства обнаружения вторжений в автоматизированные системы
2.1.3	Надежность объектов информационной инфраструктуры
2.1.4	Обеспечение информационной безопасности создания и эксплуатации автоматизированных систем
2.1.5	Практика по получению профессиональных умений и опыта профессиональной деятельности
2.1.6	Проектирование систем защиты информации автоматизированных систем
2.1.7	Теория информации
2.1.8	Компьютерная графика
2.1.9	Научно-исследовательская работа
2.1.10	Производственная практика
2.1.11	Разработка и эксплуатация автоматизированных систем в защищенном исполнении
2.1.12	Сертификация и аттестация по требованиям безопасности компьютерных систем
2.1.13	Сети и системы передачи информации
2.1.14	Управление информационной безопасностью
2.1.15	Информационная безопасность автоматизированных систем
2.1.16	Компьютерные сети
2.1.17	Методы и средства криптографической защиты информации
2.1.18	Модели безопасности компьютерных систем
2.1.19	Модели угроз и нарушителей безопасности информации объектов информатизации
2.1.20	Программно-аппаратные средства защиты информации
2.1.21	Системы управления базами данных
2.1.22	Спецдисциплина 1
2.1.23	Модели безопасности автоматизированных систем
2.1.24	Моделирование
2.1.25	Основы теории живучести сложных систем
2.1.26	Основы теории надежности
2.1.27	Спецдисциплина 3
2.1.28	Государственные стандарты по защите информации
2.1.29	Методы и средства измерения параметров акустических сигналов
2.1.30	Нормативное обеспечение информационной безопасности компьютерных систем
2.1.31	Объекты защиты информации
2.1.32	Ознакомительная практика
2.1.33	Операционные системы
2.1.34	Основы радиотехники
2.1.35	Теория вероятностей и математическая статистика
2.1.36	Учебная практика
2.1.37	Дискретная математика
2.1.38	Организация и методы программирования
2.1.39	Организация ЭВМ и систем
2.1.40	Основы информационной безопасности
2.1.41	Средства криптографической защиты информации
2.1.42	Математическая логика и теория алгоритмов
2.1.43	Математический анализ
2.1.44	Метрология и электрорадиоизмерения

2.1.45	Правовое регулирование в сфере информационно-коммуникационных технологий
2.1.46	Физика
2.1.47	Языки программирования
2.1.48	Алгебра
2.1.49	Программирование на JavaScript
2.1.50	Электроника и схемотехника
2.1.51	Инженерная графика
2.1.52	Геометрия
2.1.53	Информатика
2.1.54	История (история России, всеобщая история)
2.1.55	Основы теории живучести сложных систем
2.1.56	Нормативное обеспечение информационной безопасности компьютерных систем
2.1.57	Основы теории живучести сложных систем
2.1.58	Нормативное обеспечение информационной безопасности компьютерных систем
2.1.59	Информационная безопасность автоматизированных 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

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-1.1. Понимает роль и значение информации, информационных технологий, национальной безопасности, информационной безопасности в современном обществе для обеспечения объективных потребностей личности, общества и государства и использует это понимание в своей профессиональной деятельности

Знать
сущность, понятие и значение информации, информационной безопасности и защиты информации
Уметь
применять достижения информационных технологий для поиска в глобальных компьютерных сетях и иных источниках информацию в области обеспечения информационной безопасности
Владеть
навыками поиска научно – технической литературы, нормативных правовых и методических документов в области информационной безопасности

ОПК-1.2. Использует знание государственной информационной политики и законодательства РФ в области безопасности

Знать
интересы личности, общества и государства, в том числе в информационной сфере, место информационной безопасности в национальной безопасности
Уметь
понимать социальную значимость обеспечения информационной безопасности
Владеть
базовыми знаниями в области информационной безопасности

ОПК-1.3. Анализирует и определяет угрозы информационной безопасности

Знать
основные угрозы информационной безопасности РФ
Уметь
анализировать угрозы информационной безопасности различных субъектов информационной сферы
Владеть
навыками определения источника угрозы информационной безопасности

ОПК-1.4. Понимает роль и место защиты информации при обеспечении безопасности личности, общества и государства и использует это понимание в своей профессиональной деятельности

Знать
виды и направления защиты информации
Уметь
определять возможные результаты вредоносных воздействий на объекты информационной инфраструктуры
Владеть
навыками выявления возможных вредоносных воздействий

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 предприятиинавыками 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-мациионределять требования по защите информации в компьютерных системах
Владеть
навыками работы с научно-технической литературой в области информационных технологий и защиты информации

ОПК-3: Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

ОПК-3.1. Использует фундаментальные законы природы и основные математические методы в своей профессиональной деятельности

Знать
математические методы, используемые для построения физических моделей
Уметь
применять математические методы для построения физических моделей
Владеть
навыками применения математических методов для решения задач профессиональной деятельности

ОПК-3.2. Использует основные дискретные структуры: конечные автоматы, грамматики, графы при решении задач профессиональной деятельности

Знать
дискретные математические модели: методы их построения и оптимизации
Уметь
использовать основные дискретные структуры: конечные автоматы, грамматики, графы при решении задач профессиональной деятельности
Владеть
навыками выполнения задания с использованием математической логики, формальных грамматик и математических моделей графа, а также алгоритмов оптимизации его структуры и весов

ОПК-3.3. Применяет математические методы для решения задач теоретического и прикладного характера

Знать
основные понятия и методы алгебры для формализации и решения профессиональных задач
Уметь
применять аппарат алгебры для разработки вычислительных алгоритмов, реализующих современные математические методы
Владеть
базовыми методами алгебры

ОПК-3.4. Выбирает адекватный математический аппарат для создания моделей объектов и процессов с использованием математической логики, формальных грамматик и математических моделей графа, а также алгоритмов оптимизации его структуры и весов

Знать
основные алгоритмов для улучшения показателей исходного объекта и владение навыками разработки программных решений для последующей автоматизации этих алгоритмов
Уметь
применять графовые математические модели для моделирования различных объектов дискретной природы с целью дальнейшей оптимизации их характеристик
Владеть
навыками выполнения задания для моделирования объектов и процессов прикладных областей с использованием графовых структур

ОПК-3.5. Реализует процедуры решения задач профессиональной деятельности

Знать
методы математического моделирования для решения задач теоретического и прикладного характера
Уметь
использовать математические методы для разработки алгоритмов защиты информации
Владеть
базовыми математическими методами

ОПК-4: Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;

ОПК-4.1. Применяет физические законы для решения задач теоретического и прикладного характера

Знать
фундаментальные законы природы и основные физические законы
Уметь
фундаментальные законы природы и основные физические законы
Владеть
навыками решения физических задач

ОПК-4.2. Применяет способы проведения экспериментальных измерений физических величин, обработки и представления полученных данных и оценки погрешности результатов измерений

Знать
основные физические методы, применяемые при решении прикладных задач
Уметь
применять физические законы для решения прикладных задач
Владеть
навыками использования физических методов для решения задач

ОПК-4.3. Анализирует физическую сущность явлений и процессов при проектировании защищённых информационно-измерительных систем

Знать
методы проведения экспериментальных исследований
Уметь
планировать проведение эксперимента и проводить обработку данных, полученных в ходе физического эксперимента
Владеть
навыками представления данных, полученных в ходе физического эксперимента

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

ОПК-5.1. Проводит мероприятия по обеспечению режима секретности на объекте в соответствии с нормативными и методическими документами

Знать
нормативные правовые акты по обеспечению режима секретности.
Уметь
организовать работы по выполнению режима секретности на объекте.
Владеть
способами организации защиты информации ограниченного доступа.

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

Знать
нормативные и методические документы о защите информации в компьютерных системах.
Уметь
выполнять работы по обеспечению режима защиты информации в компьютерных системах.
Владеть
способами защиты информации в компьютерных системах.

ОПК-5.3. Применяет основы законодательства РФ в области обеспечения информационной безопасности компьютерных систем

Знать
основы законодательства РФ в области обеспечения информационной безопасности компьютерных систем.
Уметь
выполнять работы по обеспечению информационной безопасности компьютерных систем.
Владеть
способами обеспечения информационной безопасности компьютерных систем.

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

Знать
нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.
Уметь
выбрать соответствующие нормативные правовые акты, нормативные и методические документы по защите информации.
Владеть
способами организации защиты информации.

ОПК-5.5. Контролирует работы по выполнению режима защиты информации, в том числе ограниченного доступа

Знать
нормативные и методические документы по выполнению режима защиты информации, в том числе ограниченного доступа.
Уметь
контролировать выполнения режима защиты информации, в том числе ограниченного доступа.
Владеть
способами организации контроля защиты информации на объекте.

ОПК-5.6. Использует знание видов информации в организации защиты информации и обеспечении информационной безопасности

Знать

Уметь

Владеть

ОПК-5.7. Разрабатывает частные политики информационной безопасности автоматизированных систем

Знать
Требования к разработке политик информационной безопасности автоматизированных систем (АС), порядок проведения анализа АС, порядок разработки и типовую структуру разрабатываемой политики информационной безопасности АС
Уметь
Проводить анализ безопасности АС и разрабатывать политики информационной безопасности АС
Владеть
Навыками проведения анализа безопасности АС и разработки политики информационной безопасности АС

ОПК-5.8. Разрабатывает предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем

Знать
Критерии оценки эффективности и направления совершенствования системы управления информационной безопасностью
Уметь
Проводить оценку эффективности системы управления информационной безопасностью АС и определять направление совершенствования системы управления информационной безопасностью АС
Владеть
Навыками оценки эффективности системы управления информационной безопасностью АС и определения направление ее совершенствования

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-6.1. Организует защиту информации, в том числе ограниченного доступа, на объектах информатизации в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России

Знать

Уметь

Владеть

ОПК-6.2. Применяет нормативные и методические документы ФСБ России, ФСТЭК России при решении профессиональных задач

Знать

Уметь

Владеть

ОПК-6.3. Готовит документы, необходимые для получения лицензий на деятельность в области защиты информации

Знать

Уметь

Владеть

ОПК-6.4. Использует знание функций и задач регуляторов в области информационной безопасности и защиты информации

Знать

Уметь

Владеть

ОПК-6.5. Анализирует и оценивает риски информационной безопасности

Знать
Методы и средства анализа и оценки рисков информационной безопасности
Уметь
Анализировать и оценивать риски информационной безопасности
Владеть
Навыками анализа и оценки рисков информационной безопасности

ОПК-6.6. Контролирует эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем

Знать
Показатели эффективности мер по реализации частных политик информационной безопасности автоматизированных систем
Уметь
Контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем
Владеть
Навыками контроля эффективности принятых мер по реализации частных политик информационной безопасности

ОПК-7: Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

ОПК-7.1. Разрабатывает компоненты программного обеспечения компьютерных систем в интегрированных средах разработки программ

Знать
Основные интегрированные среды разработки программ
Уметь
Разрабатывать компоненты программного обеспечения компьютерных систем в интегрированных средах разработки программ
Владеть
Навыками разработки компонентов программного обеспечения компьютерных систем в интегрированных средах разработки программ

ОПК-7.2. Разрабатывает и реализует на языках программирования высокого уровня алгоритмы решения типовых профессиональных задач

Знать
Основные языки программирования высокого уровня и алгоритмы решения типовых профессиональных задач
Уметь
Разрабатывать на языках программирования высокого уровня алгоритмы решения типовых профессиональных задач
Владеть
Навыками разработки и реализации на языках программирования высокого уровня алгоритмов решения типовых профессиональных задач

ОПК-7.3. Планирует разработку программ на языках общего назначения, осуществляет обоснованный выбор инструментария программирования

Знать
Основные языки программирования общего назначения, инструментарий программирования
Уметь
Планировать разработку программ на языках общего назначения, осуществлять обоснованный выбор инструментария программирования
Владеть
Навыками планирования разработки программ на языках общего назначения, обоснованного выбора инструментария программирования

ОПК-7.4. Применяет методы и инструментальные средства программирования для решения профессиональных задач

Знать
Методы и инструментальные средства программирования для решения профессиональных задач
Уметь
Применять методы и инструментальные средства программирования для решения профессиональных задач
Владеть
Навыками применения методов и инструментальных средств программирования для решения профессиональных задач

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

ОПК-8.1. Применяет методы научных исследований при формировании математических моделей безопасности компьютерных систем

Знать
Применяет методы научных исследований при формировании математических моделей безопасности компьютерных систем
Уметь
применять методы научных исследований при формировании математи-ческих моделей безопасности компьютерных систем
Владеть

ОПК-8.2. Обосновывает необходимость защиты информации в автоматизированных системах на основе научных исследований

Знать
обоснования необходимости защиты информации в автоматизированных системах на основе научных исследований
Уметь
обосновывать необходимость защиты информации в автоматизированных системах на основе научных исследований
Владеть
обоснованием необходимости защиты информации в автоматизированных системах на основе научных иссле-дований

ОПК-8.3. Выполняет анализ объекта исследования, ставит цель и задачи исследования

Знать
типовые способы исследования систем, этапы создания и использования компьютерных моделей
Уметь
взаимодействовать с заказчиком исследования, анализировать предметную область, выбирать способ исследования
Владеть
навыками формулирования и согласования требований к компьютерным моделям систем

ОПК-8.4. Участвует в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем

Знать
методы участия в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
Уметь
участвовать в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
Владеть
методами участия в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем

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

Знать
организацию и порядок проведения научно – исследовательских работ
Уметь
определять цель научного исследования, задачи, решения которых необходимо для достижения цели, результаты решения этих задач; формулировать выводы по результатам исследования
Владеть
навыками работы с научно-технической литературой в области информационных технологий и защиты информации

ОПК-8.6. Разрабатывает и оценивает модели объектов исследования

Знать
типовые модели систем, методы генерации случайных величин с заданными законами распределения, критерии согласия
Уметь
разрабатывать и проверять генераторы случайных величин с заданным законом распределения, строить модели с использованием метода статистических испытаний
Владеть
навыками разработки, отладки и эксплуатации программ реализации вычислительного эксперимента, навыками проверки генераторов псевдослучайных чисел с заданными законами распределения

ОПК-8.7. Планирует и проводит эксперимент, обрабатывает его результаты и выполняет анализ этих результатов

Знать
теорию планирования и проведения вычислительного эксперимента, методы обработки и анализа результатов исследований
Уметь
планировать и проводить вычислительный эксперимент, применять методы обработки и анализа результатов исследований
Владеть
навыками планирования и проведения вычислительного эксперимента, сбора, обработки и анализа результатов исследований

ОПК-8.8. Определяет требования по обеспечению информационной безопасности процесса создания защищаемого объекта

Знать
навыками работы с научно-технической литературой в области информационных технологий и защиты информации
Уметь
определять объекты обеспечения информационной безопасности АСЗИ и форми-ровать для них перечни и мо-дели угроз информационной безопасности
Владеть
навыками работы формировать требования по обеспечению информацион-ной безопасности объектов обеспечения информационной безопасности, адекватные ак-туальным угрозам их инфор-мационной безопасности

ОПК-8.9. Использует при решении профессиональных задач знания математического аппарата теории информации, математических моделей сигнала, моделей и характеристик источников сообщений и каналов связи

Знать
Теоретические основы теории информации, теории сигналов, каналов связи и источников сообщений
Уметь
Применять на практике теоретические основы теории информации, теории сигналов, каналов связи и источников сообщений
Владеть
Навыками использования основ теории информации, теории сигналов, каналов связи и источников сообщений

ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;

ОПК-9.1. Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов и средств защиты информации от утечки по техническим каналам

Знать
Методы и средства защиты информации от утечки по техническим каналам в соответствии с действующими тенденциями их развития
Уметь
Решать задачи профессиональной деятельности с учетом современного состояния методов и средств защиты информации от утечки по техническим каналам
Владеть
Навыками решения задач профессиональной деятельности с учетом современного состояния методов и средств защиты информации от утечки по техническим каналам

ОПК-9.2. Решает задачи профессиональной деятельности, используя радиотехнические системы, с учетом текущего состояния развития методов и средств защиты информации от утечки по техническим каналам

Знать
Основные вопросы использования радиотехнических систем в вопросах технической защиты информации от утечки по техническим каналам
Уметь
Применять на практике радиотехнических систем в вопросах технической защиты информации от утечки по техническим каналам
Владеть
Навыками использования радиотехнических систем в вопросах технической защиты информации от утечки по техническим каналам

ОПК-9.3. Решает задачи профессиональной деятельности с учетом состояния, возможностей и тенденций развития сетей и систем передачи информации

Знать
классификацию и структуру сетей связи и вычислительных сетей; построение, методы доступа, основные протоколы вычислительных сетей; принципы построения современных систем передачи информации
Уметь
проводить анализ показателей качества сетей и систем связи
Владеть
навыками объединения средств вычислительной техники в локальные и корпоративные сети

ОПК-9.4. Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий

Знать
задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
Уметь
решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
Владеть
решением задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий

ОПК-9.5. Вычисляет теоретико-информационные характеристики источников сообщений и каналов связи при решении задач профессиональной деятельности

Знать
математический аппарат теории информации; математические модели сигнала, их особенности, области, возможности, ограничения и условия применения
Уметь
вычислять теоретико-информационные характеристики источников сообщений и каналов связи
Владеть
навыками применения математического аппарата теории информации для решения научных, практических и исследовательских задач в профессиональной деятельности

ОПК-9.6. Решает задачи профессиональной деятельности с применением методов и средств инсталляции и администрирования сетевого программного обеспечения и с учетом основных требований информационной безопасности

Знать
методы и средства инсталляции и администрирования сетевого программного обеспечения
Уметь
использовать системные и прикладные программы для анализа работы сервера и диагностики сети, распределять права
Владеть
методами и средствами инсталляции и администрирования сетевого программного обеспечения

ОПК-9.7. Использует средства защиты информации от утечки по техническим каналам при решении профессиональных задач

Знать
Общие вопросы применения средств защиты информации от утечки по техническим каналам
Уметь
Применять на практике средств защиты информации от утечки по техническим каналам
Владеть
Навыками использования средств защиты информации от утечки по техническим каналам

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

ОПК-10.1. Применяет алгоритмы функционирования криптографических систем

Знать
основные виды симметричных и асимметричных криптографических алгоритмов;математические модели шифров
Уметь
корректно применять симметричные и асимметричные криптографические алгоритмы
Владеть
криптографической терминологией

ОПК-10.2. Применяет алгоритмы функционирования электронной подписи

Знать
основные алгоритмы электронной подписи
Уметь
работать со средствами создания электронной подписи
Владеть
навыками установки и настройки средств работы с электронной подписью

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

Знать
принципы работы современных средств криптографической защиты информации
Уметь
производить установку, наладку, тестирование и обслуживание средств криптографической защиты информации
Владеть
навыками применения криптографических средств с учетом требований нормативных и правовых актов по защите информации

ОПК-11: Способен разрабатывать компоненты систем защиты информации автоматизированных систем;

ОПК-11.1. Выбирает программно-аппаратные средства защиты информации для использования в составе автоматизированных систем

Знать
Программно-аппаратные средства защиты информации, используемые в составе автоматизированных систем
Уметь
Выбирать программно-аппаратные средства защиты информации для использования в составе автоматизированных систем
Владеть
Навыками выбора программно-аппаратных средств защиты информации для использования в составе автоматизированных систем

ОПК-11.2. Применяет программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах

Знать
Программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах
Уметь
Применять программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах
Владеть
Навыками применения программно-аппаратных средств защиты информации для обеспечения безопасности информации в автоматизированных системах

ОПК-12: Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

ОПК-12.1. Использует в работе современные операционные системы и выполняет основные действия по системному администрированию

Знать
назначение, принципы построения и функционирования, эксплуатации и использования современных ОС
Уметь
выполнять все основные операции по администрированию операционных систем
Владеть
навыками администрирования современных операционных систем

ОПК-12.2. Выполняет установку, обслуживание и восстановление работоспособности компонентов общего и специального программного назначения

Знать
способы установки и обслуживания современного общего и специального программного обеспечения
Уметь
выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения
Владеть
навыками восстановления работоспособности прикладного и системного программного обеспечения

ОПК-12.3. Оценивает характеристики встроенных средств защиты информации операционных систем и прикладных программ, использует и настраивает их

Знать
способы оценки характеристики встроенных средств защиты информации в опереционных системах
Уметь
настраивать встроенные средства защиты информации операционных систем и прикладных программ
Владеть
навыками настройки встроенных средств защиты информации операционных систем и прикладных программ

ОПК-12.4. Оценивает состояние и осуществляет администрирование операционных систем

Знать
принципы установки, наладки, тестирования и обслуживания современного общего и специального программного обеспечения, включая операционные системы
Уметь
выполнять установку и обслуживание современного общего и специального программного обеспечения по восстановлению работоспособности прикладного и системного программного обеспечения
Владеть
навыками оценки характеристик основных типов программно-аппаратных средств защиты операционных систем, прикладных программ и данных

ОПК-12.5. Выбирает СУБД в соответствии с требованиями о защите информации

Знать
требования по защите информации, определяющие выбор СУБД; состав, назначение функциональных компонентов и программного обеспечения СУБД; структуру и принципы работы современных баз данных
Уметь
устанавливать, настраивать и эксплуатировать СУБД
Владеть
навыками проектирования баз данных

ОПК-12.6. Выполняет работу с базами данных с использованием языка SQL

Знать
общие принципы построения и использования языка SQL, особенности взаимодействия языков высокого и низкого уровня с СУБД
Уметь
работать с интегрированными средами разработки программного обеспечения, позволяю-щими использовать СУБД; разрабатывать запросы к базе данных на языке SQL
Владеть
навыками разработки, тестирования и отладки программ и запросов на языке SQL

ОПК-12.7. Использует и настраивает средства защиты информации в компьютерных сетях

Знать
средства защиты информации в компьютерных сетях
Уметь
использовать и настраивать средства защиты информации в компьютерных сетях
Владеть
использованием и настройкой средств защиты информации в компьютерных сетях

ОПК-12.8. Администрирует компьютерные сети

Знать
администрование компьютерных сетей
Уметь
администрировать компьютерные сети
Владеть
администрированием компьютерных сетей

ОПК-12.9. Контролирует и поддерживает корректность и эффективность функционирования компьютерных сетей

Знать
контроль и поддержку корректности и эффективности функционирования компьютерных сетей
Уметь
контролировать и поддерживать корректность и эффективность функционирования компьютерных сетей
Владеть
контролем и поддержкой корректности и эффективности функционирования компьютерных сетей

ОПК-12.10. Настраивает межсетевые экраны

Знать
межсетевые экраны
Уметь
настраивать межсетевые экраны
Владеть
Настройкой межсетевых экранов

ОПК-12.11. Осуществляет настройку СУБД в соответствии с заданной политикой безопасности

Знать
принципы работы современных СУБД
Уметь
производить настройку современных СУБД в соответствии с заданной политикой безопасности
Владеть
навыками настройки современных СУБД в соответствии с заданной политикой безопасности

ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;

ОПК-13.1. Участвует в разработке, внедрении и эксплуатации автоматизированных систем с учетом требований по защите информации, проведении подготовки исходных данных для технико-экономического обоснования проектных решений

Знать
типовой перечень и порядок проведения работ по созданию АСЗИ; основные документы ФСТЭК России и ФСБ России, определяющие требования о защите информации в АСЗИ
Уметь
использовать документы ФСТЭК России и ФСБ России в области защиты информации для определения необходимых исходных данных для формирования требований о защите информации на предпроектных стадиях создания АСЗИ
Владеть
методами подготовки исходных данных для технико – экономического обоснования проектных решений

ОПК-13.2. Осуществляет диагностику и тестирование систем защиты информации автоматизированных систем

Знать
методы осуществления диагностики и тестирования средств и систем защиты информации
Уметь
использовать документацию на средства защиты информации для проведения их диагностики и тестирования
Владеть
способами диагностики и тестирования систем защиты информации автоматизированных систем

ОПК-13.3. Проводит анализ уязвимостей систем защиты информации автоматизированных систем

Знать
типовой перечень и порядок проведения работ по созданию АСЗИ; методику оценки угроз безопасности информации в инфраструктурных системах
Уметь
определять актуальные угрозы безопасности для объектов защиты информационных систем и возможности их реализации;Определять объекты защиты информационных системопределять актуальные угрозы безопасности для объектов защиты информационных систем и возможности их реализации; определять объекты защиты информационных систем
Владеть
методами проведения анализа уязвимостей систем защиты информации автоматизированных систем

ОПК-14: Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;

ОПК-14.1. Выбирает средства защиты информации, имеющие сертификаты соответствия и удовлетворяющие требованиям безопасности информации, для проектируемых автоматизированных систем

Знать
требования к техническим средствам защиты информации, на основании которых проводится сертификация;принципы работы технических средств защиты информации;
Уметь
выбирать технические средства защиты информации;
Владеть
навыками работы с техническими средствами защиты информации

ОПК-14.2. Определяет требования к лицензиату в области технической защиты информации

Знать
нормативно-методические документы, регламентирующие требования к лицензиату в области технической защиты информации
Уметь
определять требования к лицензиату в области технической защиты информации
Владеть

ОПК-14.3. Применяет языки программирования для разработки компонентов программного обеспечения

Знать
Основные языки программирования для разработки компонентов программного обеспечения
Уметь
Применять языки программирования для разработки компонентов программного обеспечения
Владеть
Навыками применения языков программирования для разработки компонентов программного обеспечения

ОПК-14.4. Готовит исходные данные и формирует требования о защите информации в автоматизированных системах в защищенном исполнении

Знать
содержание основных работ по созданию АСЗИ, проводимых на пред проектных стадиях
Уметь
разрабатывать программу и методику обследования объектов автоматизации и автоматизируемой деятельности, предполагаемых условий размещения объектов информатизации; проводить по результатам обследования оценку угроз безопасности информации; формировать перечень требований о защите информации в АСЗИ
Владеть
навыками классификации информационных систем

ОПК-14.5. Проектирует автоматизированные системы с учетом требований о защите информации

Знать
содержание основных работ по созданию АСЗИ, проводимых на стадиях проектирования
Уметь
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

ОПК-14.6. Готовит исходные данные для технико-экономического обоснования проектных решений по автоматизированным системам в защищенном исполнении и их частям

Знать
содержание основных работ по созданию АСЗИ, проводимых на стадиях проектирования
Уметь
готовить необходимые исходные данные для технико-экономического обоснования разрабатываемых проектных решений по системе в целом и ее составным частям, в том числе разрабатывать аналитическое обоснование необходимости создания системы защиты информации в составе информационной системы
Владеть
терминологией в области проектирования информационных систем

ОПК-14.7. Осуществляет ввод в эксплуатацию и эксплуатацию автоматизированных систем в защищенном исполнении

Знать
содержание основных работ, проводимых при вводе АСЗИ в эксплуатацию; организацию и общие правила эксплуатации АСЗИ; типовой перечень и порядок проведения работ по эксплуатации АСЗИ, в том числе обеспечение режима секретности при эксплуатации АСЗИ
Уметь
разрабатывать программы и методики испытаний АСЗИ и ее составных частей, документацию на комплектование АСЗИ изделиями серийного производства
Владеть
навыками работы с эксплуатационной документацией на комплектующие изделия АСЗИ

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

ОПК-15.1. Определяет информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите

Знать
Основные информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите
Уметь
Определять информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите
Владеть
Навыками определения информационной инфраструктуры и информационных ресурсов автоматизированных систем, подлежащие защите

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

Знать
Основные угрозы безопасности автоматизированных систем в защищенном исполнении
Уметь
Основные угрозы безопасности автоматизированных систем в защищенном исполнении
Владеть
Навыками выявления угроз безопасности автоматизированных систем в защищенном исполнении

ОПК-16: Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.

ОПК-16.1. Анализирует закономерности и основные этапы исторического развития России в контексте всеобщей истории

Знать
закономерности и основные этапы исторического развития России в контексте всеобщей истории
Уметь
понимать и воспринимать разнообразие общества в социально-историческом, этическом и философском контекстах
Владеть
простейшими методами адекватного восприятия межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах

ОПК-16.2. Формирует гражданскую позицию в контексте патриотического воспитания

Знать
важность формирования своей гражданской позиции патриота своей страны и норм права, которые способствуют этому
Уметь
анализировать практические решения на предмет соответствия своей гражданской позиции
Владеть
навыками поиска нормативной правовой информации, необходимой для формирования своей гражданской активности

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

Уметь

Владеть

ОПК-8.1..2. Формулирует и обосновывает требования информационной безопасности при создании и эксплуатации автоматизированной системы в защищенном исполнении

Знать

Уметь

Владеть

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

Уметь

Владеть

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

Знать

Уметь

Владеть

ОПК-8.2..3. Осуществляет документирование системы защиты информации автоматизированных систем в защищенном исполнении

Знать

Уметь

Владеть

ОПК-8.3.: Способен организовывать и обеспечивать информационную безопасность процесса создания автоматизированной системы в защищенном исполнении;

ОПК-8.3..1. Определяет требования по обеспечению информационной безопасности процесса создания (развития) автоматизированных систем в защищенном исполнении

Знать

Уметь

Владеть

ОПК-8.3..2. Обеспечивает информационную безопасность создания (развития) автоматизированных систем в защищенном исполнении

Знать

Уметь

Владеть

ПК-1: Способен проектировать объекты информатизации в защищенном исполнении

ПК-1.1. Проектирует ОВТ в защищенном исполнении

Знать
направления защиты информации в компьютерных системах, свойства вредоносных воздействий, на противодействие которым эти направления ориентированы, свойства направлений защиты информации
Уметь
определять свойства вредоносных воздействий и необходимые для противодействия им направления защиты информации
Владеть
навыками работы с научно – технической литературой и ГОСТами в области компьютерной безопасности

ПК-1.2. Проектирует выделенные (защищаемые) помещения

Знать
объекты защиты информации и условия их функционирования, требования о защите информации на объектах информатизации
Уметь
определять необходимые виды и направления защиты информации на объектах информатизации
Владеть
навыками работы с нормативными и методическими документами в области защиты информации

ПК-2: Способен проводить аттестацию объектов информатизации на соответствие требованиям по защите информации

ПК-2.1. Проводит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации

Знать
структуру, состав и функции комплексных объектов защиты информации и их систем защиты информации
Уметь
определять факторы, воздействующие на защищаемую информацию в комплексных объектах защиты информации
Владеть
навыками работы с инструкциями на средства защиты информации

ПК-2.2. Проводит аттестацию выделенных (защищаемых) помещений на соответствие требованиям по защите информации

Знать

Уметь

Владеть

ПК-3: Способен организовывать разработку системного программного обеспечения

ПК-3.1. Планирует разработку системного программного обеспечения

Знать
Принципы разработки и жизненный цикл системного программного обеспечения
Уметь
Планировать разработку системного программного обеспечения
Владеть
Навыками планирования разработки системного программного обеспечения

ПК-3.2. Организует работу программистов в группе по разработке системного программного обеспечения

Знать
Принципы работы программистов в группе по разработке системного программного обеспечения
Уметь
Организовывать работу программистов в группе по разработке системного программного обеспечения
Владеть
Навыками организации работы программистов в группе по разработке системного программного обеспечения

ПК-4: Способен разрабатывать системы защиты информации автоматизированных, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категории значимости

ПК-4.1. Тестирует системы защиты информации автоматизированных систем

Знать

Уметь

Владеть

ПК-4.2. Разрабатывает проектные решения по защите информации в автоматизированных системах

Знать
основы проведения научных исследований
Уметь
разрабатывать типовые нормативные документы по оценке угроз информационной безопасности компьютерных систем и их формальному представлению
Владеть
навыками администрирования компьютерных сетей, систем баз данных и ОС

ПК-4.3. Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем

Знать
основы построения защищенных компьютерных сетей
Уметь
разрабатывать типовые нормативные акты по обеспечению информационной безопасности на предприятии
Владеть
навыками работы с нормативными документами по определению требований о защите информации компьютерных систем

ПК-5: Способен разрабатывать системы защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категории значимости

ПК-5.1. Обосновывает необходимость защиты информации в автоматизированной системе

Знать
основы законодательства РФ в области обеспечения информационной безопасности компьютерных систем в защищенном исполнении
Уметь
разрабатывать типовые модели угроз информационной безопасности
Владеть
навыками работы с документацией на предприятии

ПК-5.2. Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой

Знать
Руководящие и методические документы по разработке моделей угроз и нарушителей информационной безопасности
Уметь
представлять формальные модели политик безопасности
Владеть
современными информационными технологиями работы на проектами

ПК-5.3. Разрабатывает архитектуру системы защиты информации автоматизированной системы

Знать

Уметь

Владеть

В результате освоения практики обучающийся должен

3.1	**Знать:**
3.1.1	□ сущность, понятие и значение информации, информационной безопасности и защиты информации
3.1.2	□ интересы личности, общества и государства, в том числе в информационной сфере, место информационной безопасности в национальной безопасности
3.1.3	□ основные угрозы информационной безопасности РФ
3.1.4	□ виды и направления защиты информации
3.1.5	□ современные информационные технологии (операционные системы, базы данных, вычислительные сети)
3.1.6	□ виды и категории защищаемой информации
3.1.7	□ технические возможности систем защиты информации
3.1.8	□ основные математические законы и методы накопления, передачи и обработки научной информации.
3.1.9	□ дискретные математические модели: методы их построения и оптимизации
3.1.10	□ основные математические законы и методы накопления, передачи и обработки научной информации.

3.1.11	□ основные алгоритмов для улучшения показателей исходного объекта и владение навыками разработки программных решений для последующей автоматизации этих алгоритмов
3.1.12	□ основные математические законы и методы накопления, передачи и обработки научной информации.
3.1.13	□ фундаментальные законы природы и основные физические законы
3.1.14	□ основные физические методы, применяемые при решении прикладных задач
3.1.15	□ методы проведения экспериментальных исследований
3.1.16	□ нормативные правовые акты по обеспечению режима секретности.
3.1.17	□ нормативные и методические документы о защите информации в компьютерных системах.
3.1.18	□ основы законодательства РФ в области обеспечения информационной безопасности компьютерных систем.
3.1.19	□ нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.
3.1.20	□ нормативные и методические документы по выполнению режима защиты информации, в том числе ограниченного доступа
3.1.21	□ Требования к разработке политик информационной безопасности автоматизированных систем (АС), порядок проведения анализа АС, порядок разработки и типовую структуру разрабатываемой политики информационной безопасности АС
3.1.22	□ Критерии оценки эффективности и направления совершенствования системы управления информационной безопасностью
3.1.23	□ Методы и средства анализа и оценки рисков информационной безопасности
3.1.24	□ Показатели эффективности мер по реализации частных политик информационной безопасности автоматизированных систем
3.1.25	□ Основные интегрированные среды разработки программ
3.1.26	□ Основные языки программирования высокого уровня и алгоритмы решения типовых профессиональных задач
3.1.27	□ Основные языки программирования общего назначения, инструментарий программирования
3.1.28	□ Методы и инструментальные средства программирования для решения профессиональных задач
3.1.29	□ Применяет методы научных исследований при формировании математических моделей безопасности компьютерных систем
3.1.30	□ обоснования необходимости защиты информации в автоматизированных системах на основе научных исследований
3.1.31	□ Типовые способы исследования систем, этапы создания и использования компьютерных моделей
3.1.32	□ методы участия в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
3.1.33	□ организацию и порядок проведения научно – исследовательских работ
3.1.34	□ Типовые модели систем, методы генерации случайных величин с заданными законами распределения, критерии согласия
3.1.35	□ Теорию планирования и проведения вычислительного эксперимента, методы обработки и анализа результатов исследований
3.1.36	□ навыками работы с научно-технической литературой в области информационных технологий и защиты информации
3.1.37	□ Теоретические основы теории информации, теории сигналов, каналов связи и источников сообщений
3.1.38	□ Методы и средства защиты информации от утечки по техническим каналам в соответствии с действующими тенденциями их развития
3.1.39	□ Основные вопросы использования радиотехнических систем в вопросах технической защиты информации от утечки по техническим каналам
3.1.40	□ классификацию и структуру сетей связи и вычислительных сетей; построение, методы доступа, основные протоколы вычислительных сетей; принципы построения современных систем передачи информации
3.1.41	□ задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
3.1.42	□ математический аппарат теории информации; математические модели сигнала, их особенности, области, возможности, ограничения и условия применения
3.1.43	□ методы и средства инсталляции и администрирования сетевого программного обеспечения
3.1.44	□ Общие вопросы применения средств защиты информации от утечки по техническим каналам
3.1.45	□ основные виды симметричных и асимметричных криптографических алгоритмов;
3.1.46	□ математические модели шифров

3.1.47	□ основные алгоритмы электронной подписи
3.1.48	□ принципы работы современных средств криптографической защиты информации
3.1.49	□ Программно-аппаратные средства защиты информации, используемые в составе автоматизированных систем
3.1.50	□ Программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах
3.1.51	□ назначение, принципы построения и функционирования, эксплуатации и использования современных ОС
3.1.52	□ способы установки и обслуживания современного общего и специального программного обеспечения
3.1.53	□ способы оценки характеристики встроенных средств защиты информации в опереционных системах
3.1.54	□ принципы установки, наладки, тестирования и обслуживания современного общего и специального программного обеспечения, включая операционные системы
3.1.55	□ требования по защите информации, определяющие выбор СУБД; состав, назначение функциональных компонентов и программного обеспечения СУБД; структуру и принципы работы современных баз данных
3.1.56	□ общие принципы построения и использования языка SQL, особенности взаимодействия языков высокого и низкого уровня с СУБД
3.1.57	□ средства защиты информации в компьютерных сетях
3.1.58	□ администрование компьютерных сетей
3.1.59	□ контроль и поддержку корректности и эффективности функционирования компьютерных сетей
3.1.60	□ межсетевые экраны
3.1.61	□ принципы работы современных СУБД
3.1.62	□ типовой перечень и порядок проведения работ по созданию АСЗИ; основные документы ФСТЭК России и ФСБ России, определяющие требования о защите информации в АСЗИ
3.1.63	□ методы осуществления диагностики и тестирования средств и систем защиты информации
3.1.64	□ типовой перечень и порядок проведения работ по созданию АСЗИ; методику оценки угроз безопасности информации в инфраструктурных системах
3.1.65	□ требования к техническим средствам защиты информации, на основании которых проводится сертификация;
3.1.66	□ принципы работы технических средств защиты информации;
3.1.67	□ нормативно-методические документы, регламентирующие требования к лицензиату в области технической защиты информации
3.1.68	□ Основные языки программирования для разработки компонентов программного обеспечения
3.1.69	□ содержание основных работ по созданию АСЗИ, проводимых на пред проектных стадиях
3.1.70	□ содержание основных работ по созданию АСЗИ, проводимых на стадиях проектирования
3.1.71	□ содержание основных работ по созданию АСЗИ, проводимых на стадиях проектирования
3.1.72	□ содержание основных работ, проводимых при вводе АСЗИ в эксплуатацию; организацию и общие правила эксплуатации АСЗИ; типовой перечень и порядок проведения работ по эксплуатации АСЗИ, в том числе обеспечение режима секретности при эксплуатации АСЗИ
3.1.73	□ Основные информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите
3.1.74	□ Основные угрозы безопасности автоматизированных систем в защищенном исполнении
3.1.75	□ Важность формирования своей гражданской позиции патриота своей страны и норм права, которые спо-собствуют этому
3.1.76	□ потенциальные угрозы информационной безопасности автоматизированных систем.
3.1.77	□ навыками разработки модели угроз информационной безопасности автоматизированной системы.
3.1.78	□ объекты обеспечения информационной без-опасности создания (развития) АСЗИ; угрозы информа-ционной безопасности АСЗИ
3.1.79	□ определять объекты обеспечения информационной безопасности создания (раз-вития) АСЗИ и формировать для них перечни и модели угроз информационной без-опасности
3.1.80	□ навыками работы формировать требования по обеспечению информацион-ной безопасности объектов обеспечения информационной безопасности, адекватные ак-туальным угрозам их инфор-мационной безопасности, и оценивать их полноту и не-противоречивость
3.1.81	□ меры и средства обеспечения информационной безопасности создания (развития) АСЗИ
3.1.82	□ направления защиты информации в компьютерных системах, свойства вредоносных воздействий, на противодействие которым эти направления ориентированы, свойства направлений защиты информации
3.1.83	□ объекты защиты информации и условия их функционирования, требования о защите информации на объектах информатизации

3.1.84	□ основы проведения научных исследований
3.1.85	□ основы построения защищенных компьютерных сетей
3.1.86	□ структуру, состав и функции комплексных объектов защиты информации и их систем защиты информации
3.1.87	□ Принципы разработки и жизненный цикл системного программного обеспечения
3.1.88	□ Принципы работы программистов в группе по разработке системного программного обеспечения
3.1.89	□ основы законодательства РФ в области обеспечения информационной безопасности компьютерных систем в защищенном исполнении
3.1.90	□ Руководящие и методические документы по разработке моделей угроз и нарушителей информационной безопасности
3.2	**Уметь:**
3.2.1	□ применять достижения информационных технологий для поиска в глобальных компьютерных сетях и иных источниках информацию в области обеспечения информационной безопасности
3.2.2	□ понимать социальную значимость обеспечения информационной безопасности
3.2.3	□ анализировать угрозы информационной безопасности различных субъектов информационной сферы
3.2.4	□ определять возможные результаты вредоносных воздействий на объекты информационной инфраструктуры
3.2.5	□ проводить анализ угроз безопасности информации на объекте информатизации
3.2.6	□ проводить сравнение и подбор систем защиты инфор-мации
3.2.7	□ определять требования по защите информации в компьютерных системах
3.2.8	□ применять математические методы для решения задач теоретического и прикладного характера.
3.2.9	□ использовать основные дискретные структуры: конечные автоматы, грамматики, графы при решении задач профессиональной деятельности
3.2.10	□ применять математические методы для решения задач теоретического и прикладного характера.
3.2.11	□ применять графовые математические модели для моделирования различных объектов дискретной природы с целью дальнейшей оптимизации их характеристик.
3.2.12	□ применять математические методы для решения задач теоретического и прикладного характера.
3.2.13	□ применять на практике основные физические законы
3.2.14	□ применять физические законы для решения прикладных задач
3.2.15	□ планировать проведение эксперимента и проводить обработку данных, полученных в ходе физического эксперимента
3.2.16	□ организовать работы по выполнению режима секретности на объекте.
3.2.17	□ выполнять работы по обеспечению режима защиты информации в компьютерных системах.
3.2.18	□ выполнять работы по обеспечению информационной безопасности компьютерных систем.
3.2.19	□ выбрать соответствующие нормативные правовые акты, нормативные и методические документы по защите информации.
3.2.20	□ контролировать выполнения режима защиты информации, в том числе ограниченного доступа
3.2.21	□ Проводить анализ безопасности АС и разрабатывать политики информационной безопасности АС
3.2.22	□ Проводить оценку эффективности системы управления информационной безопасностью АС и определять направление совершенствования системы управления информационной безопасностью АС
3.2.23	□ Анализировать и оценивать риски информационной безопасности
3.2.24	□ Контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем
3.2.25	□ Разрабатывать компоненты программного обеспечения компьютерных систем в интегрированных средах разработки программ
3.2.26	□ Разрабатывать на языках программирования высокого уровня алгоритмы решения типовых профессиональных задач
3.2.27	□ Планировать разработку программ на языках общего назначения, осуществлять обоснованный выбор инструментария программирования
3.2.28	□ Применять методы и инструментальные средства программирования для решения профессиональных задач
3.2.29	□ применять методы научных исследований при формировании математи-ческих моделей безопасности компьютерных систем
3.2.30	□ обосновывать необходимость защиты информации в автоматизированных системах на основе научных исследований

3.2.31	Взаимодействовать с заказчиком исследования, анализировать предметную область, выбирать способ исследования
3.2.32	участвовать в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
3.2.33	определять цель научного исследования, задачи, решения которых необходимо для достижения цели, результаты решения этих задач; формулировать выводы по результатам исследования
3.2.34	Разрабатывать и проверять генераторы случайных величин с заданным законом распределения, строить модели с использованием метода статистических испытаний
3.2.35	Планировать и проводить вычислительный эксперимент, применять методы обработки и анализа результатов исследований
3.2.36	определять объекты обеспечения информационной безопасности АСЗИ и формировать для них перечни и модели угроз информационной безопасности
3.2.37	Применять на практике теоретические основы теории информации, теории сигналов, каналов связи и источников сообщений
3.2.38	Решать задачи профессиональной деятельности с учетом современного состояния методов и средств защиты информации от утечки по техническим каналам
3.2.39	Применять на практике радиотехнических систем в вопросах технической защиты информации от утечки по техническим каналам
3.2.40	проводить анализ показателей качества сетей и систем связи
3.2.41	решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
3.2.42	вычислять теоретико-информационные характеристики источников сообщений и каналов связи
3.2.43	использовать системные и прикладные программы для анализа работы сервера и диагностики сети, распределять права
3.2.44	Применять на практике средств защиты информации от утечки по техническим каналам
3.2.45	корректно применять симметричные и асимметричные криптографические алгоритмы
3.2.46	работать со средствами создания электронной подписи
3.2.47	производить установку, наладку, тестирование и обслуживание средств криптографической защиты информации
3.2.48	Выбирать программно-аппаратные средства защиты информации для использования в составе автоматизированных систем
3.2.49	Применять программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах
3.2.50	выполнять все основные операции по администрированию операционных систем
3.2.51	выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения
3.2.52	настраивать встроенные средства защиты информации операционных систем и прикладных программ
3.2.53	выполнять установку и обслуживание современного общего и специального программного обеспечения по восстановлению работоспособности прикладного и системного программного обеспечения
3.2.54	устанавливать, настраивать и эксплуатировать СУБД
3.2.55	работать с интегрированными средами разработки программного обеспечения, позволяю-щими использовать СУБД; разрабатывать запросы к базе данных на языке SQL
3.2.56	использовать и настраивать средства защиты информации в компьютерных сетях
3.2.57	администрировать компьютерные сети
3.2.58	контролировать и поддерживать корректность и эффективность функционирования компьютерных сетей
3.2.59	настраивать межсетевые экраны
3.2.60	производить настройку современных СУБД в соответствии с заданной политикой безопасности
3.2.61	использовать документы ФСТЭК России и ФСБ России в области защиты информации для определения необходимых исходных данных для формирования требований о защите информации на предпроектных стадиях создания АСЗИ
3.2.62	использовать документацию на средства защиты информации для проведения их диагностики и тестирования
3.2.63	определять актуальные угрозы безопасности для объектов защиты информационных систем и возможности их реализации;
3.2.64	Определять объекты защиты информационных систем
3.2.65	определять актуальные угрозы безопасности для объектов защиты информационных систем и возможности их реализации; определять объекты защиты информационных систем

3.2.66	□ выбирать технические средства защиты информации;
3.2.67	□ определять требования к лицензиату в области технической защиты информации
3.2.68	□ Применять языки программирования для разработки компонентов программного обеспечения
3.2.69	□ разрабатывать программу и методику обследования объектов автоматизации и автоматизируемой деятельности, предполагаемых условий размещения объектов информатизации; проводить по результатам обследования оценку угроз безопасности информации; формировать перечень требований о защите информации в АСЗИ
3.2.70	□ разрабатывать АСЗИ на проектных стадиях, в том числе разрабатывать технические задания на составные части АСЗИ
3.2.71	□ готовить необходимые исходные данные для технико-экономического обоснования разрабатываемых проектных решений по системе в целом и ее составным частям, в том числе разрабатывать аналитическое обоснование необходимости создания системы защиты информации в составе информационной системы
3.2.72	□ разрабатывать программы и методики испытаний АСЗИ и ее составных частей, документацию на комплектование АСЗИ изделиями серийного производства
3.2.73	□ Определять информационную инфраструктуру и информационные ресурсы автоматизированных систем, подлежащие защите
3.2.74	□ Основные угрозы безопасности автоматизированных систем в защищенном исполнении
3.2.75	□ Анализировать практические решения на предмет соответствия своей гражданской позиции.
3.2.76	□ определять возможные направления и способы реализации угроз информационной безопасности в автоматизированной системе.
3.2.77	□ определять требования по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированной системы.
3.2.78	□ определять объекты обеспечения информационной безопасности создания (раз-вития) АСЗИ и формировать для них перечни и модели угроз информационной без-опасности
3.2.79	□ определять объекты обеспечения информационной безопасности создания (раз-вития) АСЗИ, оценивать их достаточность
3.2.80	□ определять свойства вредоносных воздействий и необходимые для противодействия им направления защиты информации
3.2.81	□ определять необходимые виды и направления защиты информации на объектах информатизации
3.2.82	□ разрабатывать типовые нормативные документы по оценке угроз информационной безопасности компьютерных систем и их формальному представлению
3.2.83	□ разрабатывать типовые нормативные акты по обеспечению информационной безопасности на предприятии
3.2.84	□ определять факторы, воздействующие на защищаемую информацию в комплексных объектах защиты информации
3.2.85	□ Планировать разработку системного программного обеспечения
3.2.86	□ Организовывать работу программистов в группе по разработке системного программного обеспечения
3.2.87	□ разрабатывать типовые модели угроз информационной безопасности
3.2.88	□ представлять формальные модели политик безопасности
3.3	**Владеть:**
3.3.1	□ навыками поиска научно – технической литературы, нормативных правовых и методических документов в области информационной безопасности
3.3.2	□ базовыми знаниями в области информационной безопасности
3.3.3	□ навыками определения источника угрозы информационной безопасности
3.3.4	□ навыками выявления возможных вредоносных воздействий
3.3.5	□ навыками работы с документацией на предприятии
3.3.6	□ навыками анализа технической документации объектов профессиональной деятельности
3.3.7	□ навыками работы с научно-технической литературой в области информационных технологий и защиты информации
3.3.8	□ навыками использования математического аппарата при решении практических задач.
3.3.9	□ Навыками выполнения задания с использованием математической логики, формальных грамматик и математических моделей графа, а также алгоритмов оптимизации его структуры и весов
3.3.10	□ навыками использования математического аппарата при решении практических задач.
3.3.11	□ Навыками выполнения задания для моделирования объектов и процессов прикладных областей с использованием графовых структур
3.3.12	□ навыками использования математического аппарата при решении практических задач.

3.3.13	□ навыками решения физических задач
3.3.14	□ навыками использования физических методов для решения задач
3.3.15	□ навыками представления данных, полученных в ходе физического эксперимента
3.3.16	□ способами организации защиты информации ограниченного доступа.
3.3.17	□ способами защиты информации в компьютерных системах.
3.3.18	□ способами обеспечения информационной безопасности компьютерных систем.
3.3.19	□ способами организации защиты информации.
3.3.20	□ способами организации контроля защиты информации на объекте.
3.3.21	□ Навыками проведения анализа безопасности АС и разработки политики информационной безопасности АС
3.3.22	□ Навыками оценки эффективности системы управления информационной безопасностью АС и определения направление ее совершенствования
3.3.23	□ Навыками анализа и оценки рисков информационной безопасности
3.3.24	□ Навыками контроля эффективности принятых мер по реализации частных политик информационной безопасности
3.3.25	□ Навыками разработки компонентов программного обеспечения компьютерных систем в интегрированных средах разработки программ
3.3.26	□ Навыками разработки и реализации на языках программирования высокого уровня алгоритмов решения типовых профессиональных задач
3.3.27	□ Навыками планирования разработки программ на языках общего назначения, обоснованного выбора инструментария программирования
3.3.28	□ Навыками применения методов и инструментальных средств программирования для решения профессиональных задач
3.3.29	□ обоснованием необходимости защиты информации в автоматизированных системах на основе научных иссле-дований
3.3.30	□ Навыками формулирования и согласования требований к компьютерным моделям систем
3.3.31	□ методами участия в инновационных проектах, посвященных исследованию математических моделей безопасности компьютерных систем
3.3.32	□ навыками работы с научно-технической литературой в области информационных технологий и защиты информации
3.3.33	□ Навыками разработки, отладки и эксплуатации программ реализации вычислительного эксперимента, навыками проверки генераторов псевдослучайных чисел с заданными законами распределения
3.3.34	□ Навыками планирования и проведения вычислительного эксперимента, сбора, обработки и анализа результатов исследований
3.3.35	□ навыками работы формировать требования по обеспечению информацион-ной безопасности объектов обеспечения информационной безопасности, адекватные ак-туальным угрозам их инфор-мационной безопасности
3.3.36	□ Навыками использования основ теории информации, теории сигналов, каналов связи и источников сообщений
3.3.37	□ Навыками решения задач профессиональной деятельности с учетом современного состояния методов и средств защиты информации от утечки по техническим каналам
3.3.38	□ Навыками использования радиотехнических систем в вопросах технической защиты информации от утечки по техническим каналам
3.3.39	□ навыками объединения средств вычислительной техники в локальные и корпоративные сети
3.3.40	□ решением задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
3.3.41	□ навыками применения математического аппарата теории информации для решения научных, практических и исследовательских задач в профессиональной деятельности
3.3.42	□ методами и средствами инсталляции и администрирования сетевого программного обеспечения
3.3.43	□ Навыками использования средств защиты информации от утечки по техническим каналам
3.3.44	□ криптографической терминологией
3.3.45	□ навыками установки и настройки средств работы с электронной подписью
3.3.46	□ навыками применения криптографических средств с учетом требований нормативных и правовых актов по защите информации
3.3.47	□ Навыками выбора программно-аппаратных средств защиты информации для использования в составе автоматизированных систем
3.3.48	□ Навыками применения программно-аппаратных средств защиты информации для обеспечения безопасности информации в автоматизированных системах

3.3.49	□ навыками администрирования современных операционных систем
3.3.50	□ навыками восстановления работоспособности прикладного и системного программного обеспечения
3.3.51	□ навыками настройки встроенных средств защиты информации операционных систем и прикладных программ
3.3.52	□ навыками оценки характеристик основных типов программно-аппаратных средств защиты операционных систем, прикладных программ и данных.
3.3.53	□ навыками проектирования баз данных
3.3.54	□ навыками разработки, тестирования и отладки программ и запросов на языке SQL
3.3.55	□ использованием и настройкой средств защиты информации в компьютерных сетях
3.3.56	□ администрированием компьютерных сетей
3.3.57	□ контролем и поддержкой корректности и эффективности функционирования компьютерных сетей
3.3.58	□ Настройкой межсетевых экранов
3.3.59	□ навыками настройки современных СУБД в соответствии с заданной политикой безопасности
3.3.60	□ методами подготовки исходных данных для технико – экономического обоснования проектных решений
3.3.61	□ способами диагностики и тестирования систем защиты информации автоматизированных систем
3.3.62	□ методами проведения анализа уязвимостей систем защиты информации автоматизированных систем
3.3.63	□ навыками работы с техническими средствами защиты информации
3.3.64	□ Навыками применения языков программирования для разработки компонентов программного обеспечения
3.3.65	□ навыками классификации информационных систем
3.3.66	□ навыками работы с научно-технической литературой, нормативными и методическими документами в области создания объектов информатизации
3.3.67	□ терминологией в области проектирования информационных систем
3.3.68	□ навыками работы с эксплуатационной документацией на комплектующие изделия АСЗИ
3.3.69	□ Навыками определения информационной инфраструктуры и информационных ресурсов автоматизированных систем, подлежащие защите
3.3.70	□ Навыками выявления угроз безопасности автоматизированных систем в защищенном исполнении
3.3.71	□ Навыками поиска нормативной правовой информации, необходимой для формирования своей гражданской активности
3.3.72	□ навыками разработки модели угроз информационной безопасности автоматизированной системы.
3.3.73	□ навыками анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированной системы.
3.3.74	□ навыками работы формировать требования по обеспечению информацион-ной безопасности объектов обеспечения информационной безопасности, адекватные ак-туальным угрозам их инфор-мационной безопасности, и оценивать их полноту и не-противоречивость
3.3.75	□ навыками формировать оптимальный набор мер и средств обеспечения информационной безопасно-сти создания (развития) объ-ектов обеспечения информа-ционной безопасности, адек-ватных требованиям по обес-печению информационной безопасности; навыками по-иска и работы с документами в области обеспечения ин-формационной безопасности создания и эксплуатации АСЗИ
3.3.76	□ навыками работы с научно – технической литературой и ГОСТами в области компьютерной безопасности
3.3.77	□ навыками работы с нормативными и методическими документами в области защиты информации
3.3.78	□ навыками администрирования компьютерных сетей, систем баз данных и ОС
3.3.79	□ навыками работы с нормативными документами по определению требований о защите информации компьютерных систем
3.3.80	□ навыками работы с инструкциями на средства защиты информации
3.3.81	□ Навыками планирования разработки системного программного обеспечения
3.3.82	□ Навыками организации работы программистов в группе по разработке системного программного обеспечения
3.3.83	□ навыками работы с документацией на предприятии
3.3.84	□ современными информационными технологиями работы на проектами

4. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1. Заключительный этап					

1.1	Данный этап завершает практику и проводится в срок не позднее начала этапа "Подготовка к защите выпускной квалификационной работы". На этом этапе выполняются следующие работы: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. 3.3 Защита отчета по практике и получение зачета по практике (с оценкой). /Тема/	11	0			

1.2	До начала прохождения практики выполняются следующие работы: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 преддипломной 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 преддипломной 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 преддипломной практике; - требованиями, которые предъявляются к местам практики;- необходимая документация для заключения договора с предприятием о прохождении преддипломной 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. /ИФР/	11	731	ОПК-16.1-З ОПК-16.1-У ОПК-16.1-В ОПК-16.2-З ОПК-1.1-З ОПК-1.1-У ОПК-1.1-В ОПК-1.2-З ОПК-1.2-У ОПК-1.2-В ОПК-1.3-З ОПК-1.3-У ОПК-1.3-В ОПК-1.4-З ОПК-1.4-У ОПК-1.4-В 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-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-3.4-З ОПК-3.4-У ОПК-3.4-В ОПК-3.5-З ОПК-3.5-У ОПК-3.5-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В ОПК-4.3-З ОПК-4.3-У ОПК-4.3-В ОПК-5.1-З ОПК-5.1-У ОПК-5.1-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.3-З ОПК-5.3-У ОПК-5.3-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В ОПК-5.6-З ОПК-5.6-У ОПК-5.6-В ОПК-5.7-З ОПК-5.7-У ОПК-5.7-	Л1.1Л2.1	Отчет о выполнении задания

				В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.1-З ОПК-6.1-У ОПК-6.1-В ОПК-6.2-З ОПК-6.2-У ОПК-6.2-В ОПК-6.3-З ОПК-6.3-У ОПК-6.3-В ОПК-6.4-З ОПК-6.4-У ОПК-6.4-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-7.1-З ОПК-7.1-У ОПК-7.1-В ОПК-7.2-З ОПК-7.2-У ОПК-7.2-В ОПК-7.3-З ОПК-7.3-У ОПК-7.3-В ОПК-7.4-З ОПК-7.4-У ОПК-7.4-В ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.3-З ОПК-8.3-У ОПК-8.3-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-8.6-З ОПК-8.6-У ОПК-8.6-В ОПК-8.7-З ОПК-8.7-У ОПК-8.7-В ОПК-8.8-З ОПК-8.8-У ОПК-8.8-В ОПК-8.9-З ОПК-8.9-У ОПК-8.9-В ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-9.3-З ОПК-9.3-		

				У ОПК-9.3-В ОПК-9.4-З ОПК-9.4-У ОПК-9.4-В ОПК-9.5-З ОПК-9.5-У ОПК-9.5-В ОПК-9.6-З ОПК-9.6-У ОПК-9.6-В ОПК-9.7-З ОПК-9.7-У ОПК-9.7-В ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В ОПК-12.1-З ОПК-12.1-У ОПК-12.1-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В ОПК-12.4-З ОПК-12.4-У ОПК-12.4-В ОПК-12.5-З ОПК-12.5-У ОПК-12.5-В ОПК-12.6-З ОПК-12.6-У ОПК-12.6-В ОПК-12.7-З ОПК-12.7-У ОПК-12.7-В ОПК-12.8-З ОПК-12.8-У ОПК-12.8-В ОПК-12.9-З ОПК-12.9-У		

				ОПК-12.9-В ОПК-12.10-З ОПК-12.10-У ОПК-12.10-В ОПК-12.11-З ОПК-12.11-У ОПК-12.11-В ОПК-13.1-З ОПК-13.1-У ОПК-13.1-В ОПК-13.2-З ОПК-13.2-У ОПК-13.2-В ОПК-13.3-З ОПК-13.3-У ОПК-13.3-В ОПК-14.1-З ОПК-14.1-У ОПК-14.1-В ОПК-14.2-З ОПК-14.2-У ОПК-14.2-В ОПК-14.3-З ОПК-14.3-У ОПК-14.3-В ОПК-14.4-З ОПК-14.4-У ОПК-14.4-В ОПК-14.5-З ОПК-14.5-У ОПК-14.5-В ОПК-14.6-З ОПК-14.6-У ОПК-14.6-В ОПК-14.7-З ОПК-14.7-У ОПК-14.7-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-16.2-У ОПК-16.2-В ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-2.1-З		

				ПК-2.1-У ПК-2.1-В ПК-2.2-З ПК-2.2-У ПК-2.2-В ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-4.2-З ПК-4.2-У ПК-4.2-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.2-З ПК-5.2-У ПК-5.2-В ПК-5.3-З ПК-5.3-У ПК-5.3-В ОПК-15.1-В ОПК-14.2-З ОПК-16.1-З		

1.3	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/	11	14	ОПК-16.1-З ОПК-16.1-З ОПК-16.1-У ОПК-16.1-В ОПК-16.2-З ОПК-16.2-У ОПК-16.2-В ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-1.1-З ОПК-1.1-У ОПК-1.1-В ОПК-1.2-З ОПК-1.2-У ОПК-1.2-В ОПК-1.3-З ОПК-1.3-У ОПК-1.3-В ОПК-1.4-З ОПК-1.4-У ОПК-1.4-В 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-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В ОПК-3.4-З ОПК-3.4-У ОПК-3.4-В ОПК-3.5-З ОПК-3.5-У ОПК-3.5-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В ОПК-4.3-З ОПК-4.3-У ОПК-4.3-В ОПК-5.1-З ОПК-5.1-У ОПК-5.1-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.3-З ОПК-5.3-У ОПК-5.3-	Л1.1Л2.1	

				В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В ОПК-5.6-З ОПК-5.6-У ОПК-5.6-В ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.1-З ОПК-6.1-У ОПК-6.1-В ОПК-6.2-З ОПК-6.2-У ОПК-6.2-В ОПК-6.3-З ОПК-6.3-У ОПК-6.3-В ОПК-6.4-З ОПК-6.4-У ОПК-6.4-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-7.1-З ОПК-7.1-У ОПК-7.1-В ОПК-7.2-З ОПК-7.2-У ОПК-7.2-В ОПК-7.3-З ОПК-7.3-У ОПК-7.3-В ОПК-7.4-З ОПК-7.4-У ОПК-7.4-В ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.3-З ОПК-8.3-У ОПК-8.3-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-8.6-З ОПК-8.6-У ОПК-8.6-В ОПК-8.7-З ОПК-8.7-У ОПК-8.7-В ОПК-8.8-З ОПК-8.8-		

				У ОПК-8.8-В ОПК-8.9-З ОПК-8.9-У ОПК-8.9-В ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-9.3-З ОПК-9.3-У ОПК-9.3-В ОПК-9.4-З ОПК-9.4-У ОПК-9.4-В ОПК-9.5-З ОПК-9.5-У ОПК-9.5-В ОПК-9.6-З ОПК-9.6-У ОПК-9.6-В ОПК-9.7-З ОПК-9.7-У ОПК-9.7-В ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В ОПК-12.1-З ОПК-12.1-У ОПК-12.1-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В ОПК-12.4-З ОПК-12.4-У ОПК-12.4-В ОПК-12.5-З ОПК-12.5-У ОПК-12.5-В ОПК-12.6-З ОПК-12.6-У		

				ОПК-12.6-В ОПК-12.7-З ОПК-12.7-У ОПК-12.7-В ОПК-12.8-З ОПК-12.8-У ОПК-12.8-В ОПК-12.9-З ОПК-12.9-У ОПК-12.9-В ОПК-12.10-З ОПК-12.10-У ОПК-12.10-В ОПК-12.11-З ОПК-12.11-У ОПК-12.11-В ОПК-13.1-З ОПК-13.1-У ОПК-13.1-В ОПК-13.2-З ОПК-13.2-У ОПК-13.2-В ОПК-13.3-З ОПК-13.3-У ОПК-13.3-В ОПК-14.1-З ОПК-14.1-У ОПК-14.1-В ОПК-14.2-З ОПК-14.2-У ОПК-14.2-В ОПК-14.3-З ОПК-14.3-У ОПК-14.3-В ОПК-14.4-З ОПК-14.4-У ОПК-14.4-В ОПК-14.5-З ОПК-14.5-У ОПК-14.5-В ОПК-14.6-З ОПК-14.6-У ОПК-14.6-В ОПК-14.7-З ОПК-14.7-У ОПК-14.7-В ОПК-8.1..1-З ОПК-8.1..1-У ОПК-8.1..1-В ОПК-8.1..2		

				-З ОПК-8.1..2-У ОПК-8.1..2-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-В ОПК-8.2..3-З ОПК-8.2..3-У ОПК-8.2..3-В ОПК-8.3..1-З ОПК-8.3..1-У ОПК-8.3..1-В ОПК-8.3..2-З ОПК-8.3..2-У ОПК-8.3..2-В ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-2.2-З ПК-2.2-У ПК-2.2-В ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В ПК-4.1-З ПК-4.1-У ПК-4.1-В ПК-4.2-З ПК-4.2-У ПК-4.2-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ПК-5.1-З ПК-5.1-У		
1.4	Прием зачета /ИКР/	11	0,25	ОПК-16.1-З ОПК-15.1-В ОПК-14.2-З ОПК-16.1-З	Л1.1Л2.1	

1.5	/Кнс/	11	2	ОПК-16.1-З ОПК-15.1-З ОПК-15.1-У ОПК-15.1-В ОПК-15.2-З ОПК-15.2-У ОПК-15.2-В ОПК-14.1-З ОПК-14.1-У ОПК-14.1-В ОПК-14.2-З ОПК-14.2-У ОПК-14.2-В ОПК-14.3-З ОПК-14.3-У ОПК-14.3-В ОПК-13.1-З ОПК-13.1-У ОПК-13.1-В ОПК-13.2-З ОПК-13.2-У ОПК-13.2-В ОПК-13.3-З ОПК-13.3-У ОПК-13.3-В ОПК-12.1-З ОПК-12.1-У ОПК-12.1-В ОПК-12.2-З ОПК-12.2-У ОПК-12.2-В ОПК-12.3-З ОПК-12.3-У ОПК-12.3-В ОПК-11.1-З ОПК-11.1-У ОПК-11.1-В ОПК-11.2-З ОПК-11.2-У ОПК-11.2-В ОПК-10.1-З ОПК-10.1-У ОПК-10.1-В ОПК-10.2-З ОПК-10.2-У ОПК-10.2-В ОПК-9.1-З ОПК-9.1-У ОПК-9.1-В ОПК-9.2-З ОПК-9.2-У ОПК-9.2-В ОПК-9.3-	Л1.1Л2.1	

				З ОПК-9.3-У ОПК-9.3-В ОПК-8.1-З ОПК-8.1-У ОПК-8.1-В ОПК-8.2-З ОПК-8.2-У ОПК-8.2-В ОПК-8.3-З ОПК-8.3-У ОПК-8.3-В ОПК-7.1-З ОПК-7.1-У ОПК-7.1-В ОПК-7.2-З ОПК-7.2-У ОПК-7.2-В ОПК-7.3-З ОПК-7.3-У ОПК-7.3-В ОПК-5.1-З ОПК-5.1-У ОПК-5.1-В ОПК-5.2-З ОПК-5.2-У ОПК-5.2-В ОПК-5.3-З ОПК-5.3-У ОПК-5.3-В ОПК-4.1-З ОПК-4.1-У ОПК-4.1-В ОПК-4.2-З ОПК-4.2-У ОПК-4.2-В ОПК-4.3-З ОПК-4.3-У ОПК-4.3-В ОПК-3.1-З ОПК-3.1-У ОПК-3.1-В ОПК-3.2-З ОПК-3.2-У ОПК-3.2-В ОПК-3.3-З ОПК-3.3-У ОПК-3.3-В 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-1.1-З ОПК-1.1-У ОПК-1.1-В ОПК-1.2-З ОПК-1.2-У ОПК-1.2-В ОПК-1.3-З ОПК-1.3-У ОПК-1.3-В ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В		

				ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.1-З ПК-3.1-У ПК-3.1-В ПК-3.2-З ПК-3.2-У ПК-3.2-В ПК-4.2-З ПК-4.2-У ПК-4.2-В ПК-5.1-З ПК-5.1-У ПК-5.1-В ПК-5.2-З ПК-5.2-У ПК-5.2-В ОПК-1.4-З ОПК-1.4-У ОПК-1.4-В ОПК-3.4-У ОПК-3.4-З ОПК-3.4-В ОПК-3.5-З ОПК-3.5-У ОПК-3.5-В ОПК-5.4-З ОПК-5.4-У ОПК-5.4-В ОПК-5.5-З ОПК-5.5-У ОПК-5.5-В ОПК-5.7-З ОПК-5.7-У ОПК-5.7-В ОПК-5.8-З ОПК-5.8-У ОПК-5.8-В ОПК-6.5-З ОПК-6.5-У ОПК-6.5-В ОПК-6.6-З ОПК-6.6-У ОПК-6.6-В ОПК-7.4-З ОПК-7.4-У ОПК-7.4-В ОПК-8.4-З ОПК-8.4-У ОПК-8.4-В ОПК-8.5-З ОПК-8.5-У ОПК-8.5-В ОПК-8.6-З ОПК-8.6-У ОПК-8.6-В ОПК-8.7-З ОПК-8.7-У ОПК-8.7-В ОПК-8.8-З ОПК-8.8-У ОПК-8.8-В ОПК-8.9-З ОПК-8.9-У ОПК-8.9-В ОПК-9.4-З ОПК-9.4-У		

				ОПК-9.4-В ОПК-9.5-З ОПК-9.5-У ОПК-9.5-В ОПК-9.6-З ОПК-9.6-У ОПК-9.6-В ОПК-9.7-З ОПК-9.7-У ОПК-9.7-В ОПК-12.4-З ОПК-12.4-У ОПК-12.4-В ОПК-12.5-З ОПК-12.5-У ОПК-12.5-В ОПК-12.6-З ОПК-12.6-У ОПК-12.6-В ОПК-12.7-З ОПК-12.7-У ОПК-12.7-В ОПК-12.8-З ОПК-12.8-У ОПК-12.8-В ОПК-12.9-З ОПК-12.9-У ОПК-12.9-В ОПК-12.10-З ОПК-12.10-У ОПК-12.10-В ОПК-14.4-З ОПК-14.4-У ОПК-14.4-В ОПК-14.5-З ОПК-14.5-У ОПК-14.5-В ОПК-14.6-З ОПК-14.6-У ОПК-14.6-В ОПК-14.7-З ОПК-14.7-У ОПК-14.7-В ОПК-10.3-З ОПК-10.3-У ОПК-10.3-В ОПК-12.11-З ОПК-12.11-У ОПК-12.11-В ПК-4.3-З ПК-4.3-У ПК-4.3-В ОПК-16.1-З ОПК-16.1-У		

				ОПК-16.1-В ОПК-16.2-З ОПК-16.2-У ОПК-16.2-В		
1.6	/ЗаО/	11	8,75	ОПК-16.1-З ОПК-15.1-В ОПК-14.2-З ОПК-16.1-З	Л1.1Л2.1	Опрос. Сбор отчетов и отзывов. Анализ результатов.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРАКТИКИ

Оценочные материалы приведены в Приложении 1 к рабочей программе дисциплины (см. документ "Оценочные материалы по дисциплине "Преддипломная 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	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	Сухов В.Е., Фомина К.Ю.	Информатика : метод. указ. к лаб. работам	Рязань, 2015, 48с.	, 1

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
LibreOffice	Свободное ПО
VirtualBox	Свободное ПО
Chrome	Свободное ПО
7 Zip	Свободное ПО
VMware Player	Свободное ПО
Файловый менеджер FAR	Свободное ПО
Cisco Packet Tracer	Свободное ПО
Kaspersky Endpoint Security	Коммерческая лицензия
Microsoft Visio	Microsoft Imagine, номер подписки 700102019

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	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.

3	264 учебно-административный корпус. учебная аудитория для проведения учебных занятий Специализированная мебель (16 посадочных мест), 5 рабочих мест (стол), магнитно-маркерная доска.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПРАКТИКЕ

Методическое обеспечение дисциплины приведено в Приложении 2 к рабочей программе дисциплины (см. докумет "Методические указания дисциплины "Преддипломная практика").

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**29.09.23** 16:42 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**29.09.23** 16:42 (MSK)	Простая подпись
ПОДПИСАНО ПРОРЕКТОРОМ ПО УР	**ФГБОУ ВО "РГРТУ", РГРТУ,** Корячко Алексей Вячеславович, Проректор по учебной работе	**29.09.23** 17:22 (MSK)	Простая подпись