



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
Институт кибербезопасности и цифровых технологий

УТВЕРЖДАЮ

И.о. директора ИКБ

_____ Бакаев А.А.

«__» _____ 2025 г.

Рабочая программа практики
Производственная практика
Преддипломная практика

Читающее подразделение **кафедра КБ-1 «Защита информации»**
Специальность **10.05.03 Информационная безопасность**
Специализация **автоматизированных систем**
специализация N 8 "Разработка автоматизированных
систем в защищенном исполнении"
Квалификация **специалист по защите информации**
Форма обучения **очная**
Общая трудоемкость **15 з.е.**

Распределение часов дисциплины и форм промежуточной аттестации по семестрам

Семестр	Зачётные единицы	Распределение часов							Формы промежуточной аттестации
		Всего	Лекции	Лабораторные	Практические	Самостоятельная работа	Контактная работа в период практики и (или) аттестации	Контроль	
11	15	540	0	0	0	512,25	10	17,75	Зачет с оценкой
из них на практ. подготовку			0	0	0	256	0	0	

Программу составил(и):

канд. воен. наук, доцент, Федин Ф.О. _____

преподаватель, Метелев И.А. _____

Рабочая программа практики

Преддипломная практика

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

составлена на основании учебного плана:

специальность: 10.05.03 Информационная безопасность автоматизированных систем

специализация: «специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"»

Рабочая программа одобрена на заседании кафедры

кафедра КБ-1 «Защита информации»

Протокол от 23.01.2025 № 6

Зав. кафедрой Артемова С.В. _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
кафедра КБ-1 «Защита информации»

Протокол от _____ 2026 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
кафедра КБ-1 «Защита информации»

Протокол от _____ 2027 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
кафедра КБ-1 «Защита информации»

Протокол от _____ 2028 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры
кафедра КБ-1 «Защита информации»

Протокол от _____ 2029 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

1. ЦЕЛИ ОСВОЕНИЯ ПРАКТИКИ

«Преддипломная практика» имеет своей целью сформировать, закрепить и развить практические навыки и компетенции, предусмотренные данной рабочей программой в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем с учетом специфики специализации подготовки – «специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"».

Практическая подготовка при проведении практики организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация:	специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"
Блок:	Практика
Часть:	Обязательная часть
Общая трудоемкость:	15 з.е. (540 акад. час.).

3. ТИП, ВИД И СПОСОБ ПРОВЕДЕНИЯ ПРАКТИКИ

Вид практики:	Производственная практика
Тип практики:	Преддипломная практика

Способ (способы) проведения практики определяются в соответствии с федеральным государственным образовательным стандартом. В случае, если стандарт не регламентирует способ проведения практики, то она проводится стационарно.

4. МЕСТО И ВРЕМЯ ПРОВЕДЕНИЯ ПРАКТИКИ

«Преддипломная практика» специальности 10.05.03 Информационная безопасность автоматизированных систем проводится на базе структурных подразделений РТУ МИРЭА или в организации, осуществляющей деятельность по профилю соответствующей образовательной программы (далее - профильная организация), в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки, на основании договора, заключаемого между образовательной организацией и профильной организацией.

5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ

В результате освоения практики обучающийся должен овладеть компетенциями:

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

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

УК-9 - Способен принимать обоснованные экономические решения в различных областях жизнедеятельности

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

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

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

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-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-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-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;

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ, ХАРАКТЕРИЗУЮЩИЕ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

УК-1 : Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

УК-1.2 : Применяет системный подход для решения поставленных задач

Знать:

- знает нормативно-правовую базу в области управления информационной безопасностью автоматизированных систем в защищенном исполнении

Уметь:

- умеет анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ

Владеть:

- владеет терминологией и инструментальными средствами моделирования систем управления ИБ

УК-9 : Способен принимать обоснованные экономические решения в различных областях жизнедеятельности

УК-9.2 : Обосновывает экономические решения в различных областях жизнедеятельности

Знать:

- знает задачи оценки эффективности разработки автоматизированных информационных систем в защищенном исполнении

Уметь:

- умеет применять экономические знания по оценке эффективности разработки автоматизированных информационных систем в защищенном исполнении

Владеть:

- владеет умениями выполнять оценку эффективности создания автоматизированных информационных систем в защищенном исполнении

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 принципы работы современных информационных технологий

Знать:

- знает роль информации, в обеспечении информационной безопасности автоматизированных систем в защищенном исполнении

Уметь:

- умеет выполнять сравнительный анализ программных и программно-аппаратных средств защиты информации автоматизированных информационных систем в защищенном исполнении

Владеть:

- владеет умениями применять инструментальные средства защиты информации автоматизированных информационных систем в защищенном исполнении

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

ОПК-3.1 : Применяет математические методы для решения поставленных задач

Знать:

- знает основные математические методы и модели, применяемые для решения задач обеспечения информационной безопасности автоматизированных систем

Уметь:

- умеет применять и модифицировать математические методы и модели, применяемые для решения задач обеспечения информационной безопасности автоматизированных систем

Владеть:

- владеет умениями применять математические методы и модели для решения задач обеспечения информационной безопасности автоматизированных систем

ОПК-3.2 : Применяет математические методы для формализации задач профессиональной деятельности

Знать:

- возможности программных средств защиты информации автоматизированных систем в защищенном исполнении

Уметь:

- умеет использовать возможности программных средств защиты информации автоматизированных систем в защищенном исполнении

Владеть:

- владеет умениями применять программные средства защиты информации автоматизированных систем в защищенном исполнении

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 основные физические законы и модели для решения поставленных задач

Знать:

- законы электрической и магнитной природы

Уметь:

- использовать правильные формулы для вычисления задач

Владеть:

- навыками применения определенных законов физики для решения задач

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

ОПК-5.1 : Применяет нормативно-правовые акты, регламентирующие деятельность по защите информации

Знать:

- знает нормативно-правовую базу в области защиты информации автоматизированных информационных систем в защищенном исполнении

Уметь:

- умеет применять нормативно-правовую базу в области защиты информации автоматизированных информационных систем в защищенном исполнении

Владеть:

- владеет умениями, применения средства защиты информации опираясь на нормативно-правовую базу в области защиты информации автоматизированных информационных систем

ОПК-5.2 : Применяет нормативно-методические документы, регламентирующие деятельность по защите информации

Знать:

- знает правовой режим защиты информации автоматизированных систем в защищенном исполнении

Уметь:

- умеет обеспечивать правовой режим защиты информации автоматизированных систем в защищенном исполнении

Владеть:

- владеет методами обеспечения правового режима защиты информации автоматизированных систем в защищенном исполнении

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 : Участвует в организации защиты информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативно-правовыми актами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при решении профессиональных задач

Знать:

- знает нормативно-правовые акты, регулирующие защиту информации в автоматизированных системах

Уметь:

- умеет применять нормативно-правовую базу для защиты информации в автоматизированных системах

Владеть:

- владеет способами организации защиты информации в автоматизированных информационных системах

ОПК-6.2 : Участвует в организации защиты информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативно-методическими

документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при решении профессиональных задач

Знать:

- знает нормативные и методические документы ФСБ и ФСТЭК в области защиты информации автоматизированных систем

Уметь:

- умеет организовывать защиту информации в соответствии с требованиями нормативных и методических документов ФСБ и ФСТЭК в области защиты информации автоматизированных систем

Владеть:

- владеет умениями организовывать защиту информации в соответствии с требованиями нормативных и методических документов ФСБ и ФСТЭК в области защиты информации автоматизированных систем

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-7.2 : Выбирает, обосновывает и применяет методы и инструментальные средства программирования для решения профессиональных задач

Знать:

- знает методы и инструментальные средства программирования, применяемые для создания автоматизированных информационных систем в защищенном исполнении

Уметь:

- умеет осуществлять обоснованный выбор методов и средств программирования автоматизированных информационных систем в защищенном исполнении

Владеть:

- владеет инструментальными средствами программирования автоматизированных информационных систем в защищенном исполнении

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

ОПК-8.2 : Обосновывает полученные результаты и оформляет их с соблюдением основных требований

Знать:

- знает методы исследования предметной области в целях обоснования целесообразности создания автоматизированной системы в защищенном исполнении и формирования требования к этой системе, процессу её создания и эксплуатации

Уметь:

- умеет обосновывать целесообразность создания автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу её создания и эксплуатации

Владеть:

- владеет инструментальными средствами моделирования предметной области функционирования автоматизированных информационных систем в защищенном исполнении

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 защиты информации в операционных системах**Знать:**

- знает принципы работы технических средств защиты информации от утечки по техническим каналам

Уметь:

- умеет применять технические средства защиты информации от утечки по техническим каналам

Владеть:

- владеет умениями решать задачи защиты информации автоматизированных систем от утечки по техническим каналам

ОПК-9.2 : Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в компьютерных и телекоммуникационных сетях**Знать:**

- знает принципы работы программно-аппаратных средств защиты информации автоматизированных систем

Уметь:

- умеет применять программно-аппаратные средства защиты информации автоматизированных систем

Владеть:

- владеет умениями решать задачи защиты баз данных автоматизированных информационных систем

ОПК-13 : Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;**ОПК-13.2 : Проводит анализ уязвимостей систем защиты информации автоматизированных систем****Знать:**

- знает классификацию уязвимостей автоматизированных информационных систем

Уметь:

- умеет строить модель нарушителя и модель угроз информационной безопасности автоматизированных информационных систем

Владеть:

- владеет умениями проведения анализа уязвимостей автоматизированной информационной системы

В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ ОБУЧАЮЩИЙСЯ ДОЛЖЕН**Знать:**

- знает нормативно-правовую базу в области управления информационной безопасностью автоматизированных систем в защищенном исполнении
- знает нормативно-правовые акты, регулирующие защиту информации в автоматизированных системах
- знает нормативно-правовую базу в области защиты информации автоматизированных информационных систем в защищенном исполнении
- знает нормативные и методические документы ФСБ и ФСТЭК в области защиты информации автоматизированных систем
- законы электрической и магнитной природы

- знает методы и инструментальные средства программирования, применяемые для создания автоматизированных информационных систем в защищенном исполнении
- возможности программных средств защиты информации автоматизированных систем в защищенном исполнении
- знает основные математические методы и модели, применяемые для решения задач обеспечения информационной безопасности автоматизированных систем
- знает методы исследования предметной области в целях обоснования целесообразности создания автоматизированной системы в защищенном исполнении и формирования требования к этой системе, процессу её создания и эксплуатации
- знает принципы работы технических средств защиты информации от утечки по техническим каналам
- знает роль информации, в обеспечении информационной безопасности автоматизированных систем в защищенном исполнении
- знает принципы работы программно-аппаратных средств защиты информации автоматизированных систем
- знает задачи оценки эффективности разработки автоматизированных информационных систем в защищенном исполнении
- знает классификацию уязвимостей автоматизированных информационных систем
- знает правовой режим защиты информации автоматизированных систем в защищенном исполнении

Уметь:

- умеет строить модель нарушителя и модель угроз информационной безопасности автоматизированных информационных систем
- умеет осуществлять обоснованный выбор методов и средств программирования автоматизированных информационных систем в защищенном исполнении
- умеет применять технические средства защиты информации от утечки по техническим каналам
- умеет организовывать защиту информации в соответствии с требованиями нормативных и методических документов ФСБ и ФСТЭК в области защиты информации автоматизированных систем
- умеет применять нормативно-правовую базу для защиты информации в автоматизированных системах
- умеет применять программно-аппаратные средства защиты информации автоматизированных систем
- умеет обосновывать целесообразность создания автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу её создания и эксплуатации
- умеет обеспечивать правовой режим защиты информации автоматизированных систем в защищенном исполнении
- умеет применять и модифицировать математические методы и модели, применяемые для решения задач обеспечения информационной безопасности автоматизированных систем
- умеет применять нормативно-правовую базу в области защиты информации автоматизированных информационных систем в защищенном исполнении
- умеет анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ
- использовать правильные формулы для вычисления задач
- умеет применять экономические знания по оценке эффективности разработки автоматизированных информационных систем в защищенном исполнении
- умеет использовать возможности программных средств защиты информации автоматизированных систем в защищенном исполнении

- умеет выполнять сравнительный анализ программных и программно-аппаратных средств защиты информации автоматизированных информационных систем в защищенном исполнении

Владеть:

- владеет умениями решать задачи защиты баз данных автоматизированных информационных систем
- владеет терминологией и инструментальными средствами моделирования систем управления ИБ
- владеет умениями решать задачи защиты информации автоматизированных систем от утечки по техническим каналам
- владеет умениями выполнять оценку эффективности создания автоматизированных информационных систем в защищенном исполнении
- владеет инструментальными средствами моделирования предметной области функционирования автоматизированных информационных систем в защищенном исполнении
- владеет методами обеспечения правового режима защиты информации автоматизированных систем в защищенном исполнении
- владеет умениями, применения средства защиты информации опираясь на нормативно-правовую базу в области защиты информации автоматизированных информационных систем
- владеет инструментальными средствами программирования автоматизированных информационных систем в защищенном исполнении
- владеет умениями применять математические методы и модели для решения задач обеспечения информационной безопасности автоматизированных систем
- владеет умениями организовывать защиту информации в соответствии с требованиями нормативных и методических документов ФСБ и ФСТЭК в области защиты информации автоматизированных систем
- владеет умениями применять программные средства защиты информации автоматизированных систем в защищенном исполнении
- владеет способами организации защиты информации в автоматизированных информационных системах
- навыками применения определенных законов физики для решения задач
- владеет умениями применять инструментальные средства защиты информации автоматизированных информационных систем в защищенном исполнении
- владеет умениями проведения анализа уязвимостей автоматизированной информационной системы

6. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

При проведении учебных занятий организация обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений и лидерских качеств.

Код занятия	Наименование разделов и тем /вид занятия/	Сем.	Часов
1. Организационно-подготовительный раздел			
1.1	Инструктаж по требованиям техники безопасности и охране труда. Доведения порядка выполнения преддипломной практики. (КрПА). Инструктирование обучаемых	11	6
1.2	Организационное собрание (КрПА). Выдача заданий, знакомство с целью и основными этапами практики	11	3,75

2. Получение навыков практической деятельности, сбор материалов и формирование			
2.1	Выполнение заданий направленных на получение навыков практической подготовки (Ср). Этап сбора практических документальных материалов, этап практической деятельности и выполнение индивидуальных заданий	11	292,25 (из них 256 на практ. подг.)
2.2	Анализ информации и формирование отчёта по практической подготовке (Ср). Этап сбора обработки и анализа выявленной информации. Подведение итогов. Выводы. Составление отчета.	11	220
3. Промежуточная аттестация (зачёт с оценкой)			
3.1	Подготовка к сдаче промежуточной аттестации (ЗачётСОц).	11	17,75
3.2	Контактная работа с преподавателем в период промежуточной аттестации (КрПА).	11	0,25

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

7.1. Перечень компетенций

Перечень компетенций, на освоение которых направлена «Преддипломная практика», с указанием результатов их формирования в процессе освоения образовательной программы, представлен в п.3 настоящей рабочей программы

7.2. Типовые контрольные вопросы и задания

1. Особенности системного подхода к критическому анализу проблемных ситуаций и поиску достоверной информации в области обеспечения информационной безопасности автоматизированных систем в защищенном исполнении
2. Методы поиска достоверной информации для разрешения проблемных ситуаций в области обеспечения информационной безопасности автоматизированных систем в защищенном исполнении
3. Нормативно-правовая база в области управления информационной безопасностью автоматизированных систем в защищенном исполнении
4. Методы анализа текущего состояния информационной безопасности в организации с целью разработки требований к создаваемой автоматизированной системе в защищенном исполнении
5. Терминология и инструментальные средства моделирования систем управления информационной безопасностью автоматизированных систем в защищенном исполнении
6. Задачи оценки экономической эффективности создания автоматизированных информационных систем в защищенном исполнении
7. Способы оценки экономической эффективности создания автоматизированных информационных систем в защищенном исполнении
8. Роль информации и информационных технологий в обеспечении информационной безопасности автоматизированных систем в защищенном исполнении
9. Сравнительный анализ программных и программно-аппаратных средств защиты информации автоматизированных информационных систем в защищенном исполнении
10. Инструментальные средства моделирования систем защиты информации автоматизированных информационных систем в защищенном исполнении
11. Значение информации, информационных технологий в области обеспечения информационной безопасности автоматизированных систем в защищенном исполнении
12. Сравнительный анализ инструментальных средств проектирования и разработки автоматизированных систем в защищенном исполнении
13. Использование современных информационных технологий и методов поиска информации для решения практических задач обеспечения информационной безопасности автоматизированных систем в защищенном исполнении

14. Источники угроз информационной безопасности автоматизированных систем в защищенном исполнении
15. Классификация угроз информационной безопасности автоматизированных систем в защищенном исполнении
16. Классификация защищаемой в автоматизированных системах информации по видам тайны и степеням конфиденциальности
17. Оценка рисков нарушения информационной безопасности автоматизированных информационных систем в защищенном исполнении
18. Математические методы и модели, применяемые для решения задач обеспечения информационной безопасности автоматизированных систем в защищенном исполнении
19. Возможности программных средств защиты информации автоматизированных систем в защищенном исполнении
20. Возможности CASE-средств для построения моделей предметной области функционирования автоматизированных систем в защищенном исполнении
21. Нормативно-правовая база в области защиты информации автоматизированных информационных систем в защищенном исполнении
22. Правовой режим защиты информации автоматизированных систем в защищенном исполнении
23. Нормативные и методические документы ФСБ и ФСТЭК в области защиты информации автоматизированных систем
24. Организация защиты информации в соответствии с требованиями нормативных и методических документов ФСБ и ФСТЭК в области защиты информации автоматизированных систем
25. Методы и инструментальные средства программирования
26. Характеристика инструментальных средств программирования автоматизированных информационных систем в защищенном исполнении
27. Методы исследования предметной области в целях обоснования целесообразности создания автоматизированной системы в защищенном исполнении
28. Требования к автоматизированной системе в защищенном исполнении, процессу её создания и эксплуатации
29. Характеристика инструментальных средств моделирования предметной области функционирования автоматизированных информационных систем в защищенном исполнении
30. Принципы работы технических средств защиты информации от утечки по техническим каналам
31. Задачи защиты информации автоматизированных систем от утечки по техническим каналам
32. Принципы работы программно-аппаратных средств защиты информации автоматизированных систем
33. Классификация уязвимостей автоматизированных информационных систем
34. Модель угроз информационной безопасности автоматизированных информационных систем
35. Модель нарушителя информационной безопасности автоматизированных информационных систем

7.3. Фонд оценочных материалов

Полный перечень оценочных материалов представлен в приложении 1.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

Наименование помещения	Перечень основного оборудования
------------------------	---------------------------------

Компьютерный класс	Компьютерная техника с возможностью подключения к сети «Интернет», мультимедийное оборудование, специализированная мебель.
Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мультимедийное оборудование, специализированная мебель, наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации.
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.
Лаборатория защищенных автоматизированных систем	Аппаратно-программные средства управления доступом к данным, шифрования, средства дублирования и восстановления данных, средства мониторинга состояния автоматизированных систем, источники бесперебойного и аварийного питания, средства контроля и управления доступом в помещения, охранная и пожарная сигнализация, средства климатического контроля
Лаборатория автоматизированных систем в защищенном исполнении	Аппаратно-программные средства управления доступом к данным, средства криптографической защиты информации, средства дублирования и восстановления данных, средства мониторинга состояния автоматизированных систем, средства контроля и управления доступом в помещения
Лаборатория безопасности вычислительных сетей	Стенды для изучения проводных и беспроводных компьютерных сетей, включающие абонентские устройства, коммутаторы, маршрутизаторы, точки доступа, межсетевые экраны, системы обнаружения компьютерных атак, системы углубленной проверки сетевых пакетов и системы защиты от утечки данных, анализаторы кабельных сетей
Лаборатория безопасности сетей ЭВМ	Стенды для изучения проводных и беспроводных компьютерных сетей, включающие абонентские устройства, коммутаторы, маршрутизаторы, точки доступа, межсетевые экраны, системы обнаружения компьютерных атак, системы углубленной проверки сетевых пакетов и системы защиты от утечки данных, анализаторы кабельных сетей
Базы практики	Оборудование и технические средства обучения, позволяющем выполнять определенные виды работ, предусмотренные заданием на практику.

8.2. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Р7-Офис.

8.3. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

8.3.1. Основная литература

1. Нестеров С. А. Основы информационной безопасности [Электронный ресурс]: учебное пособие. - Санкт-Петербург: Лань, 2019. - 324 с. – Режим доступа: <https://e.lanbook.com/book/114688>
2. Тумбинская М. В., Петровский М. В. Комплексное обеспечение информационной безопасности на предприятии [Электронный ресурс]: учебник. - Санкт-Петербург: Лань, 2019. - 344 с. – Режим доступа: <https://e.lanbook.com/book/125739>
3. Гвоздева Т. В., Баллод Б. А. Проектирование информационных систем. Стандартизация [Электронный ресурс]: учебное пособие. - Санкт-Петербург: Лань, 2019. - 252 с. – Режим доступа: <https://e.lanbook.com/book/115515>

8.3.2. Дополнительная литература

1. [Электронный ресурс]: ?????? ? ????. ?????? ?? ?????????? ?????????????? ?????? . - : : , 2011. - 51 – Режим доступа: <https://lib.rucont.ru/efd/319654>
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: . - М.: Горячая линия- Телеком, 2006. - 544 с.
3. Романов О. А., Бабин С. А., Жданов С. Г. Организационное обеспечение информационной безопасности: . - М.: Академия, 2008. - 189 с.
4. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: Учеб. пособие. - М.: РИОР: ИНФРА-М, 2014. - 255 с.
5. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: . - М.: ИТК "Дашков и К", 2007. - 335 с.
6. Гребенюк Е. И., Гребенюк Н. А. Технические средства информатизации: . - М.: Академия, 2009. - 266 с.
7. Остапенко Г. А. Информационные операции и атаки в социотехнических системах: . - М.: Горячая линия- Телеком, 2007. - 134 с.
8. Лапина М. А., Марков Д. М., Гиш Т. А., Песков М. В., Меденец В. В. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум. специальность 10.05.03. (090303.65) – информационная безопасность автоматизированных систем. специализация «защищенные автоматизированные системы управления». квалификация: специалист. - Ставрополь: СКФУ, 2016. - 242 с. – Режим доступа: <https://e.lanbook.com/book/155111>
9. Ярочкин В. И. Информационная безопасность: . - М.: Академический Проект; Фонд "Мир", 2003. - 639 с.
10. Бородин И. Ф., Судник Ю. А. Автоматизация технологических процессов: . - М.: КолосС, 2007. - 344 с.
11. Кирюхина Т. Г., Членов А.Н. Технические средства безопасности: . - М.: НОУ "Такир", 2002. - 215 с.

8.4. РЕКОМЕНДУЕМЫЙ ПЕРЕЧЕНЬ СОВРЕМЕННЫХ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. Консультант Плюс [http:// www.consultant.ru](http://www.consultant.ru)
2. Информационно-правовой портал ГАРАНТ [http:// www.garant.ru](http://www.garant.ru)

8.5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ПРАКТИКИ

На первом организационном собрании необходимо ознакомить студентов с содержанием рабочей программы практики, с порядком и графиком прохождения практики.

В начале прохождения практики, на организационно-подготовительном этапе студентам необходимо:

- оформить задание на практику;
- пройти инструктаж по технике безопасности и противопожарной технике;
- ознакомиться с содержанием рабочей программы практики, правилами и

обязанностями практиканта на предприятии, структурой подразделений (рабочих мест) практики, режимом работы предприятия;

- ознакомиться со структурой заключительного отчета по практике.

За период прохождения производственной практики студент самостоятельно изучает документацию, связанную с будущей профессиональной деятельностью, учебную, справочную, нормативную и научно-техническую литературу по соответствующим разделам данной программы. Литература подбирается в библиотеке университета (включая доступ к ЭБС), публичных научно-технических библиотеках. Закрепление результатов практики осуществляется путем самостоятельной работы студентов с рекомендуемой литературой.

В ходе прохождения практики студент должен решить все поставленные перед ним задачи и написать отчет о своей деятельности в рамках практики, а также выполненные работы (трудовые действия, трудовые функции), связанные с будущей профессиональной деятельностью обучающегося. В отчете должны быть описаны все основные этапы прохождения практики в соответствии с заданием. Окончательно оформленный и подписанный студентом отчет сдается руководителю практики не позже, чем за 3 дня до защиты. В указанное руководителем практики время студент обязан явиться на кафедру для защиты отчета.

8.6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБУЧЕНИЮ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

Освоение практики обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Медиа материалы также следует использовать и адаптировать с учетом индивидуальных особенностей обучения лиц с ОВЗ.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.