Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 16.06.2026 09:40:21
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационных технологий»
_____ / Д.Г. Демидов /
«26» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Преддипломная практика»

Направление подготовки
10.04.01 «Информационная безопасность»

Профиль/специализация
«Системы управления информационной безопасностью»»

Образовательная программа (профиль)
«Системы управления информационной безопасностью»

Квалификация
Магистр

Форма обучения
Очная

Москва 2026 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

Согласовано:
Заведующий кафедрой «Информационная безопасность»  И.В.Калуцкий

Руководитель образовательной программы
Доцент. к.т.н.  /С.А. Кесель/

Содержание

1. Цели, задачи и планируемые результаты прохождения практики 4
2. Место практики в структуре образовательной программы 10
3. Характеристика практики 10
4. Структура и содержание практики 10
5. Учебно-методическое и информационное обеспечение 11
5.1 Нормативные документы и ГОСТы 11
5.2 Основная литература 12
5.3 Дополнительная литература 12
5.4 Электронные образовательные ресурсы 13
5.5 Лицензионное и свободно распространяемое программное обеспечение 13
5.6 Современные профессиональные базы данных и информационные справочные системы 13
6. Материально-техническое обеспечение 13
8. Фонд оценочных средств 14
8.1 Методы контроля и оценивания результатов прохождения практики 14
8.2 Шкала и критерии оценивания результатов прохождения практики 14
8.3 Оценочные средства 14

1. Цели, задачи и планируемые результаты прохождения практики

К **основным целям** освоения преддипломной практики следует отнести:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла и дисциплин специализации;
- приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника.

К **основным задачам** освоения преддипломной практики следует отнести:

- ознакомление с должностными обязанностями сотрудников организации по профилю подготовки;
- освоение способов комплексного применения средств обеспечения информационной безопасности объекта защиты и оценки эффективности принимаемых мер.

Компетенции обучающегося, формируемые в результате прохождения практики

В результате освоения преддипломной практики у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Код и содержание индикатора достижения компетенции
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1. Анализирует проблемную ситуацию как систему, осуществляет её декомпозицию и определяет связи между ее составляющими. ИУК-1.2. Определяет противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивает релевантность используемых информационных источников. ИУК-1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	ИУК-2.1. Разрабатывает концепцию управления проектом на всех этапах его жизненного цикла в рамках обозначенной проблемы: формулирует цель и пути достижения, задачи и способы их решения, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения. ИУК-2.2. Разрабатывает план реализации проекта в соответствии с существующими условиями, необходимыми ресурсами, возможными рисками и распределением зон ответственности участников проекта. ИУК-2.3. Осуществляет мониторинг реализации проекта на всех этапах его жизненного цикла, вносит необходимые изменения в план реализации проекта с учетом количественных и качественных параметров достигнутых промежуточных результатов.

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.1. Демонстрирует управленческую компетентность, необходимую для формирования команды и руководства ее работой на основе разработанной стратегии сотрудничества. ИУК-3.2. Планирует, организует, мотивирует, оценивает и корректирует совместную деятельность по достижению поставленной цели с учетом интересов, особенностей поведения и мнений ее членов. ИУК-3.3. Применяет способы, методы и стратегии оптимизации социально психологического климата в коллективе, предупреждения и разрешения конфликтов, технологии обучения и развития профессиональной и коммуникативной компетентности членов команды
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	ИУК-4.1. Устанавливает и развивает профессиональные контакты, осуществляет академическое и профессиональное взаимодействие с применением современных коммуникативных технологий, в том числе на иностранном языке. ИУК-4.2. Составляет и редактирует документацию с целью обеспечения академического и профессионального взаимодействия, в том числе на иностранном языке. ИУК-4.3. Демонстрирует коммуникативную компетентность в условиях научно-исследовательской и проектной деятельности и презентации ее результатов на различных публичных мероприятиях, включая международные, в том числе на иностранном языке
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания. ИУК-6.2. Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям. ИУК-6.3. Выстраивает собственную профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда.
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Умеет: обосновывать требования к системе обеспечения информационной безопасности; разрабатывать проект технического задания на ее создание
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.1. Умеет: разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности
ОПК-3. Способен разрабатывать проекты организационно – распорядительных документов по обеспечению информационной безопасности	ИОПК-3.1 Умеет: разрабатывать проекты организационно- распорядительных документов по обеспечению информационной безопасности
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ИОПК-4.1. Умеет: осуществлять сбор, обработку и анализ научно— технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.
ОПК-5. Способен проводить научные исследования,	ИОПК-5.1. Умеет:

включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно—технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ИПК-1.1. Применяет знания направлений развития информационных технологий, основных видов политик безопасности объектов защиты; ИПК-1.2. Умеет прогнозировать эффективность функционирования, оценивать затраты и риски объектов защиты; ИПК-1.3. Владеет навыками формирования политики безопасности объектов защиты
ПК-2. Способен разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	ИПК-2.1. Знает методы концептуального проектирования технологий обеспечения информационной безопасности; ИПК-2.2. Умеет применять методы разработки систем, комплексов, средств и технологий обеспечения информационной безопасности; ИПК-2.3. Владеет навыками разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;
ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	ИПК-3.1. Знает: отечественные и международные стандарты информационной безопасности; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные методы и средства обеспечения безопасности операционных систем; основные методы и средства обеспечения сетевой безопасности; основные методы и средства обеспечения безопасности в системах управления базами данных. ИПК-3.2. Умеет: обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. ИПК-3.3. Владеет: навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем
ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ИПК-4.1. Знает: программы и методики испытаний средств и систем обеспечения информационной безопасности в соответствии с нормативными актами. ИПК-4.2. Умеет: разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности

	ИПК-4.3. Владеет: навыками проведения испытаний средств и систем обеспечения информационной безопасности
ПК-5. Способен анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	ИПК-5.1. Знает: фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества. ИПК-5.2. Умеет: анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества. ИПК-5.3. Владеет: навыками анализа фундаментальных и прикладных проблемы информационной безопасности
ПК-6. Способен осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	ИПК-6.1. Знает: методы и средства сбора, обработки, анализа и систематизации научно-технической информации по теме исследования для решения задач ИПК-6.2. Умеет: осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок. ИПК-6.3. Владеет методами и средствами сбора, обработки, анализа и систематизации научно-технической информации по теме исследования для решения задач, планами и программами проведения научных исследований и технических разработок
ПК-7. Способен проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ИПК-7.1. Знает: методы экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. ИПК-7.2. Умеет: проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента. ИПК-7.3. Владеет: навыками проведения экспериментальных исследований защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.
ПК-8. Способен обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ИПК-8.1. Знает: методы экспериментальных исследований. ИПК-8.2. Умеет: применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; готовить по результатам выполненных исследований научные доклады и статьи ИПК-8.3. Владеет: навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации

ПК-9. Способен проводить аудит информационной безопасности информационных систем и объектов информатизации	ИПК-9.1. Знает: каналы утечки информации. ИПК-9.2. Умеет проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации. ИПК-9.3. Владеет: методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем и объектов информатизации.
ПК-10. Способен проводить аттестацию объектов информатизации по требованиям безопасности информации	ИПК-10.1. Знает: возможности технических средств перехвата информации. ИПК-10.2. Умеет: проводить экспериментально исследовательские работы при аттестации объектов информатизации с учетом нормативных документов по защите информации. ИПК-10.3. Владеет: навыками проведения экспериментально исследовательских работ при аттестации объектов информатизации с учетом нормативных документов по защите информации
ПК-11. Способен проводить занятия по предметной области данного направления и разрабатывать методические материалы	ИПК-11.1. Знает: структуру и состав методических материалов, используемые в образовательной деятельности. ИПК-11.2. Умеет: проводить занятия по избранным дисциплинам предметной области данного направления. ИПК-11.3. Владеет: навыками разработки методических материалы, используемых в образовательной деятельности
ПК-12. Способен организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	ИПК-12.1. Знает: основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения; - проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно технических решений, реализованных при построении ЭВМ и систем; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. ИПК-12.2. Умеет: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей;

	- контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем. ИПК-12.3. Владеет: - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные системы.
ПК-13. Способен организовать управление информационной безопасностью	ИПК-13.1. Знает: - современные подходы к управлению ИБ и направлениям их развития; - основные стандарты, регламентирующие управление ИБ; - принципы построения СУИБ; - принципы разработки процессов управления ИБ; - взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; - подходы к интеграции СУИБ в общую систему управления предприятием. ИПК-13.2. Умеет: - анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; - применять процессный подход к управлению ИБ в различных сферах деятельности; - используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; - практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. ИПК-13.3. Владеет: - навыками управления информационной безопасностью простых объектов; - терминологией и процессным подходом построения систем управления ИБ;

	- навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и систем процессов в целом
ПК-14. Способен организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ИПК-14.1. Знает: правовые нормативные актами и нормативными методическими документами ФСБ России, ФСТЭК России. ИПК-14.2. Умеет: организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности. ИПК-14.3. Владеет: навыками управления организации работ по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности.
ПК-15. Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	ИПК-15.1. Знает методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности ИПК-15.2. Умеет: Организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности ИПК-15.3. Владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

2. Место практики в структуре образовательной программы

Преддипломная практика относится к базовой части блока 2 «Практики, в том числе, научно-исследовательская работа (НИР)» основной образовательной программы.

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

3. Характеристика практики

Тип и вид практики – преддипломная, стационарная.

Способ и форма проведения практики – непрерывно.

Практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика проводится в 10 семестре на базе предприятий требуемого профиля (8 недель).

4. Структура и содержание практики

Общая трудоемкость практики составляет 9 зачетных единиц, 324 часа в 4 семестре.

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов и трудоемкость (в зачетных единицах, часах)			Формы текущего контроля
		Виды работ	ЗЕ	Час	
1	Структура, история и традиции организации	Структура, история и традиции организации. Нормативные документы, регламентирующие деятельность организации. Основные обязанности должностных лиц организации по профилю подготовки.	1	36	Раздел отчета
2	Основные технологические процессы	Основные технологические процессы и производственное оборудование по профилю деятельности.	2	72	Раздел отчета
3	Стандарты и условия	Действующие стандарты, технические условия, положения и инструкции по эксплуатации аппаратных и программных средств, используемых по профилю деятельности.	2	72	Раздел отчета
4	Технологии защиты информации на предприятии	Функциональные обязанности сотрудника организации по должности, определенной на период практики. Технологии применения программных и аппаратных средств организации для решения профессиональных задач.	2	72	Раздел отчета
5	Методики защиты информации	Методики применения измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.	2	72	Раздел отчета

5. Учебно-методическое и информационное обеспечение

5.1 Нормативные документы и ГОСТы

1. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)
2. ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».
3. ГОСТ Р ИСО/МЭК 27005-2010 Национальный стандарт российской федерации информационная технология методы и средства обеспечения безопасности менеджмент риска информационной безопасности
4. "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"
5. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»
6. Федеральный государственный образовательный стандарт (ФГОС) высшего образования по направлению подготовки 10.04.01 — «Информатика и

вычислительная техника», уровень высшего образования — магистратура.
7. 06.032 Специалист по безопасности компьютерных систем и сетей
8. 06.033 Специалист по защите информации в автоматизированных системах
9. ГОСТ 7.32-2001 (Отчет о научно-исследовательской работе);
10. ГОСТ Р 7.05-2008 (Библиографическая ссылка);
11. ГОСТ 7.1-2003 (Библиографическая запись. Библиографическое описание. Общие требования и правила составления).

5.2 Основная литература

1. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. N 17.

2. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703
3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания : учебное пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. — Ростов-на-Дону : ИУБиП, 2020. — 114 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/248747
4. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401
5. Потерпеев, Г. Ю. Безопасность операционных систем : учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва : РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182416

5.3 Дополнительная литература

1. Комплексное обеспечение информационной безопасности на предприятии: учебник [Электронный ресурс]:
   Тумбинская М. В., Петровский М. В.
   Издательство «Лань» https://e.lanbook.com/book/207095
2. Организационно-правовое обеспечение информационной безопасности: учебник [Электронный ресурс]:
   Стрельцов А. А., Пожарский В. Н., Минаев В. А., Тарапанова Е. А., Фролов Д. Б., Скрыль С. В., Сычев А. М., Коробец Б. Н., Вайц Е. В., Грачёва Ю. В.
   МГТУ им. Баумана. Золотая коллекция https://e.lanbook.com/book/172840
3. Право интеллектуальной собственности [Электронный ресурс]:
   Новосёлова Л.А.
   Издательство «СТАТУТ» https://e.lanbook.com/book/113594
4. Управление интеллектуальной собственностью: создание и коммерциализация: Учебно-методическое пособие [Электронный ресурс]:
   Остапенко Г. Ф., Остапенко В. Д.

Пермский национальный исследовательский политехнический университет
https://e.lanbook.com/book/161117
5. Основы информационной безопасности [Электронный ресурс]:
Галатенко В.А.
Национальный Открытый Университет «ИНТУИТ» https://e.lanbook.com/book/100295
6. Основы информационной безопасности: Учебное пособие [Электронный ресурс]:
Поляков Е.А.
Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского https://e.lanbook.com/book/282890
7. Методы и средства защиты информации [Электронный ресурс]:
Киреева Н. В., Крыжановский А. В., Чупахина Л. Р., Караулова О. А.
Поволжский государственный университет телекоммуникаций и информатики
https://e.lanbook.com/book/255449
8. Системная и программная инженерия [Электронный ресурс]:
Батоврин В.К.
Издательство «ДМК Пресс» https://e.lanbook.com/book/1097
9. Информационные технологии в управлении качеством и защита информации [Электронный ресурс]:
Годенова Е.Г.
Томский государственный университет систем управления и радиоэлектроники
https://e.lanbook.com/book/11676

5.4 Электронные образовательные ресурсы

1. ЭОР разрабатывается
2. Научно-образовательный кластер CLAIM (it-claim.ru.)
3. ЭБС Лань (lanbook.com)
4. Образовательная платформа Юрайт. Для вузов и ссузов. (urait.ru)

5.5 Лицензионное и свободно распространяемое программное обеспечение

Определяется предприятием

5.6 Современные профессиональные базы данных и информационные справочные системы

Определяется предприятием

6. Материально-техническое обеспечение

Материально-техническое обеспечение практики определяется предприятием.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО по направлению подготовки 10.04.01 «Информационная безопасность».

7. Методические рекомендации

7.1 Учебно-методическое обеспечение самостоятельной работы студентов на практике

Контрольные вопросы и задания для проведения аттестации по итогам практики

1. Структура, история и традиции организации.
2. Нормативные документы, регламентирующие деятельность организации.
3. Основные обязанности должностных лиц организации по профилю подготовки.
4. Основные технологические процессы.
5. Производственное оборудование по профилю деятельности.
6. Действующие стандарты, технические условия, положения и инструкции по эксплуатации аппаратных и программных средств, используемых по профилю деятельности.
7. Функциональные обязанности сотрудника организации по должности, определенной на период практики.
8. Технологии применения программных и аппаратных средств организации для решения профессиональных задач.
9. Методики применения измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.

7.2 Методические указания для обучающихся по освоению дисциплины

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций, закрепленных за производственной практикой по получению профессиональных умений и профессионального опыта, осуществляется в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение практики на месте ее проведения руководителем практики от предприятия.

8. Фонд оценочных средств

8.1 Методы контроля и оценивания результатов прохождения практики

В качестве основной формы отчетности является письменный отчет. Форма контроля прохождения практики - дифференцированный зачет.

8.2 Шкала и критерии оценивания результатов прохождения практики

По окончании практики студент-практикант составляет письменный отчет и в порядке, установленном кафедрой, сдает его и другие отчетные материалы, предусмотренные методическими указаниями кафедры к прохождению практики, подписанные руководителем практики от организации.

Отчет должен содержать сведения о конкретно выполненной студентом работе в период прохождения практики.

При оценке итогов работы студента принимается во внимание характеристика, данная ему руководителем практики от предприятия.