МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Производственная практика (преддипломная)

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
аудиторные занятия 4,25
самостоятельная работа 211,75

Виды контроля в семестрах:
зачеты 10

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель				
Вид занятий	УП	РП	УП	РП
Лекции	4	4	4	4
Иные виды контактной работы	0,25	0,25	0,25	0,25
Итого ауд.	4,25	4,25	4,25	4,25
Контактная работа	4,25	4,25	4,25	4,25
Сам. работа	211,75	211,75	211,75	211,75
Итого	216	216	216	216

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целями преддипломной практики являются:
1.2	- закрепление и конкретизация результатов теоретического обучения;
1.3	- приобретение студентами умений и навыков самостоятельной практической работы по направлению "Информационная безопасность";
1.4	- получение студентами практических навыков выполнения мероприятий по организационной, правовой и технической защите информации, овладение методами работы с техническими и программно-аппаратными средствами защиты информации;
1.5	- развитие у студентов навыков проведения анализа деятельности предприятий и организаций по усовершенствованию их работы;
1.6	- подготовка выпускной квалификационной работы.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Физическая культура и спорт
2.1.2	Философия
2.1.3	Защита информации в сети Интернет
2.1.4	Экономика
2.1.5	Автоматизированные системы управления
2.1.6	Электромагнитные поля и волны
2.1.7	Общая физика
2.1.8	Производственная практика (научно-исследовательская работа)
2.1.9	Производственная практика (технологическая)
2.1.10	Производственная практика (эксплуатационная)
2.1.11	Биометрические технологии контроля доступа
2.1.12	Практикум по решению эксплуатационных задач профессиональной деятельности
2.1.13	Практикум по решению проектных задач профессиональной деятельности
2.1.14	Цифровая обработка сигналов в системах обеспечения информационной безопасности автоматизированных систем управления
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Технологии защиты информации в различных отраслях деятельности
2.2.2	Защита электронного документооборта

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	
Знать:	
Уровень 1	Условия и ограничения успешного выполнения порученной работы на основе собственных личностных, ситуативных, профессиональных качеств и возможности их совершенствования
Уровень 2	Основы эффективного использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата;
Уровень 3	инструменты и методы управления временем при выполнении конкретных задач, выстраивания траектории собственного профессионального роста
Уметь:	
Уровень 1	Применять знания о своих ресурсах и их пределах (личностных, ситуативных, временных и т.д.), для успешного выполнения порученной работы;
Уровень 2	Определять приоритеты собственной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда;
Уровень 3	Проводить оценку современных требований рынка труда для выстраивания траектории собственного профессионального развития
Владеть:	
Уровень 1	информацией о потребностях рынка труда в образовательных услугах для выстраивания траектории собственного профессионального развития
Уровень 2	навыками реализации намеченных целей деятельности с учетом условий, средств, личностных

	возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда
Уровень 3	Способами оценки эффективности использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата

ПК-1: Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	
Знать:	
Уровень 1	методы проведения физических исследований, технические и программные средства, применяемые при анализе электромагнитных полей и волн; уравнения и законы электродинамики и распространения радиоволн; модели элементарных излучателей; основные типы антенн, применяемых при анализе электромагнитных полей; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов;
Уровень 2	назначение, функции и структуру информационных и библиографических систем; методы поиска, изучения и обобщения научно-технической литературы, нормативных и методических материалов; основные методы исследования по теме своей научно- исследовательской работы; основы теории цифровой обработки сигналов как теоретической базы для разработки и исследования методов обработки, приема и передачи данных в системах обеспечения информационной безопасности автоматизированных систем управления; актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности; цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ
Уровень 3	состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления; области задач организации информационных технологий и современные инструменты построения интеллектуальных систем, обеспечивающих информационную безопасность; основные принципы и проблематику теории обучения машин, основные современные методы обучении по прецедентам — классификации, кластеризации и регрессии; принципы организации информационных систем в соответствии с требованиями по защите информации; основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона - Фано и Хаффмана); уязвимости современных АСУ ТП, подходы к устранению уязвимостей и построению системы защиты современных АСУ ТП; основные виды математических моделей информационных потоков и систем защиты информации и методы их построения
Уметь:	
Уровень 1	использовать методы проведения физических исследований, технические и программные средства для анализа электромагнитных полей технических средств автоматизированных систем; использовать методы исследования электромагнитных полей для оценки физических характеристик технических средств автоматизированных систем; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; определять параметры информационной системы и ее структуру в соответствии с заданными функциями;
Уровень 2	составлять обзоры по вопросам обеспечения информационной безопасности по теме своей научно-исследовательской работы; применять методы исследования по теме своей научно-исследовательской работы; формировать математическое описание дискретных систем в виде алгоритмов; выполнять компьютерное моделирование дискретных систем на основе их математического описания; анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации; анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации; формулировать основные задачи, возникающие при анализе данных, пути их решения, выбирать адекватные алгоритмы решения задачи анализа данных, оценивать качество получаемых решений, обеспечивающих информационную безопасность;
Уровень 3	формализовать постановки прикладных задач анализа данных, применять основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование; оценивать информационные риски в информационных системах; решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей;

	анализировать структуры АСУ ТП, строить их модели, оценивать риски функциональной безопасности, распознавать атаки социальной инженерии; на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ
Владеть:	
Уровень 1	навыком применения методик исследования электромагнитных полей; навыком применения исследовательских методов электродинамики и распространения радиоволн; навыками поиска и изучения научно-технической литературы, а также изложения и оформления результатов своей научно-исследовательской работы; навыком составления математических моделей дискретных систем и сигналов;
Уровень 2	навыком разработки алгоритмов цифровой обработки сигналов в системах информационной безопасности; навыком выбора методов проведения и обработки экспериментальных исследований, оформления научно-технических отчётов, обзоров, докладов, статей; навыком выбора и обоснованием критериев эффективности функционирования защищенных информационных систем
Уровень 3	навыком применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ; навыком разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети; навыком применения математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности

ПК-2: Способен разрабатывать проектные решения по защите информации в автоматизированных системах	
Знать:	
Уровень 1	основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; основные алгоритмы при цифровой обработке сигналов, факторы, определяющие связь эксплуатационных свойств систем цифровой обработки сигналов с их техническими характеристиками; цели и задачи проектирования систем инженерно-технической защиты объектов; основные понятия и терминологию, принятые в проектировании систем инженерно-технической защиты объектов
Уровень 2	основные принципы проектирования систем инженерно-технической защиты объектов; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование
Уровень 3	базовые алгоритмы анализа данных: k-средних, метод опорных векторов, линейная регрессия, ассоциативные правила, деревья решений, анализ выбросов или анализ аномалий, искусственные нейронные сети; меры, операции и приемы, направленные на предотвращение утечки защищаемой информации, несанкционированного и непреднамеренного воздействия на защищаемую информацию в сферах федерального, регионального управления и электронной коммерции; основные этапы реализации проектных решений в области автоматизированных систем электронного документооборота
Уметь:	
Уровень 1	определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; обоснованно оценивать необходимые параметры дискретизации и квантования, интерполяции и децимации сигналов; объяснять принцип методов оценки параметров сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления; изучать научно-техническую информацию, отечественный и зарубежный опыт и организовывать работы по практическому использованию новых технологий в области цифровой обработки сигналов
Уровень 2	проводить анализ вероятных угроз охраняемому объекту; выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту; выбирать технические средства для решения задачи охраны объекта; определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации; реализовывать в виде программного кода базовые алгоритмы анализа данных: k- средних, метод опорных векторов, линейная регрессия, ассоциативные правила, искусственные нейронные сети
Уровень 3	*
Владеть:	
Уровень 1	навыком применения типовых прикладных пакетов для синтеза алгоритмов цифровой обработки сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления; навыком разработки проектов нормативных документов, регламентирующих работу по защите информации

Уровень 2	навыком разработки алгоритмов интеллектуального анализа данных в системах информационной безопасности; навыком разработки предложений по совершенствованию систем информационной безопасности предприятий и организаций, комплексно обеспечивающих повышение ее уровня
Уровень 3	навыком разработки и анализом проектных решений в области автоматизированных систем электронного документооборота

ПК-4: Способен разрабатывать организационно-распорядительные документы и внедрять организационные меры по защите информации в автоматизированных системах	
Знать:	
Уровень 1	правовые основы организации защиты государственной тайны и/или конфиденциальной информации; задачи органов защиты государственной тайны и/или служб защиты информации на предприятии; свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления;
Уровень 2	задачи органов защиты информации на предприятиях; действующие нормативные и методические документы по оформлению рабочей технической документации; понятие и виды террористической деятельности, основы государственной политики Российской Федерации по противодействию терроризму в информационной сфере; нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности значимых объектов критической информационной инфраструктуры;
Уровень 3	категории и характеристики значимых объектов критической информационной инфраструктуры; способы выявления угроз информационной безопасности значимых объектов критической информационной инфраструктуры; нормативные документы Российской федерации в области кибербезопасности; особенности организации подразделения центра управления инцидентами (ЦУИ ИБ) для поддержки информационной безопасности промышленной сети; основы правового обеспечения и основные нормативные правовые акты в области защиты информации в различных отраслях деятельности; организацию работы специалистов с документами в автоматизированных системах электронного документооборота
Уметь:	
Уровень 1	анализировать правовые акты и осуществлять правовую оценку информации, циркулирующей в автоматизированной системе; квалифицированно исследовать состав документации предприятия (организации);
Уровень 2	разрабатывать проекты нормативных и организационно -распорядительных документов, регламентирующих работу по защите информации; реализовывать с учетом особенностей функционирования систем управления значимых объектов критической информационной инфраструктуры требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам противодействия террористической деятельности
Уровень 3	разрабатывать предложения по совершенствованию организационно- распорядительных документов по безопасности значимых объектов и представлять их руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу); применять средства юридической защиты информации ограниченного доступа; определять задачи по разработке требований к автоматизированным системам обработки и хранения электронных документов
Владеть:	
Уровень 1	навыком разработки организационно- распорядительных документов по защите информации в автоматизированных системах; навыком формирования требований по защите информации
Уровень 2	навыком применения современной нормативной базы для построения системы организационных и программно -технических мер по выявлению, предупреждению и пресечению террористической деятельности в отношении систем управления значимых объектов критической информационной инфраструктуры
Уровень 3	навыком использования профессиональной терминологии в области защиты информации в различных отраслях деятельности

ПК-5: Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их работоспособность при возникновении нештатных ситуаций	
Знать:	
Уровень 1	методы и средства контроля и управления доступом при обеспечении безопасности автоматизированных систем; политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой

	информационной подсистемы; современные методы предотвращения несанкционированного доступа (НСД) к объектам информатизации, основанные на биометрических технологиях распознавания личности
Уровень 2	принципы организации и структуру систем защиты программного обеспечения автоматизированных систем; средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; принципы формирования политики информационной безопасности автоматизированной системы; основные направления защиты информации в информационно- телекоммуникационных системах в соответствии с законодательством Российской Федерации
Уровень 3	современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; архитектуру автоматизированной системы управления технологическим процессом (АСУ ТП), модели промышленных систем автоматизации, сетевые технологии, используемые в современных АСУ ТП, понятия функциональной и информационной безопасности, их взаимосвязь и противоречия; основы организации своевременной и полноценной обработки инцидентов безопасности
Уметь:	
Уровень 1	использовать устройства контроля и управления доступом при обеспечении безопасности автоматизированных систем; применять политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; использовать устройства контроля доступа на основе биометрических характеристик человека
Уровень 2	регистрировать события, связанные с защитой информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять комплекс мер (правила, процедуры, практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; проводить оценку угроз безопасности информационно-телекоммуникационной системы, подключенной к сети Интернет;
Уровень 3	реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; работать со средствами обеспечения безопасности в системах промышленной автоматизации; настраивать межсетевой экран для обеспечения защиты периметра сети, для обеспечения сегментации внутренней сети
Владеть:	
Уровень 1	навыком использования систем контроля и управления доступом для управления процессами обеспечения безопасности автоматизированных систем; навыком применения инструментов администрирования подсистем информационной безопасности автоматизированной системы; навыком использования специальных средств биометрической идентификации личности для управления процессами обеспечения безопасности автоматизированных систем
Уровень 2	навыком обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы; навыком обеспечения работоспособности автоматизированных систем при возникновении нештатных ситуаций; навыком разработки частных политик информационной безопасности автоматизированных систем
Уровень 3	навыком использования антивирусного программного обеспечения для защиты информации в информационно- телекоммуникационных системах, подключенных к сети Интернет; анализом инцидентов кибербезопасности в современных промышленных системах автоматизации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона- Фано и Хаффмана);
3.1.2	цели и задачи проектирования систем инженерно-технической защиты объектов;
3.1.3	основные понятия и терминологию, принятые в проектировании систем инженерно технической защиты объектов;
3.1.4	основные принципы проектирования систем инженерно технической защиты объектов, физические принципы, на которых строятся системы инженерно-технической защиты объектов;
3.1.5	принципы организации и структуру систем защиты программного обеспечения автоматизированных систем;
3.1.6	основные направления защиты информации в информационно-телекоммуникационных системах в соответствии с законодательством Российской Федерации;
3.1.7	современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет;
3.1.8	методы и средства контроля и управления доступом при обеспечении безопасности автоматизированных систем;

3.2	**Уметь:**
3.2.1	решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей;
3.2.2	проводить анализ вероятных угроз охраняемому объекту;
3.2.3	выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту;
3.2.4	выбирать технические средства для решения задачи охраны объекта, проводить оптимизацию структуры комплексов инженерно-технической защиты объектов;
3.2.5	регистрировать события, связанные с защитой информации в автоматизированных системах;
3.2.6	проводить оценку угроз безопасности информационно-телекоммуникационной системы, подключенной к сети Интернет;
3.2.7	реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет;
3.2.8	использовать устройства контроля и управления доступом при обеспечении безопасности автоматизированных систем;
3.3	**Владеть:**
3.3.1	применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ;
3.3.2	анализа критериев оценки параметров технических средств охраны объектов;
3.3.3	составления программы испытаний систем инженерно-технической защиты объектов;
3.3.4	обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы;
3.3.5	использования антивирусного программного обеспечения для защиты информации в информационно
3.3.6	телекоммуникационных системах, подключенных к сети Интернет;
3.3.7	использования систем контроля и управления доступом для управления процессами обеспечения безопасности автоматизированных систем;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Тема 1.						
1.1	Введение.Постановказадачпрактики. Производственный инструктаж, в том числе инструктаж по технике безопасности. /Лек/	10	4			0	
	Раздел 2. Тема 2.						

2.1	Знакомство с организацией и анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности:- объекта информатизации (включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере);- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;- процесса управления информационной безопасностью защищаемого объекта. Выбор объекта проектирования. Сбор, обработка и систематизация фактического материала по выбранному объекту проектирования. /Ср/	10	70			0	
2.2	Знакомствонормативными правовыми актами в области 24 обеспечения информационной безопасности и нормативными методическими документами ФСБ России и ФСТЭК России в области защиты информации, необходимыми для обеспечения информационной безопасности выбранного объекта проектирования. /Ср/	10	60			0	
2.3	Разработка комплекса организационно -технических мероприятий, необходимых для обеспечения информационной безопасности выбранного объекта проектирования. /Ср/	10	50			0	
2.4	Выбор программно-аппаратных и технических средств защиты информации, необходимых для обеспечения информационной безопасности выбранного объекта проектирования. /Ср/	10	10			0	
2.5	Разработкадокументационного обеспечения защиты информации выбранного объекта проектирования. /Ср/	10	10			0	
2.6	Проведение технико-экономического обоснования разработанных проектных решений для обеспечения защиты информации выбранного объекта проектирования. /Ср/	10	7,75			0	
	Раздел 3. Тема 3.						

3.1	Оформлениеотчетапопреддипломнойпрактике. /Ср/	10	4			0	
3.2	Зачет /ИВКР/	10	0,25			0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

1. Каковы основные задачи преддипломной практики в сфере информационной безопасности?
2. Какие теоретические знания наиболее важны для успешного прохождения практики?
3. Какие направления ИБ наиболее актуальны для практической подготовки студентов?
4. Какие умения и навыки необходимо продемонстрировать во время практики?
5. Как вы применяли полученные знания при решении реальных задач на практике?
6. Какие методы организационной защиты информации применяются на практике?
7. Какие виды правовой защиты информации вы изучили в рамках практики?
8. Какие документы по правовому обеспечению ИБ были использованы на практике?
9. Как осуществляется контроль соблюдения политик безопасности в организациях?
10. Какие программно-аппаратные средства защиты вы использовали во время практики?
11. С какими техническими средствами защиты информации вы работали?
12. Какова роль криптографических средств защиты на предприятии, где проходила практика?
13. Какие методы аутентификации применяются на вашем объекте практики?
14. Какие типы уязвимостей чаще всего встречаются в инфраструктуре организации?
15. Как осуществляется защита сетевого трафика в организации?
16. Какие меры принимаются для защиты информации от внутренних угроз?
17. Какие категории персональных данных обрабатываются в организации?
18. Какие меры применяются для соблюдения законодательства о персональных данных?
19. Какие регламенты и инструкции по ИБ вы изучили во время практики?
20. Как организовано реагирование на инциденты информационной безопасности?
21. Какие программные средства мониторинга применяются в организации?
22. Какие способы резервного копирования используются на предприятии?
23. Как осуществляется физическая защита ИТ-инфраструктуры в организации?
24. Как происходит разграничение прав доступа пользователей?
25. Как ведётся аудит информационной безопасности в организации?
26. Какие мероприятия по защите информации вы выполняли самостоятельно?
27. Какие трудности возникли при выполнении практических задач?
28. Какой метод защиты информации вы считаете наиболее эффективным и почему?
29. Как вы оцениваете уровень защищенности объекта практики?
30. Какие предложения по улучшению защиты информации вы сформулировали?
31. Какие процедуры вы бы порекомендовали внедрить дополнительно в организации?
32. Как вы оценили взаимодействие между ИБ-службой и другими подразделениями?
33. Какие подходы к оценке рисков применяются на объекте практики?
34. Как проводится анализ инцидентов безопасности в организации?
35. Какие выводы вы сделали по результатам анализа деятельности предприятия?
36. Какие навыки аналитической работы вы приобрели во время практики?
37. Какие ИБ-отчеты или документы вам довелось составлять?
38. Какие методики оценки эффективности системы ИБ вы использовали?
39. Какова роль студента в процессе подготовки выпускной квалификационной работы?
40. Как практика помогла вам определиться с темой ВКР?
41. Какие данные или наблюдения с практики вы планируете использовать в ВКР?
42. Какие проблемы в области ИБ вы выбрали в качестве объекта исследования в ВКР?
43. Как сформулировать цель и задачи ВКР на основе практического опыта?
44. Какие предложения по улучшению ИБ-системы войдут в ВКР?
45. Какие методы исследования вы примените в ВКР, опираясь на опыт практики?
46. Как происходит взаимодействие с научным руководителем при подготовке ВКР на основе практики?
47. Какие рекомендации вы можете дать будущим практикантам по направлению ИБ?
48. Как вы оцениваете собственную профессиональную готовность к работе в сфере ИБ?
49. Что вы бы улучшили в своей практике, если бы проходили её снова?
50. Какие знания и навыки, полученные на практике, вы считаете наиболее значимыми?

5.2. Темы письменных работ

не предусмотрено

5.3. Оценочные средства

Рабочая программа "Производственная практика (преддипломная)" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 10 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	База данных научных электронных журналов "eLibrary"
6.3.2.2	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")
6.3.2.3	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
3	Специализированная многофункциональная учебная аудитория № 3 для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Компьютерные столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Стеллаж для учебно-методических материалов, в том числе учебно-наглядных пособий; Многофункциональное устройство (принтер, сканер, ксерокс); Интерактивная доска; Мультимедийный проектор; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Производственная практика (преддипломная)" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности,

характеризующих этапы формирования компетенций.