федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

Протокол заседания Ученого совета
от 29.06.2021 г. № 16

С изменениями и дополнениями
от 26.10.2022 г. (протокол заседания
ученого совета № 3)

УТВЕРЖДАЮ
Врио проректора по учебной работе
_____ О.Н. Наумова
29.06 2021 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б2.В.02 (Пд). ПРОИЗВОДСТВЕННАЯ ПРАКТИКА: ПРЕДДИПЛОМНАЯ ПРАКТИКА

ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВЫСШЕГО ОБРАЗОВАНИЯ - ПРОГРАММЫ БАКАЛАВРИАТА

Направление подготовки:
10.03.01 Информационная безопасность

Направленность (профиль) программы бакалавриата:
«**ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ**»

Квалификация выпускника: **бакалавр**

Формы обучения: **очная, очно-заочная**

Тольятти 2021

АННОТАЦИЯ

1. В Блок 2 "Практика" образовательной программы «ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ» направления подготовки 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ входят учебная и производственная практики (далее вместе - практики).

Типы учебной практики:
- ознакомительная практика;
- проектная практика

Типы производственной практики:
- технологическая практика;
- эксплуатационная практика;
- преддипломная практика.

№	Вид практики	Тип практики	Объём практики		Продолжительность практики, кол-во недель	Курс*
			з/ед.	академ. час.		
Б.2.О.01 (У)	Учебная практика	Ознакомительная практика	3	108	2	2
Б.2.В.01 (У)	Учебная практика	Проектная практика	9	324	6	1-4
Б2.О.02 (П)	Производственная практика	Технологическая практика	6	216	4	3
Б2.О.03 (П)	Производственная практика:	Эксплуатационная практика	3	108	2	4
Б2.В.03 (Пд)	Производственная практика	Преддипломная практика	6	216	4	4
		ИТОГО	**27**	**972**		

Примечание: *курс указан для очной формы обучения; для очно-заочной - в соответствии с учебным планом*

2. Практика является обязательным компонентом образовательной программы и организуется в форме практической подготовки путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенции по профилю образовательной программы.

3. Практическая подготовка может быть организована:

1) непосредственно в университете, в том числе в структурном подразделении образовательной организации, предназначенном для проведения практической подготовки;

2) 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 университетом и профильной организацией.

4. Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям образовательной программы к проведению практики.

5. При наличии в профильной организации или университете (при организации практической подготовки в университете) вакантной должности, работа на которой соответствует требованиям к практической подготовке, с обучающимся может быть заключен срочный трудовой договор о замещении такой должности.

6. Направление на практику оформляется приказом ректора или иного уполномоченного им должностного лица с указанием закрепления каждого обучающегося за организацией (структурного подразделения университета или профильной организацией), а также с указанием вида (типа) и срока прохождения практики.

Обучающемуся назначается руководитель по практической подготовке от университета, который:

- обеспечивает организацию образовательной деятельности в форме практической подготовки при реализации практики;

- организует участие обучающихся в выполнении определенных видов работ, связанных с будущей профессиональной деятельностью;

- оказывает методическую помощь обучающимся при выполнении определенных видов работ, связанных с будущей профессиональной деятельностью;

- несет ответственность совместно с ответственным работником профильной организации за реализацию практики в форме практической подготовки, за жизнь и здоровье обучающихся, соблюдение ими правил противопожарной безопасности, правил охраны труда, техники безопасности и санитарно-эпидемиологических правил и гигиенических нормативов.

7. При реализации практики руководитель по практической подготовке обеспечивает проведение текущего контроля успеваемости и промежуточной аттестации обучающихся. Текущий контроль успеваемости обеспечивает оценивание хода прохождения практик, промежуточная аттестация обучающихся - оценивание окончательных результатов прохождения практик.

8. Неудовлетворительные результаты промежуточной аттестации по практике или непрохождение промежуточной аттестации при отсутствии уважительных причин признаются академической задолженностью.

Обучающиеся обязаны ликвидировать академическую задолженность. Университет устанавливает для обучающихся, имеющих академическую задолженность, сроки повторной промежуточной аттестации по практике. Если обучающийся не ликвидировал академическую задолженность при прохождении повторной промежуточной аттестации в первый раз, ему предоставляется возможность пройти повторную промежуточную аттестацию во второй раз с проведением указанной аттестации комиссией, созданной в университете.

Повторная промежуточная аттестация проводится не позднее истечения периода времени, составляющего один год после образования академической задолженности.

9. При реализации практики университет вправе применять электронное обучение, дистанционные образовательные технологии, в том числе использование системы дистанционного обучения Moodle.

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Производственная практика (преддипломная) завершает процесс обучения по образовательной программе, углубляет и закрепляет теоретические и методические знания, практические умения и навыки, полученные при изучении дисциплин и прохождении практик обязательной части и части, формируемой участниками образовательных отношений, учебного плана.

Цель производственной практики (преддипломной):

- достижение планируемых результатов обучения, соотнесенных с индикаторами достижения компетенций и целью реализации ОПОП;
- сбор, систематизация и обобщение материала для выпускной квалификационной работы в соответствии с темой ВКР и задачами профессиональной деятельности;

Производственная практика (преддипломная) соотносится с такими типами задач профессиональной деятельности, как:

- - эксплуатационный;
- проектно-технологический;
- организационно-управленческий.

Прохождение производственной практики (преддипломной) направлено на подготовку к выполнению следующих трудовых функций (таблица 1):

Таблица 1 - Характеристика трудовых функций, выполняемых на практике, в соответствии с профессиональными стандартами

Наименование профессиональных стандартов	Код, наименование и уровень квалификации обобщенных трудовых функций (ОТФ), на которые ориентирована образовательная программа	Код и наименование трудовых функций, на которые ориентирована образовательная программа
06.032 «Специалист по безопасности компьютерных систем и сетей»	ОТФ 3.2 Администрирование средств защиты информации в компьютерных системах и сетях Уровень квалификации 6	B/01.6 Администрирование подсистем защиты информации в операционных системах B/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях B/03.6 Администрирование средств защиты информации прикладного и системного программного обеспечения
	ОТФ 3.2 Администрирование средств защиты информации в компьютерных системах и сетях Уровень квалификации 6	B/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях
06.033 «Специалист по защите информации в автоматизированных системах»	ОТФ 3.2 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации Уровень квалификации 6	B/02.6 Администрирование систем защиты информации автоматизированных систем B/04.6 Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций
	ОТФ 3.2 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации Уровень квалификации 6	B/01.6 Диагностика систем защиты информации автоматизированных систем
	ОТФ 3.2 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации Уровень квалификации 6	B/03.6 Управление защитой информации в автоматизированных системах B/05.6 Мониторинг защищенности информации в автоматизированных системах B/06.6 Аудит защищенности информации в автоматизированных

Наименование профессиональных стандартов	Код, наименование и уровень квалификации обобщенных трудовых функций (ОТФ), на которые ориентирована образовательная программа	Код и наименование трудовых функций, на которые ориентирована образовательная программа
		системах

Задачами преддипломной практики являются:

1. Изучить методики анализа рисков информационных систем на практике, нормативно-правовые документы по обеспечению информационной безопасности используемые на предприятии, стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов в действии.
2. Овладеть навыками делового общения, принятия организационно-управленческих решений, работы с учебно-методическим и информационным обеспечением информационной безопасности на предприятии, законодательными и правовыми актами в области информационной безопасности и охраны окружающей среды, требованиями к безопасности технических регламентов в отраслях промышленности.
3. Развить навыки: использования правовых нормами в конкретной жизненной ситуации, составлением юридических документов; формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; аналитической и научно-исследовательской деятельности, подготовки аналитических отчетов и информационных обзоров.
4. Овладеть методами и приобрести опыт решения профессиональных задач в области информационной безопасности.

В период преддипломной практики студент:
- Знакомится: с деятельностью и организационной структурой подразделений предприятия; с методическим обеспечением процесса защиты информации и формами организации информационной безопасности; с составом и особенностями эксплуатации программных и технических средств защиты информации; с актуальными для подразделения проблемами обеспечения информационной безопасности.
- Изучает: концепцию информационной безопасности компании политики организации защиты информации на рабочих местах; политику конфиденциального делопроизводства; основных обязанностей должностных лиц подразделения в области информационной безопасности; основных характеристик и возможностей, используемых в подразделении технических, программных средств защиты информации.
- Приобретает практические навыки: разработки инструкций по использованию технических и программных средств защиты информации; выполнения основных функциональных обязанностей в соответствии с должностью; работы с документацией, анализа и обобщения материалов; реализации и апробации предложений и проектных решений в области информационной безопасности.

5. 2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Производственная практика (научно-исследовательская работа) относится к части, формируемой участниками образовательных отношений, Блока 2 «Практики» образовательной программы «ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ».

Вид практики: производственная практика
Тип практики: преддипломная практика
Объем практики: 6 зачётных единиц, 216 академических часов
Продолжительность практики: 4 недели
Время проведения практики: в соответствии с учебным планом образовательной программы в последнем семестре.
Форма промежуточной аттестации по итогам практики: дифференциальный зачет, который выставляется на основе отчетных документов, предоставляемых обучающимся.
Форма организации практики: практическая подготовка, предусматривающая выполнение обучающимися видов работ, связанных с будущей профессиональной деятельностью.

Производственная практика проводится в форме самостоятельной работы обучающихся, направленной на получение умений и навыков профессиональной деятельности.

Местом прохождения преддипломной практики могут быть организации, предприятия и учреждения, деятельность которых соответствует профилю образовательной программы, любой организационно-правовой формы:
- промышленные организации;
- организации сферы услуг;
- страховые организации;
- некоммерческие организации;
- государственные и муниципальные органы управления финансами;
- банки, биржи, фонды;
- прочие финансовые институты.

Основными партнерами университета, согласно договоров о сотрудничестве и договоров на проведение практик, являются: ГАУ «ЦИКСО», ООО «Интеллект-ИТ», ОАО «Порт Тольятти», ООО «Техноторг», ООО Соцкультбыт-Автоваз МНК «Фортуна ЛАДА-РЕЗОРТ», Межрайонная ИФНС России №15 по Самарской области, АО «Тольяттихимбанк» и др.

В исключительных случаях преддипломная практика может проводиться в структурных подразделениях университета, предназначенных для проведения практической подготовки.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ

Результаты обучения при прохождении практики соотнесены с планируемыми результатами освоения образовательной программы и с установленными в образовательной программе индикаторами достижения компетенций.

В результате прохождения практики у обучающихся должны быть сформированы элементы следующих компетенций в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, с учетом трудовых функций, к выполнению которых в ходе практики готовится обучающийся (таблица 2).

Таблица 2 - Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
ПК-1 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ИПК-1.1. Устанавливает, настраивает и обслуживает программное обеспечение, программно-аппаратные и технические средства защиты информации с соблюдением требований по защите информации ИПК-1.2. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации	**B/01.6 Администрирование подсистем защиты информации в операционных системах** **Трудовые действия:** – Определение состава применяемых программно-аппаратных средств защиты информации в операционных системах – Разработка порядка применения программно-аппаратных средств защиты информации в операционных системах – Формирование шаблонов установки программно-аппаратных средств защиты информации в операционных системах – Установка программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации – Конфигурирование программно-аппаратных средств защиты информации в операционных системах – Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах – Управление антивирусной защитой операционных систем в соответствии с действующими требованиями **Необходимые умения:** – Формулировать политики безопасности операционных систем – Настраивать политики безопасности операционных систем – Оценивать угрозы безопасности информации операционных систем – Противодействовать угрозам безопасности информации с использованием – встроенных средств защиты информации операционных систем – Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах – Настраивать антивирусные средства защиты информации в операционных системах – Устанавливать обновления программного обеспечения и средств антивирусной защиты – Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах – Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах – Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов
ПК-2. Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ИПК-2.1. Противодействует угрозам безопасности информации с использованием встроенных средств защиты информации. ИПК-2.2. Контролирует корректность функционирования программно- аппаратных средств защиты информации в операционных системах	
ПК-3 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных,	ИПК-3.1Оценивает работоспособность применяемых средств защиты информации с использованием штатных средств и методик ИПК-3.2Оценивает эффективность применяемых средств защиты информации с	

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
программно-аппаратных и технических средств защиты информации	использованием штатных средств и методик ИПК-3.3Определяет уровень защищенности и доверия средств защиты информации	функционирования в операционных системах **Необходимые знания:** – Архитектура и принципы построения операционных систем – Программные интерфейсы операционных систем – Виды политик управления доступом и информационными потоками применительно к операционным системам – Архитектура подсистем защиты информации в операционных системах – Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы – Состав типовых конфигураций программно-аппаратных средств защиты информации – Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам – Порядок реализации методов и средств антивирусной защиты в операционных системах – Программно-аппаратные средства и методы защиты информации в операционных системах – Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации – Нормативные правовые акты в области защиты информации – Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации **B/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях** **Трудовые действия:** – Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях – Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях – Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях – Настройка программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации – Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях – Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях – Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями **Необходимые умения:** – Оценивать угрозы безопасности информации в компьютерных сетях – Настраивать правила фильтрации пакетов в компьютерных сетях – Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
		сетях – Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях – Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях – Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях – Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях – Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях **Необходимые знания:** – Принципы построения компьютерных сетей – Стек сетевых протоколов операционных систем – Стек протоколов сетевого оборудования – Порядок реализации методов и средств межсетевого экранирования – Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы – Виды политик управления доступом и информационными потоками в компьютерных сетях – Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению – Состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях – Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации – Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных – средств защиты информации – Программно-аппаратные средства и методы защиты информации в компьютерных сетях – Нормативные правовые акты в области защиты информации – Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации **B/03.6 Администрирование средств защиты информации прикладного и системного программного обеспечения** **Трудовые действия:** – Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность – Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе – Оценка последствий от реализации угроз безопасности информации в автоматизированной системе – Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации **Необходимые умения:** – Оценивать информационные риски в автоматизированных системах – Классифицировать и оценивать угрозы безопасности

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
		информации – Определять подлежащие защите информационные ресурсы автоматизированных систем – Применять нормативные документы по противодействию технической разведке – Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем – Конфигурировать параметры системы защиты информации автоматизированных систем – Применять технические средства контроля эффективности мер защиты информации **Необходимые знания:** – Основные методы управления защитой информации – Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах – Методы защиты информации от "утечки" по техническим каналам – Нормативные правовые акты в области защиты информации – Национальные, межгосударственные и международные стандарты в области защиты информации – Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
ПК-4 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации автоматизированных системах	ИПК-4.1. Применяет программные, программно-аппаратные и технические средства защиты информации автоматизированных систем, в том числе криптографические методы, алгоритмы и протоколы. ИПК-4.2. Осуществляет конфигурирование параметров программных, программно-аппаратных и технических средств защиты информации автоматизированных систем ПК-4.3. Принимает участие в организации и проведении проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.	В/04.6 Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций **Трудовые действия:** – Обнаружение неисправностей в работе системы защиты информации автоматизированной системы – Устранение неисправностей в работе системы защиты информации автоматизированной системы – Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций – Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций – Восстановление после сбоев и отказов программного обеспечения автоматизированных систем **Необходимые умения:** – Применять типовые программные средства резервирования и восстановления информации в автоматизированных системах – Применять средства обеспечения отказоустойчивости автоматизированных систем – Классифицировать и оценивать угрозы информационной безопасности – Применять программные средства обеспечения безопасности данных – Документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы **Необходимые знания:** – Методы и способы обеспечения отказоустойчивости автоматизированных систем – Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем – Основные информационные технологии, используемые в
ПК-5 Способен выявлять уязвимости в системах защиты информации автоматизированных систем, разрабатывать методики, предложения и	ИПК-5.1. Осуществляет сбор и анализ исходных данных, необходимых для проектирования систем защиты информации автоматизированных систем. ИПК-5.2. Осуществляет поиск уязвимостей в	

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
процедуры совершенствования процесса защиты информации, оптимизировать параметры программных, программно-аппаратных и технических средств защиты информации автоматизированных систем	параметрах автоматизированных систем. ИПК-5.3. Оформляет рабочую техническую документацию, в том числе программы и методики процесса защиты информации автоматизированных систем.	автоматизированных системах – Принципы построения средств защиты информации от "утечки" по техническим каналам – Программно-аппаратные средства обеспечения защиты информации автоматизированных систем – Нормативные правовые акты в области защиты информации – Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации – Организационные меры по защите информации
ПК-6 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-6.1 Применяет в профессиональной деятельности нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ПК-6.2Работает с программным обеспечением с соблюдением действующих требований по защите информации ПК-6.3Принимает организационные меры по защите информации	В/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях В/01.6 Диагностика систем защиты информации автоматизированных систем
ПК-7Способен организовать, поддерживать и управлять процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации	ИПК-7.1. Принимает участие в организации, поддержании в актуальном состоянии процесса защиты информации автоматизированных систем и совершенствовании системы управления защиты информации автоматизированных систем ИПК-7.2. Организует работу (содержание и порядок) деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации. ИПК-7.3. Осуществляет управление процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной	В/03.6 Управление защитой информации в автоматизированных системах В/05.6 Мониторинг защищенности информации в автоматизированных системах В/06.6 Аудит защищенности информации в автоматизированных системах

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
	правовой и организационно-методической документации по защите информации ПК-7.4. Осуществляет разработку, внедрение и контроль реализации правил и процедур управления системой защиты информации, работы с угрозами, инцидентами, автоматизированными системами и системами защиты информации	

4. СОДЕРЖАНИЕ ПРАКТИКИ

Процесс прохождения практики в форме практической подготовки состоит из этапов:
- подготовительный;
- основной;
- заключительный.

Содержание практики по этапам ее прохождения приведено в таблице 3.

Таблица 3 - Содержание практики по этапам

Этапы практики	Результаты обучения (компетенции)	Виды работы на практике	Трудоемкость, час
Подготови-тельный этап		Организационное собрание. Консультация руководителя практики от университета. Получение материалов для прохождения практики (программа практики, формы отчетных документов). Подготовка плана практики. Ознакомление с заданием. Инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка **Задание 1.** Совместно с руководителем практики от университета составить план прохождения практики и выполнения задания для выполнения определенных видов работ, связанных с будущей профессиональной деятельностью, в том числе с использованием современных информационных технологий для решения коммуникативных задач (e-mail, bbb, zoom, и др.) (УК-1,ОПК-2).	9
Основной этап *1 неделя*	ПК-1	**Задание 2.** Собрать исходную информацию о деятельности предприятия, необходимую для выполнения разделов отчета по практике, в том числе (ПК-1): 2.1. Собрать информацию для аналитического раздела: -место и роль предприятия на рынке, тенденции развития отрасли, в которой функционирует предприятие, а также основные вопросы, раскрывающие сущность индивидуального задания. 2.2. Собрать информацию для раздела «1.1. Описание деятельности предприятия (организации) и его организационная структура» и раздела «1.2. Основные процессы деятельности предприятия (организации)»	45
Основной этап *2 неделя* *3 неделя*	ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7	**Задание 3.** На основе изучения нормативно-правовых документов предприятия в области информационной безопасности: 3.1. Построить схему информационных потоков информации» (ПК-1, ПК-3); 3.2. . Собрать информацию для раздела «Техническое и программное обеспечение предприятия» (ПК-1, ПК-2, ПК-3); 3.3. Собрать информацию для раздела «Определение требований к комплексной системе защиты информации» (ПК-1, ПК-2, ПК-3); 3.4. Собрать информацию для раздела «Классификация вредоносного ПО» (ПК-1, ПК-2, ПК-3). 3.5 Собрать информацию для раздела «Классификация вредоносного ПО» (ПК-1, ПК-2, ПК-3). 3.6 Собрать информацию для раздела «Разработка процесса проектирования комплексной системы защиты информации	90

Этапы практики	Результаты обучения (компетенции)	Виды работы на практике	Трудоемкость, час
		для предприятия (организации)» (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7).	
Основной этап *4 неделя*	ПК-1 ПК-2 ПК-3	**Задание 4.** Собрать информацию выполнения индивидуального задания по теме ВКР (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7). **Задание 5.** Сформулировать выводы по проведенному анализу, выявить недостатки и сформулировать возможные управленческие решения для устранения недостатков. Для обоснования целесообразности управленческих решений использовать метод экспертной оценки (ПК-1, ПК-2).	45
Заключи-тельный этап		Обработка и анализ полученной информации по результатам практики. Оформление отчетной документации (отчет, дневник, аттестационный лист). Согласование отчетной документации с руководителем практики (от университета, от профильной организации). Получение характеристики Промежуточная аттестация в форме дифференцированного зачета. Подведение итогов практики. Анализ собственной деятельности. **Задание 6.** Подготовить и оформить отчет по практике. Своевременно предоставить отчет по практике на проверку. Защитить отчет по практике (подготовить и выступить с докладом, предоставить дневник, отчет, приложения к отчету, подтверждающие практический опыт, полученный на практике (фотоматериалы, наглядные образцы и др.), аттестационный лист), разместить отчет и дневник в ЭИОС университета. Структура отчета представлена в учебно-методическом пособии по практике. Приложениями к отчету должны служить ксерокопии отчетных документов предприятия, расчетные таблицы, схемы, фотографии и т.д. (ПК-1, ПК-2, ПК-3).	27
		ИТОГО	**216 (4 недели)**

Содержание этапов преддипломной практики:

Подготовительный этап. Обучающийся должен принять участие в организационном собрании, проводимом руководителем практики от университета и получить информацию о целях и задачах практики, формах отчетности и др. На организационном собрании обучающийся получает задания на практику для выполнения определенных видов работ, связанных с будущей профессиональной деятельностью, а также необходимую бланочную документацию.

Для всех обучающихся проводится инструктаж по технике безопасности и ознакомление с правилами внутреннего распорядка и ознакомление с требованиями организационно-правовых документов по охране труда и технике безопасности. При прохождении практики в профильной организации для всех обучающихся, а также руководителей практики от университета представитель профильной организации обязан провести инструктаж по охране труда до начала практики.

Для лиц с ограниченными возможностями здоровья руководитель разрабатывает индивидуальные задания, план и порядок прохождения практики с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Задание 1. Совместно с руководителем практики от университета составить план прохождения практики и выполнения задания для выполнения определенных видов работ, связанных с будущей профессиональной деятельностью, в том числе с использованием современных информационных технологий для решения коммуникативных задач (e-mail, bbb, zoom, и др.).

Основной этап. Обучающиеся решают поставленные перед ними руководителем практики практические задания.

Задание 2. Собрать исходную информацию о деятельности предприятия, необходимую для выполнения разделов отчета по практике, в том числе (ПК-1):

2.1. Собрать информацию для аналитического раздела:

- место и роль предприятия на рынке, тенденции развития отрасли, в которой функционирует предприятие, а также основные вопросы, раскрывающие сущность индивидуального задания.

2.2. Собрать информацию для раздела «1.1. Описание деятельности компании и его организационная структура» и раздела «1.2. Основные процессы деятельности организации»

Задание 3. На основе изучения нормативно-правовых документов предприятия в области информационной безопасности:

3.1. Построить схему информационных потоков информации» (ПК-1, ПК-3);

3.2. . Собрать информацию для раздела «Техническое и программное обеспечение предприятия» (ПК-1, ПК-2, ПК-3);

3.3. Собрать информацию для раздела «Определение требований к комплексной системе защиты информации» (ПК-1, ПК-2, ПК-3);

3.4. Собрать информацию для раздела «Классификация вредоносного ПО» (ПК-1, ПК-2, ПК-3).

3.5 Собрать информацию для раздела «Классификация вредоносного ПО» (ПК-1, ПК-2, ПК-3).

3.6 Собрать информацию для раздела «Разработка процесса проектирования комплексной системы защиты информации для организации» (ПК-1, ПК-2, ПК-3).

Задание 4. Собрать информацию и рассчитать показатели для выполнения индивидуального задания по теме ВКР.

Примерная тематика выпускных квалификационных работ:

1. Исследование и разработка системы противодействия внутренним угрозам предприятия
2. Разработка системы защиты персональных данных в организации
3. Проектирование комплексной системы защиты информации в организации
4. Проектирование комплексной системы защиты информации в организации
5. Бизнес-проект (стартап) «Medsecurity: проект информационной системы учета данных по защите информации в медицинских учреждениях»
6. Проектирование комплексной системы защиты информации в организации
7. Проектирование комплексной системы защиты информации в организации
8. Разработка системы управления рисками информационной безопасности предприятия
9. Проектирование и организация комплексной системы защиты информации на предприятии
10. Особенности использования методов защиты информации при разработке защищенного web-приложения
11. Разработка системы политики информационной безопасности предприятия

Программа государственной итоговой аттестации, требования к выпускным квалификационным работам, а также критерии оценки знаний, утвержденные образовательной организацией, доводятся до сведения студентов, не позднее чем за шесть месяцев до начала государственной итоговой аттестации.

В ходе преддипломной практики обучающимся необходимо составить и реализовать план исследования по теме выпускной квалификационной работы, в т.ч.:

1) определить цели и задач исследования, объекта и предмета, практической значимости, методов исследования, обосновать актуальность темы ВКР;
2) дать оценку деятельности предприятия, предложить направления развития с учетом исследований, проводимых в ВКР;
3) выполнить структурирование ВКР и составить план в соответствии с утвержденной темой ВКР;
4) выполнить подбор и анализ литературы по теме ВКР и составить библиографию исследования в соответствии с действующими техническими требованиями;
5) провести научно-исследовательский и/или патентный поиск по теме исследования;
6) подготовить материалы для проектной и экономической частей выпускной квалификационной работы.

Задание 5. Сформулировать выводы по проведенному анализу, выявить недостатки и сформулировать возможные управленческие решения для устранения недостатков. Для обоснования целесообразности управленческих решений использовать метод экспертной оценки.

Заключительный этап. На заключительном этапе обучающиеся формируют отчет о практике, содержащий информацию и выводы по каждому заданию. При написании отчета по практике обучающийся учитывает замечания руководителя практики и после их устранения окончательно оформляет отчет.

Подготовленный отчет по практике, а также заполненные дневник практики и аттестационный лист представляются руководителю практики. Обучающийся проходит процедуру защиты отчета по практике. Защита отчета по практике проводится руководителем практики от университета в форме собеседования. Студент кратко докладывает о содержании своей работы во время практики, отвечает на вопросы.

Задание 6. Подготовить и оформить отчет по практике. Своевременно предоставить отчет по практике на проверку. Защитить отчет по практике (подготовить и выступить с докладом, предоставить отчет, приложения к отчету, подтверждающие практический опыт, полученный на практике (фотоматериалы, наглядные образцы и др.), аттестационный лист), разместить отчет и дневник в ЭИОС университета. Приложениями к отчету должны служить ксерокопии отчетных документов предприятия, расчетные таблицы, схемы, фотографии и т.д.

5. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Формы отчетности - это комплект отчетных документов в соответствии с локальным нормативным актом университета, регламентирующим практическую подготовку.

По итогам прохождения практики в форме практической подготовки обучающийся представляет руководителю практики отчет по практике. Отчет по практике должен содержать сведения о конкретно выполненных видах работ, связанных с будущей профессиональной деятельностью, в соответствии с заданием. .

Содержание отчета по практике должно полностью соответствовать программе практики с кратким изложением всех вопросов, отражать умение студента применять на практике теоретические знания, полученные при изучении дисциплин (модулей).

Примерная структура отчета по производственной (преддипломной) практике:

Отчет об учебной практике является индивидуальным, и содержит ответы на основные вопросы, поставленные в ходе практики. Отчет об учебной практике включает в себя следующие элементы:

1. Титульный лист (приложение 2)
2. Содержание
3. Введение
4. Основная часть

4.1. Анализ основной деятельности и организационной структуры

4.2. Описание основных информационных потоков и процессов деятельности

4.3. Аппаратное и программное обеспечение

4.4. Информационные ресурсы как объект защиты и обслуживания

4.5. Определение требований к комплексной системе защиты информации

4.6. Анализ информационных активов, угроз и анализ рисков организации

4.7. Разработка процесса проектирования комплексной системы защиты информации для организации

6. Список литературы
7. Приложения

Оформление отчета должно соответствовать установленным требованиям.

Текстовая часть отчета оформляется на листах формата А4. Необходимо установить следующие размеры полей: верхнее - 2,0 см., нижнее - 2,0 см., левое - 2,5 см., правое - 1,5 см., интервал 1,5. Текст записки оформляется шрифтом TimesNewRoman (шрифт 12 пт, 1,5 интервала). Выставить выравнивание текста и заголовков «по ширине страницы». Нумерация страниц проставляется в «верхнем колонтитуле» по центру страницы. Титульный лист не нумеруется.

Текст отчета разделяют на разделы и подразделы. Разделы должны иметь порядковые номера в пределах всего документа, обозначенные арабскими цифрами без точки и записанные с абзацного отступа. Подразделы должны иметь нумерацию в пределах каждого раздела, номер подраздела состоит из номера раздела и подраздела, разделенных точкой. В конце номера подраздела, а также после названия раздела или подраздела точка не ставится. Каждый раздел начинается с нового листа.

Объем текстовой части отчета по практике должен быть не менее 20 стр.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

6.1. Основная литература

1. ГОСТ Р 56545–2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей [Электронный ресурс] : введ. 2016-04-01. – Режим доступа: http://www.consultant.ru.

2. ГОСТ Р 56939–2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования [Электронный ресурс] : введ. 2017-06-01. – Режим доступа: http://www.consultant.ru.

3. ГОСТ Р 58412-2019. Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения [Электронный ресурс] : введ. 2019-11-01. – Режим доступа: http://www.consultant.ru.

4. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования [Электронный ресурс] : введ. 2022-01-01. – Режим доступа: http://www.consultant.ru.

5. ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности [Электронный ресурс] : введ. 2021-11-30. – Режим доступа: http://www.consultant.ru.

6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [Электронный ресурс] : введ. 2011-12-01. – Режим доступа: http://www.consultant.ru.

7. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Электронный ресурс] : введ. 2007-06-01. – Режим доступа: http://www.consultant.ru.

8. ISO/IEC 27001:2022. Information security management systems [Электронный ресурс] : введ. 2022-10. – Режим доступа: https://www.iso.org.

9. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Information security controls [Электронный ресурс] : введ. 2022-02. – Режим доступа: https://www.iso.org.

10. ISO/IEC 27003:2017. Information technology. Security techniques. Information security management systems [Электронный ресурс] : введ. 2017-03. – Режим доступа: https://www.iso.org.

11. ISO/IEC 27004:2016. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation [Электронный ресурс] : введ. 2016-12. – Режим доступа: https://www.iso.org.

12. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Электронный ресурс] : введ. 2019-06-01. – Режим доступа: http://www.consultant.ru.

13. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования [Электронный ресурс] : введ. 1998-04-16. – Режим доступа: http://www.consultant.ru.

14. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс] : введ. 2019-06-01. – Режим доступа: http://www.consultant.ru.

15. Российская Федерация. Закон. О персональных данных [Электронный ресурс] : федер. закон № 152 : принят Гос. Думой 8 июля 2006 г. – Режим доступа: http://www.consultant.ru.

16. Российская Федерация. Закон. О коммерческой тайне [Электронный ресурс] : федер. закон № 98 : принят Гос. Думой 9 июля 2004 г. – Режим доступа: http://www.consultant.ru.

17. Российская Федерация. Закон. Об электронной цифровой подписи [Электронный ресурс] : федер. закон № 63 : принят Гос. Думой 25 марта 2011 г. – Режим доступа: http://www.consultant.ru.

18. Российская Федерация. Закон. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон № 149 : принят Гос. Думой 8 июля 2006 г. – Режим доступа: http://www.consultant.ru.

19. Гражданский кодекс Российской Федерации. Часть четвертая [Электронный ресурс] : принят Гос. Думой 24 ноября 2006 г. – Режим доступа: http://www.consultant.ru.

20. Аверченков, В. И. Аудит информационной безопасности: учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. – Текст : электронный. - URL: https://znanium.com/catalog/product/1843184 – Режим доступа: по подписке.

21. Аверченков, В. И. Защита персональных данных в организации : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 124 с. - ISBN 978-5-9765-1273-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843194 – Режим доступа: по подписке.

22. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 – Режим доступа: по подписке.

23. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 – Режим доступа: по подписке.

24. Баранова, Е. К. Основы информационней безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2022. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1860126 – Режим доступа: по подписке.

25. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148383

26. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181222

27. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2021. — 118 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178152 – Режим доступа: по подписке.

28. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. - Москва : ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178150 – Режим доступа: по подписке.

29. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ИНФРА-М, 2023. — 216 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016719-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1900721 – Режим доступа: по подписке.

30. Егошина, И. Л. Средства и методы обеспечения безопасности объектов и защиты информации : практикум / И. Л. Егошина. - Йошкар-Ола : Поволжский государственный технологический университет, 2021. - 158 с. - ISBN 978-5-8158-2240-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1894515 – Режим доступа: по подписке.

31. Защита программ и данных : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020 — Часть 1 : Способы анализа — 2020. — 72 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL:https://e.lanbook.com/book/180081

32. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927

33. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. - Москва : Директ-Медиа, 2020. - 270 с. - ISBN 978-5-4499-0496-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1908082 – Режим доступа: по подписке.

34. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518005

6.2. Дополнительная литература

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 – Режим доступа: по подписке.

2. Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова. — Уфа : БашГУ, 2020. — 120 с. — ISBN 978-5-7477-5228-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179914

3. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1899016 – Режим доступа: по подписке.

4. Маршаков, Д. В. Методы и средства криптографической защиты информации. Практический курс : учебное пособие / Д.В. Маршаков, Д.В. Фахти. — Москва : ИНФРА-М, 2022. — 76 с. — (Высшее образование). - ISBN 978-5-16-110842-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1891129 – Режим доступа: по подписке.

5. Международная информационная безопасность: теория и практика : в трех томах. Том 1 : учебник / под общ. ред А. В. Крутских. - 2-е изд., доп. - Москва : Издательство «Аспект Пресс», 2021. - 384 с. - ISBN 978-5-7567-1098-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1241985 – Режим доступа: по подписке.

6. Мельников, Д.А. Информационная безопасность открытых систем : учебник / Д.А. Мельников. — 3-е изд., стер. — Москва : ФЛИНТА, 2019. - 444 с. - ISBN 978-5-9765-1613-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1042499 – Режим доступа: по подписке.

7. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. - Саров : РФЯЦ-ВНИИЭФ, 2019. - 224 с. - ISBN 978-5-9515-0429-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1230827 – Режим доступа: по подписке.

8. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации : учебник / сост. И. Г. Дровникова, А. В. Калач, И. И. Лившиц [и др]. - Воронеж : Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1999941 – Режим доступа: по подписке.

9. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. - Саров :

РФЯЦ-ВНИИЭФ, 2019. - 267 с. - ISBN 978-5-9515-0426-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1230831 – Режим доступа: по подписке.

10. Основы технологий передачи данных и защиты информации в корпоративных сетях : учебное пособие / А. В. Мансуров ; Министерство науки и высшего образования Российской Федерации, Алтайский государственный университет. - Барнаул : Изд-во Алтайского гос. ун-та, 2020

11. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189328 – Режим доступа: по подписке.

12. Платунова, С. М. Реализация комплексной безопасности в корпоративных сетях. Шлюз безопасности как универсальное средство для обеспечения защиты данных и предотвращения вторжений : учебно-методическое пособие / С. М. Платунова, И. В. Елисеев, Е. Ю. Авксентьева. — Санкт-Петербург : НИУ ИТМО, 2020. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/190813

13. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193 – Режим доступа: по подписке.

14. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под. ред. А. В. Душкина. - Москва : Горячая линия-Телеком, 2022. - 248 с. - ISBN 978-5-9912-0470-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1911635 – Режим доступа: по подписке.

15. Системы обнаружения компьютерных атак : учебное пособие для высших учебных заведений по группе специальностей и направлений подготовки 10.00.00 "Информационная безопасность" / А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков. - Москва : Горячая линия-Телеком, 2022. - 123 с

16. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084

17. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. - Москва : ИНФРА-М, 2021. - 223 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178148 – Режим доступа: по подписке.

18. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. - Йошкар-Ола : Поволжский государственный технологический университет, 2020. - 154 с. - ISBN 978-5-8158-2165-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1894130 – Режим доступа: по подписке.

19. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2023. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1910870 – Режим доступа: по подписке.

20. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022 – Режим доступа: по подписке.

21. Шейдаков, Н. Е. Физические основы защиты информации : учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. — Москва : РИОР : ИНФРА-М, 2022. — 204 с. — (Высшее образование). — DOI: https://doi.org/10.12737/21158. - ISBN 978-5-369-01603-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1851140 – Режим доступа: по подписке.

6.3. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. КонсультантПлюс [Электронный ресурс]: Справочная правовая система. - Режим доступа: http://www.consultant.ru/.
2. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. – Режим доступа: http://elib.tolgas.ru./ - Загл. с экрана.
3. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: http://znanium.com/. – Загл. с экрана.
4. Электронно-библиотечная система «Издательство Лань» [Электронный ресурс]. - Режим доступа: https://e.lanbook.com/. – Загл. с экрана.
5. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp. - Загл с экрана.

6.4. Программное обеспечение

Информационное обеспечение практики осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Местом прохождения преддипломной практики являются организации, предприятия и учреждения, деятельность которых соответствует профилю образовательной программы, любой организационно-правовой формы. Для выполнения программы практики обучающийся должен быть обеспечен рабочим местом в структурном подразделении организации, где он проходи практику.

В исключительных случаях преддипломная практика может проводиться в структурных подразделениях университета, предназначенных для проведения практической подготовки.

Для проведения практики в университете используется следующее материально-техническое обеспечение:

- лаборатории, оснащенные лабораторным оборудованием, компьютерами с лицензионным программным обеспечением;
- аудитории для проведения групповых и индивидуальных консультаций, укомплектованные специализированной мебелью и техническими средствами обучения;
- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации;
- помещения для хранения и профилактического обслуживания учебного оборудования.

Основное учебное оборудование:

- персональные компьютеры, объединенные в локальную сеть, с выходом в Интернет;
- технические средства для демонстрации теоретического и практического материала: персональный компьютер, мультимедиа-оборудование.

Оборудование предприятий и технологическое оснащение рабочих мест практической подготовки при проведении практики в профильной организации соответствует содержанию деятельности и дает возможность обучающемуся овладеть профессиональными компетенциями по всем осваиваемым видам деятельности, предусмотренным программой с использованием современных технологий, материалов и оборудования.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее. Организовано асинхронное взаимодействие обучающегося и руководителя практики от университета с использованием ЭИОС.

Для проведения промежуточной аттестации по практике используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Практическая подготовка обучающихся с ограниченными возможностями здоровья и инвалидов организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

Контроль и оценка результатов освоения практики осуществляется руководителем практики в процессе текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация осуществляется в соответствии с расписанием занятий в форме дифференцированного зачета, который выставляется по результатам проверки отчетной документации, собеседования и защиты отчета. Защита отчета проходит, как правило, в последний день практики (с учетом календарного учебного графика по образовательной программе).

Проведение промежуточной аттестации предполагает определение руководителем практики уровня овладения обучающимся практическими навыками работы и степени применения на практике полученных в период обучения теоретических знаний в соответствии с компетенциями, формирование которых предусмотрено программой практики.

Обучающийся размещает в ЭИОС письменный отчет по практике и другие отчетные документы. Руководитель практики от университета проверяет и верифицирует размещенные отчетные документы и проставляет оценку по результатам промежуточной аттестации.

8.1. Описание показателей и критериев оценивания компетенций и шкал оценивания

Предметом оценки по практике является приобретение умений, навыков и практического опыта. Работа студента в ходе прохождения практики оценивается по четырехбалльной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

При оценке результатов работы студента на практике принимаются во внимание количественные и качественные показатели выполнения студентом заданий практики, полнота, грамотность, правильность оформления отчетной документации, характеристика, данная руководителем практики от предприятия.

Для описания показателей и критериев оценивания компетенций на разных этапах их формирования в ходе учебной практике и описания шкал оценивания применяется единый подход согласно балльно-рейтинговой системы, действующей в университете.

Таблица 4 - Шкала оценки результатов прохождения практики, сформированности результатов обучения при прохождении практики

Форма проведения промежуточной аттестации	Условия допуска	Шкалы оценки уровня сформированности результатов обучения		Шкала оценивания результатов обучения при прохождении практики		
		Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Зачет дифференцированный	допускаются все студенты, выполнившие программу практики и предоставившие все отчетные документы	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
		пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
				70-85,9	«хорошо» / 4	зачтено
		повышенный	86-100	86-100	«отлично» / 5	зачтено

Таблица 5 - Показатели и критерии оценивания планируемых результатов освоения компетенций и результатов обучения

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
ПК-1 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ИПК-1.1. Устанавливает, настраивает и обслуживает программное обеспечение, программно-аппаратные и технические средства защиты информации с соблюдением требований по защите информации ИПК-1.2. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации	**Умеет верно и в полном объеме:** Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Уверенно выполняет трудовые действия:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия с незначительными замечаниями:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Пороговый / 70-85,9 баллов/ Хорошо
		Умеет на базовом уровне, с ошибками: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
		системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия на базовом уровне, с ошибками:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	
		Не умеет на базовом уровне: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Не умеет выполнять трудовые действия на базовом уровне:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Допороговый / менее 61 балла/ Недовлетвори-тельно
ПК-2. Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ИПК-2.1. Противодействует угрозам безопасности информации с использованием встроенных средств защиты информации. ИПК-2.2. Контролирует корректность функционирования программно- аппаратных средств защиты информации в операционных системах программного обеспечения, включая системы управления базами данных и средства электронного документооборота,	**Умеет верно и в полном объеме:** Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Уверенно выполняет трудовые действия:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-	Пороговый / 70-85,9 баллов/ Хорошо

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
	формулировать правила безопасной эксплуатации операционных системах	аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия с незначительными замечаниями:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	
		Умеет на базовом уровне, с ошибками: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия на базовом уровне, с ошибками:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно
		Не умеет на базовом уровне: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Не умеет выполнять трудовые действия на базовом уровне:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства	Допороговый / менее 61 балла/ Недовлетвори-тельно

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
		криптографической защиты информации (В/01.6, В/02.6, В/03.6).	
ПК-3 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ИПК-3.1Оценивает работоспособность применяемых средств защиты информации с использованием штатных средств и методик ИПК-3.2Оценивает эффективность применяемых средств защиты информации с использованием штатных средств и методик ИПК-3.3Определяет уровень защищенности и доверия средств защиты информации	**Умеет верно и в полном объеме:** Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Уверенно выполняет трудовые действия:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия с незначительными замечаниями:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Пороговый / 70-85,9 баллов/ Хорошо
		Умеет на базовом уровне, с ошибками: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6).	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
		Выполняет трудовые действия на базовом уровне, с ошибками: Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	
		Не умеет на базовом уровне: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Не умеет выполнять трудовые действия на базовом уровне:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Допороговый / менее 61 балла/ Недовлетвори-тельно
ПК-4 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации автоматизированных системах	ИПК-4.1. Применяет программные, программно-аппаратные и технические средства защиты информации автоматизированных систем, в том числе криптографические методы, алгоритмы и протоколы. ИПК-4.2. Осуществляет конфигурирование параметров программных, программно-аппаратных и технических средств защиты информации автоматизированных систем	**Умеет верно и в полном объеме:** Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Уверенно выполняет трудовые действия:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в	Пороговый / 70-85,9 баллов/ Хорошо

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
	ПК-4.3. Принимает участие в организации и проведении проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.	операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия с незначительными замечаниями:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	
		Умеет на базовом уровне, с ошибками: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия на базовом уровне, с ошибками:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно
		Не умеет на базовом уровне: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Не умеет выполнять трудовые действия на базовом уровне:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Допороговый / менее 61 балла/ Недовлетвори-тельно

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
ПК-5 Способен выявлять уязвимости в системах защиты информации автоматизированных систем, разрабатывать методики, предложения и процедуры совершенствования процесса защиты информации, оптимизировать параметры программных, программно-аппаратных и технических средств защиты информации автоматизированных систем	ИПК-5.1. Осуществляет сбор и анализ исходных данных, необходимых для проектирования систем защиты информации автоматизированных систем. ИПК-5.2. Осуществляет поиск уязвимостей в параметрах автоматизированных систем. ИПК-5.3. Оформляет рабочую техническую документацию, в том числе программы и методики процесса защиты информации автоматизированных систем.	**Умеет верно и в полном объеме:** Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Уверенно выполняет трудовые действия:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия с незначительными замечаниями:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Пороговый / 70-85,9 баллов/ Хорошо
		Умеет на базовом уровне, с ошибками: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия на базовом уровне, с ошибками:**	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
		Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	
		Не умеет на базовом уровне: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Не умеет выполнять трудовые действия на базовом уровне:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Допороговый / менее 61 балла/ Недовлетвори-тельно
ПК-6 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-6.1 Применяетв профессиональной деятельности нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ПК-6.2Работает с программным обеспечением с соблюдением действующих требований	**Умеет верно и в полном объеме:** Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Уверенно выполняет трудовые действия:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить	Пороговый / 70-85,9 баллов/ Хорошо

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
	по защите информации ПК-6.3Принимает организационные меры по защите информации	мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия с незначительными замечаниями:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	
		Умеет на базовом уровне, с ошибками: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия на базовом уровне, с ошибками:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно
		Не умеет на базовом уровне: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Не умеет выполнять трудовые действия на базовом уровне:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Допороговый / менее 61 балла/ Недовлетвори-тельно
ПК-7Способен	ИПК-7.1. Принимает	**Умеет верно и в полном объеме:**	Повышенный /

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
организовать, поддерживать и управлять процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации	участие в организации, поддержании в актуальном состоянии процесса защиты информации автоматизированных систем и совершенствовании системы управления защиты информации автоматизированных систем ИПК-7.2. Организует работу (содержание и порядок) деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации. ИПК-7.3. Осуществляет управление процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации по защите информации ПК-7.4. Осуществляет разработку, внедрение и контроль реализации	Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Уверенно выполняет трудовые действия:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия с незначительными замечаниями:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Пороговый / 70-85,9 баллов/ Хорошо
		Умеет на базовом уровне, с ошибками: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Выполняет трудовые действия на базовом уровне, с ошибками:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах.	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
	правил и процедур управления системой защиты информации, работы с угрозами, инцидентами, автоматизированными системами и системами защиты информации	Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	
		Не умеет на базовом уровне: Формулировать политики безопасности операционных систем. Настраивать политики безопасности операционных систем. Оценивать угрозы безопасности информации операционных систем. Противодействовать угрозам безопасности информации с использованием. встроенных средств защиты информации операционных систем. Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах. Настраивать антивирусные средства защиты информации в операционных системах. Устанавливать обновления программного обеспечения и средств антивирусной защиты. Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах. Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах. Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах (В/01.6, В/02.6, В/03.6). **Не умеет выполнять трудовые действия на базовом уровне:** Определяет состава применяемых программно-аппаратных средств защиты информации в операционных системах. Осуществляет разработку порядка применения программно-аппаратных средств защиты информации в операционных системах. Формирует шаблоны установки программно-аппаратных средств защиты информации в операционных системах. Осуществляет установку программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации (В/01.6, В/02.6, В/03.6).	Допороговый / менее 61 балла/ Недовлетвори-тельно

Примерные вопросы для проведения промежуточной аттестации (дифференцированного зачета) по итогам производственной (преддипломной) практики:

1. Какие профессиональные задачи решались Вами за период практики? Как Вы их решали? Какие получили результаты (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7)
2. Какие знания, умения и навыки были приобретены или развиты в результате прохождения практики? (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7)
3. Какие задания были выполнены в ходе прохождения практики? (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7)
4. Перечислите нормативно-правовые документы в области информационной безопасности, применяемые вами на практике? (ПК-3)
5. Перечислите отчетные документы предприятия, на основе которых проводился анализ существующих уязвимостей? (ПК-1)
6. Какие сильные и слабые стороны деятельности в области защиты информации на предприятия были выявлены в ходе прохождения практики? (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7)
7. Какая проблемы была изучена в ходе прохождения практики в соответствии с заявленной темой выпускной квалификационной работы? (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7)
8. Какие научно-исследовательские задачи решались Вами за период практики? Какие методы применялись для их решения? (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7)
9. Обоснуйте актуальность выбранной темы исследования для Вашего объекта исследования ? (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7)
10. Какие проблемы в функционировании предприятия были выявлены в процессе исследования? Какие рекомендации можно предложить для их решения? (ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7)

8.2. Критерии итоговой оценки результатов практики

Критериями оценки результатов прохождения обучающимися практики в форме практической подготовки являются сформированность предусмотренных программой компетенций, т.е полученных практических навыков и умений выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Таблица 5 - Критерии оценивания результатов практики

Оценка	Уровень подготовки
Отлично	Предусмотренные программой практики результаты обучения в рамках компетенций достигнуты.Обучающийся демонстрирует высокий уровень подготовки. Большинство компетенций сформированы на повышенном уровне. Имеющихся знаний, умений, навыков и практического опыта в полной мере достаточно для решения стандартных и нестандартных профессиональных задач. Обучающийся вовремя представил подробный отчет по практике, активно работал в течение всего периода практики. Ответ на каждое задание сопровождается полноценными выводами. Отчет соответствует всем предъявляемым требованиям.
Хорошо	Предусмотренные программой практики результаты обучения в рамках компетенций достигнуты практически полностью. Все компетенции сформированы на пороговом или повышенном уровнях. Имеющихся знаний, умений, практического опыта в целом достаточно для решения стандартных профессиональных задач. Обучающийся демонстрирует в целом хорошую подготовку, но при подготовке отчета по практике и проведении собеседования допускает незначительные ошибки или недочеты. Обучающийся активно работал в течение всего периода практики. Отчет соответствует всем предъявляемым требованиям.

Оценка	Уровень подготовки
Удовлетворительно	Предусмотренные программой практики результаты обучения в рамках компетенций в целом достигнуты, но имеются явные недочеты в демонстрации умений и навыков. Все компетенции сформированы, но большинство на пороговом уровне. Обучающийся показывает минимальный уровень теоретических знаний, делает существенные ошибки при выполнении определенных видов работ, связанных с будущей профессиональной деятельностью, но при ответах на наводящие вопросы во время собеседования, может правильно сориентироваться и в общих чертах дать правильный ответ. Обучающийся имел пропуски в течение периода практики. Подготовил аналитический отчет с ошибками
Неудовлетворительно	Предусмотренные программой практики результаты обучения в рамках компетенций в целом не достигнуты, обучающийся не представил своевременно /представил отчет по практике, несоответствующий заданию. Пропустил большую часть времени, отведенного на прохождение практики.

Неудовлетворительные результаты промежуточной аттестации по практике или непрохождение промежуточной аттестации при отсутствии уважительных причин признаются академической задолженностью. Обучающиеся, имеющие академическую задолженность по итогам прохождения преддипломной практики не допускаются к прохождению ГИА.