МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
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 24.01.2022 г. № 7

с изменениями от 28.06.2023 г.
протокол № 19

УТВЕРЖДАЮ
Проректор по образовательной деятельности
О.Н. Наумова
24.01.2022 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б.2.О.04 (П). ПРОИЗВОДСТВЕННАЯ ПРАКТИКА: ПРОЕКТНО-ТЕХНОЛОГИЧЕСКАЯ ПРАКТИКА

ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВЫСШЕГО ОБРАЗОВАНИЯ - ПРОГРАММЫ МАГИСТРАТУРЫ

Направление подготовки:
10.04.01 Информационная безопасность

Направленность (профиль) программы магистратуры:
«**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ И ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ**»

Квалификация выпускника: **магистр**

Формы обучения: **очно-заочная**

Тольятти 2022

АННОТАЦИЯ

1. В Блок 2 "Практика" образовательной программы «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ И ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ» направления подготовки 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ входят разные типы производственной практики (далее вместе - практики):

- научно-исследовательская работа;
- проектно-технологическая практика;
- преддипломная практика.

№	Вид практики	Тип практики	Объём практики		Продолжи-тельность практики, кол-во недель в семестр	Курс*
			з/ед.	академ. час.		
Б.2.О.01-03 (П)	Производственная практика	Научно-исследовательская работа	12	432	2/2/4	1/2
Б.2.О.04 (П)	Производственная практика	Проектно-технологическая практика	9	324	6	2
Б2.В.01 (Пд)	Производственная практика	Преддипломная практика	6	216	4	2
ИТОГО			**27**	**972**		

Примечание: *курс указан для очной формы обучения*

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

Целью производственной практики (проектно-технологической практики) является достижение планируемых результатов обучения, соотнесенных с индикаторами достижения компетенций и целью реализации ОПОП.

Проектно-технологическая практика во время прохождения производственной практики соотносится с такими типами задач профессиональной деятельности, как (таблица 1):

- проектный.

Таблица 1 - Перечень основных задач профессиональной деятельности, решаемых в ходе практики

Область профессиональной деятельности (по Реестру Минтруда)	Типы задач профессиональной деятельности	Задачи профессиональной деятельности
06 Связь, информационные и коммуникационные технологии	проектный	- проведение обследования и анализа деятельности подразделений предприятия, и, на основе полученных данных, выбор технологий и основных компонент создаваемых систем безопасности, а также интеллектуальных и информационно-аналитических систем; - оценка угроз безопасности информации автоматизированной системы и обоснование необходимости её защиты; - обоснование требований к системе обеспечения информационной безопасности и разработка проекта технического задания на ее создание; - разработка технического проекта системы обеспечения информационной безопасности; - разработка проектов организационно-распорядительных документов по обеспечению информационной безопасности

Научно-исследовательская работа студента при прохождении производственной практики направлена на подготовку к выполнению следующих трудовых функций (таблица 2):

Таблица 2 - 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
ПС 06.031 Специалист по автоматизации информационно-аналитической деятельности	ОТФ C. Проектирование ИАС в защищенном исполнении, уровень квалификации - 7	C/01.7. Проведение предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений C/02.7 Выбор технологии и основных компонентов обеспечивающей части создаваемых ИАС C/03.7. Разработка проектных документов на создаваемые ИАС C/04.7. Проектирование обеспечивающей части ИАС
ПС 06.033 Специалист по защите информации в автоматизированных системах	ОТФ D. Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, уровень квалификации - 7	D/01.7. Обоснование необходимости защиты информации в автоматизированной системе D/02.7. Определение угроз безопасности информации, обрабатываемой автоматизированной системой D/03.7. Разработка архитектуры системы защиты информации автоматизированной системы D/04.7. Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации

Задачи производственной практики (проектно-технологической практики):

- ознакомление с нормативно правовой базой в сфере информационной безопасности,

применение полученных знаний на практике;

- изучение и применение в профессиональной деятельности отечественных и международных стандартов по разработке и оценки систем комплексной безопасности предприятий и организаций, с учетом их особенностей;
- изучение инструментов представления бизнес процессов предприятия, а также моделирования систем безопасности;
- построение модели угроз предприятия и разработка технического задания на проект системы безопасности предприятия;
- разработка технических и организационных проектов системы обеспечения информационной безопасности;
- разработка проектов организационно-распорядительных документов по обеспечению информационной безопасности;
- обоснование и оценка всех принятых решений по совершенствованию комплексной системы безопасности предприятия.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Производственная практика (проектно-технологической практики) относится к обязательной части Блока 2 «Практики» образовательной программы «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ И ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ».

Вид практики: производственная практика

Тип практики: проектно-технологическая практика

Объем практики: 9 зачётных единиц, 324 академических часа

Продолжительность практики: 6 недель.

Время проведения практики: в соответствии с учебным планом образовательной программы

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 научной и профессиональной деятельности.

Производственная практика базируется на входных знаниях, умениях и компетенциях, полученных обучающимися в процессе обучения по направлению подготовки 10.04.01 Информационная безопасность по дисциплинам:

- Управление информационной безопасностью;
- Технологии обеспечения информационной безопасности;
- Интеллектуальные системы и технологии;
- Комплексное обеспечение информационной безопасности автоматизированных систем и объектов информатизации;
- Моделирование защищённых автоматизированных систем;
- Проектирование интеллектуальных и информационно-аналитических систем в защищённом исполнении;
- Интеграция систем обработки и защиты информации.

Прохождение практики необходимо для получения знаний, умений и навыков, формируемых для последующих практик и написания выпускной квалификационной работы, а также для применения в профессиональной деятельности.

Местом прохождения производственной практики (научно-исследовательская работа) могут быть организации, предприятия и учреждения, деятельность которых непосредственно соответствует профилю образовательной программы, в том числе службы

безопасности, правоохранительные органы, частные охранные предприятия и предприятия, в чью основную сферу деятельности входит обеспечение информационной безопасности, а также специализированные подразделения организаций, предприятий и учреждений любой организационно-правовой формы:

- промышленные организации;
- организации сферы услуг;
- страховые организации;
- некоммерческие организации;
- государственные и муниципальные органы управления;
- банки и др.

Основными партнерами университета, согласно договоров о сотрудничестве и договоров на проведение практик, являются: АО «АвтоВАЗ», ПАО «КУЙБЫШЕВАЗОТ», Администрация городского округа Тольятти, ООО «ПрограмМастер», ООО «Технология Безопасности», ООО «Систематика», ООО ЧООО «Калибр-П», ПАО Сбербанк, технопарк «Жигулёвская долина», АО «Тольяттихимбанк», и др.

Производственная практика (проектно-технологическая 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 10.04.01 Информационная безопасность, с учетом трудовых функций, к выполнению которых в ходе практики готовится обучающийся (таблица 3).

Таблица 3 - 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
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации ИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации	**Умеет:** применять принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации; разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации **Владеет:** навыками обоснования требований к системе информационной безопасности на основе принципов, требований и структуры системы обеспечения информационной безопасности и защиты информации; навыками разработки технического задания на создание системы обеспечения информационной безопасности

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.1. Понимает принципы системного анализа и применяет их для проектирования системы обеспечения информационной безопасности ИОПК-2.2. Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемы ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем	**Умеет:** применять принципы системного анализа в профессиональной деятельности; разрабатывать проекты систем обеспечения информационной безопасности и технические проекты защищённых информационных систем. **Владеет:** навыками разработки технических проектов системы обеспечения информационной безопасности, ее компонентов и подсистем.
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ИОПК-3.1. Применяет нормативные правовые акты, методические документы при подготовке распорядительных документов по обеспечению информационной безопасности, в том числе при разработке ИАС ИОПК-3.2. Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности	**Умеет:** применять нормативные правовые акты, методические документы при подготовке распорядительных документов; а также разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности **Владеет:** навыками применения и разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.
ПК-1. Способен провести обследование и анализ деятельности подразделений предприятия, и на их основе выбрать технологии и основные компоненты создаваемых интеллектуальных и информационно-аналитических систем	ИПК-1.1. Проводит предпроектное обследование и анализ деятельности подразделений предприятия и выявляет их потребности, в том числе с применением интеллектуального анализа данных; ИПК 1.2. Применяет знания принципов функционирования, а также конфигураций и состава информационно-аналитических и экспертных систем для обоснования выбора технологий и компонент создаваемых интеллектуальных и информационно-аналитических систем	**Необходимые умения** Производить изучение служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7) Выявлять информационные потребности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7) Производить формализацию предметной области с целью создания ИАС (ПС 06.031, ТФ С/01.7) Составлять техническое задание на разработку ИАС (ПС 06.031, ТФ С/01.7) Готовить проектную документацию на создаваемые ИАС (ПС 06.031, ТФ С/01.7) Строить инфологическую модель предметной области (ПС 06.031, ТФ С/02.7) Описывать функциональную часть ИАС (ПС 06.031, ТФ С/02.7) Выбирать эффективную технологию функционирования ИАС на базе моделирования (ПС 06.031, ТФ С/02.7) Производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7) Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности (ПС 06.031, ТФ С/02.7) Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации (ПС 06.031, ТФ С/02.7) Выбирать состав комплекса средств защиты информации в ИАС (ПС 06.031, ТФ С/02.7) **Трудовые действия** Реализация типовых методик изучения служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7) Изучение процессов функционирования автоматизируемых подразделений в целях

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
		определения их информационных потребностей (ПС 06.031, ТФ C/01.7) Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС (ПС 06.031, ТФ C/01.7) Формирование функциональной части ИАС (ПС 06.031, ТФ C/02.7) Формирование технологии функционирования ИАС (ПС 06.031, ТФ C/02.7) Формирование конфигурации и состава обеспечивающей части ИАС (ПС 06.031, ТФ C/02.7) Формирование комплекса мер защиты информации при создании ИАС (ПС 06.031, ТФ C/02.7)
ПК-3. Способен оценить угрозы безопасности информации автоматизированной системы и обосновать необходимость её защиты	ИПК-3.1. Строит модель угроз безопасности информации, обрабатываемой автоматизированной системы; ИПК-3.2. Обосновывает необходимость защиты информации в интеллектуальных и информационно-аналитических системах.	**Необходимые умения** Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами (ПС 06.033, ТФ D/01.7) Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем (ПС 06.033, ТФ D/01.7) Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации (ПС 06.033, ТФ D/01.7) Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем (ПС 06.033, ТФ D/01.7) Использовать рисковую методологию управления защитой информации в автоматизированной системе (ПС 06.033, ТФ D/01.7) Определять класс защищенности автоматизированных систем и ее составных частей (ПС 06.033, ТФ D/01.7) Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе (ПС 06.033, ТФ D/02.7) Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7) Систематизировать результаты проведенных исследований (ПС 06.033, ТФ D/02.7) Анализировать возможные уязвимости информационных систем (ПС 06.033, ТФ D/02.7) Выявлять известные уязвимости информационных систем (ПС 06.033, ТФ

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике
		D/02.7) Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах (ПС 06.033, ТФ D/02.7) **Трудовые действия** Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите (ПС 06.033, ТФ D/01.7) Выявление степени участия персонала в обработке защищаемой информации (ПС 06.033, ТФ D/01.7) Планирование мероприятий по обеспечению защиты информации в автоматизированной системе (ПС 06.033, ТФ D/01.7) Определение требуемого класса (уровня) защищенности автоматизированной системы (ПС 06.033, ТФ D/01.7) Обоснование необходимости использования криптографических средств защиты информации (ПС 06.033, ТФ D/01.7) Разработка отчетных документов и разделов технических заданий (ПС 06.033, ТФ D/01.7) Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7) Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7) Определение оценки возможностей внешних и внутренних нарушителей (ПС 06.033, ТФ D/02.7) Разработка модели угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7) Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы (ПС 06.033, ТФ D/02.7) Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации (ПС 06.033, ТФ D/02.7) Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации в автоматизированных системах (ПС 06.033, ТФ D/02.7)

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 4.

Таблица 4 - Содержание практики по этапам

Этапы практики	Результаты обучения (компетенции)	Виды работы на практике	Трудоемкость, час
Подготови-тельный этап	ОПК-1 ПК-1	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 и др.) (ОПК-1, ПК-1).	22
Основной этап *1 неделя* *2 неделя*	ОПК-2 ПК-1	**Задание 2.** Собрать исходную информацию о деятельности предприятия, необходимую для выполнения разделов отчета по практике, в том числе (ОПК-2, ПК-1): 2.1. Собрать информацию для раздела «Введение»: - тенденции развития отрасли, в которой функционирует предприятие, а также актуальность основных вопросов, раскрывающих сущность индивидуального задания, - предмет и объект изучения; - цель и задачи исследования. 2.2. Собрать информацию для раздела «Краткая характеристика предприятия, описание и анализ его основных бизнес-процессов»: - определить и найти документальное описание основных бизнес-процессов предприятия; - используя современные стандарты и инструменты моделирования бизнес-процессов, представить их в виде модели с описанием; - определить и найти документальное описание движения основных информационно-материальных потоков предприятия; - с помощью современных информационных технологий, представить их в виде схемы с описанием.	70
Основной этап *3 неделя* *4 неделя* *5 неделя*	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-3	**Задание 3.** Изучить нормативно-правовую информацию предприятия, связанную с защитой информации по описанным процессам, а также построить модель угроз и оценить их влияние на деятельность предприятия. На основе изучения отечественных и зарубежных стандартов и методов	100

Этапы практики	Результаты обучения (компетенции)	Виды работы на практике	Трудоемкость, час
		защиты информации, внести обоснованные предложения в модернизацию системы комплексной защиты информации предприятия: 3.1. Собрать информацию и провести её анализ для раздела «Описание и анализ нормативно-правовой базы предприятия в области информационной безопасности» (ОПК-1, ОПК-2, ПК-1, ПК-3); 3.2. Изучить существующую систему защиты информации на предприятии и провести её оценку для раздела «Описание и оценка существующей системы информационной безопасности на предприятии. Модель угроз предприятия и её оценка» (ОПК-2, ПК-1, ПК-3); 3.3. Оценить всю полученную и изученную информацию и внести предложения по совершенствованию комплексной системы защиты информации предприятия в разделе «Предложения по совершенствованию комплексной системы защиты информации на предприятии», который формируется на основе выбранной темы магистерской диссертации (ОПК-1, ОПК-2, ОПК-3, ПК-1, ПК-3).	
Основной этап *6 неделя*	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-3	**Задание 4.** На основе изученной информации рассмотреть существующие методы и инструменты информационной безопасности, нормативно-правовые акты, инструменты и технические возможности для выполнения индивидуального задания по теме магистерской диссертации. Сформулировать выводы по проведенному анализу, выявить недостатки и сформулировать возможные управленческие решения для устранения недостатков в системе безопасности предприятия. Обосновать все предложения и разработать техническое задание для дальнейшей проектной деятельности (ПК-1, ПК-3). **Задание 5.** Разработать проект комплексной системы защиты информации предприятия, соответствующую ему проектную документацию, а также провести расчёт затрат и эффективности проекта. Сформировать разделы отчёта по практике «Проект комплексной системы защиты информации на предприятии» и «Расчёт затрат и эффективности проекта» соответственно (ОПК-1, ОПК-2, ОПК-3, ПК-1, ПК-3).	100
Заключи-тельный этап	ОПК-1 ОПК-3	Обработка и анализ полученной информации по результатам практики. Оформление отчетной документации. Согласование отчетной документации с руководителем практики (от университета, от профильной организации). Получение характеристики. Промежуточная аттестация в форме дифференцированного зачета. Подведение итогов практики. **Задание 6.** Подготовить и оформить отчет по практике. Своевременно предоставить отчет по практике на проверку. Защитить отчет по практике (подготовить и выступить с докладом, отчет, приложения к отчету, подтверждающие практический	32

Этапы практики	Результаты обучения (компетенции)	Виды работы на практике	Трудоемкость, час
		опыт, полученный на практике (фотоматериалы, наглядные образцы и др.), аттестационный лист), разместить отчет в ЭИОС университета. (ОПК-1, ОПК-3).	
		ИТОГО	**324 (6 недель)**

Содержание этапов 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 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:

2.1. Собрать информацию для раздела «Введение»:

- тенденции развития отрасли, в которой функционирует предприятие, а также актуальность основных вопросов, раскрывающих сущность индивидуального задания,
- предмет и объект изучения;
- цель и задачи исследования.

2.2. Собрать информацию для раздела «Краткая характеристика предприятия, описание и анализ его основных бизнес-процессов»:

- определить и найти документальное описание основных бизнес-процессов предприятия;
- используя современные стандарты и инструменты моделирования бизнес-процессов, представить их в виде модели с описанием;
- определить и найти документальное описание движения основных информационно-материальных потоков предприятия;
- с помощью современных информационных технологий, представить их в виде схемы с описанием.

Задание 3. Изучить нормативно-правовую информацию предприятия, связанную с защитой информации по описанным процессам, а также построить модель угроз и оценить их влияние на деятельность предприятия. На основе изучения отечественных и зарубежных

стандартов и методов защиты информации, внести обоснованные предложения в модернизацию системы комплексной защиты информации предприятия:

3.1. Собрать информацию и провести её анализ для раздела «Описание и анализ нормативно-правовой базы предприятия в области информационной безопасности»;

3.2. Изучить существующую систему защиты информации на предприятии и провести её оценку для раздела «Описание и оценка существующей системы информационной безопасности на предприятии. Модель угроз предприятия и её оценка»;

3.3. Оценить всю полученную и изученную информацию и внести предложения по совершенствованию комплексной системы защиты информации предприятия в разделе «Предложения по совершенствованию комплексной системы защиты информации на предприятии», который формируется на основе выбранной темы магистерской диссертации.

В период прохождения практики студент выполняет индивидуальное задание по выбранной теме будущей магистерской диссертации. Примерные темы исследований:

1. Исследование возможностей применения платформы Oracle APEX для разработки мобильных приложений учета уязвимостей инфраструктуры организаций.

2. Исследование и анализ особенностей организации безопасности в программном обеспечении.

3. Исследование и разработка антивирусных программ и антихакерских средств.

4. Исследование возможностей применения платформы Linux для разработки отдельных проектных решений для управления информационной безопасностью предприятия.

5. Исследование возможностей применения платформы Pega Platform для разработки мобильных приложений по учету уязвимости сетевых ресурсов.

6. Проект интеллектуальной информационной системы для учета уязвимостей внутренней среды предприятия на основе аппарата нечеткой логики.

7. Проект интеллектуальной информационной системы для обеспечения организационных и технических средств защиты данных на основе аппарата байесовской сети.

8. Создание системы шифрования и расшифровки сообщений.

9. Проект интеллектуальной информационной системы идентификации объектов защиты на основе API интерфейса.

10. Проект экспертной системы для анализа уязвимости и угроз в организации.

11. Использование биометрических технологий в системах безопасности.

12. Модель интеллектуальной защиты от утечки информации на основе разделения зашифрованных и сжатых данных.

13. Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей.

14. Исследование методов контроля выполнения политики безопасности организации в операционных системах семейства Linux.

15. Исследование методов контроля выполнения политики безопасности организации в операционных системах семейства Windows.

16. Исследование методов контроля выполнения политики безопасности организации в операционных системах семейства iOS.

17. Анализ и прогнозирование угроз безопасности информации

18. Использование технологии блокчейн для обеспечения безопасности данных.

19. Модель угроз информационной безопасности программного обеспечения компьютерных сетей.

20. Использование технологии ИИ для мониторинга безопасности сетей.

21. Исследование и анализ особенностей организации комплексной системы безопасности в вузе.

22. Проект экспертной системы для анализа уязвимости и угроз в вузе.

23. Анализ и прогнозирование угроз безопасности информации в вузе.

24. Модель угроз информационной безопасности программного обеспечения компьютерных сетей вуза.

Задание 4. На основе изученной информации рассмотреть существующие методы и инструменты информационной безопасности, нормативно-правовые акты, инструменты и технические возможности для выполнения индивидуального задания по теме магистерской диссертации. Сформулировать выводы по проведенному анализу, выявить недостатки и сформулировать возможные управленческие решения для устранения недостатков в системе безопасности предприятия. Обосновать все предложения и разработать техническое задание для дальнейшей проектной деятельности;

Задание 5. Разработать проект комплексной системы защиты информации предприятия, соответствующую ему проектную документацию, а также провести расчёт затрат и эффективности проекта. Сформировать разделы отчёта по практике «Проект комплексной системы защиты информации на предприятии» и «Расчёт затрат и эффективности проекта» соответственно.

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 заполненный 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, отчет, приложения к отчету, подтверждающие практический опыт, полученный на практике (фотоматериалы, наглядные образцы и др.), аттестационный лист), разместить отчет в ЭИОС университета.

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 практике (проектно-технологической практике):

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

1. Титульный лист
2. Содержание
3. Введение
4. Основная часть

4.1. Краткая характеристика предприятия, описание и анализ его основных бизнес-процессов.

4.2. Описание и анализ нормативно-правовой базы предприятия в области информационной безопасности

4.3. Описание и оценка существующей системы информационной безопасности на предприятии. Модель угроз предприятия и её оценка.

4.4. Предложения по совершенствованию комплексной системы защиты информации на предприятии в соответствие с индивидуальной темой магистерской диссертации.

4.5. Проект комплексной системы защиты информации на предприятии

4.6. Расчёт затрат и эффективности проекта.

5. Заключение
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. Андрейчиков, А. В. Интеллектуальные информационные системы и методы искусственного интеллекта : учеб. для вузов по инженерному делу, технологиям и технич. наукам по направлениям подгот. магистратуры / А. В. Андрейчиков, О. Н. Андрейчикова. - Документ read. - Москва : ИНФРА-М, 2023. - 530 с. - (Высшее образование - Магистратура). - Прил. - URL: https://znanium.com/read?id=417737 (дата обращения: 21.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-107381-0. - Текст : электронный.

2. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Документ read. - Москва : РИОР [и др.], 2022. - 336 с. - (Высшее образование). - Прил. - URL: https://znanium.com/read?id=393765 (дата обращения: 25.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01761-6. - 978-5-16-106532-7. - Текст : электронный.

3. Баранова, Е. К. Моделирование системы защиты информации. Практикум : учеб. пособие для вузов по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - Изд. 3-е, перераб. и доп. - Документ read. - Москва : РИОР [и др.], 2023. - 320 с. - (Высшее образование). - Прил. - URL: https://znanium.ru/read?id=435530 (дата обращения: 20.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01848-4. - 978-5-16-108538-7. - Текст : электронный.

4. Защита информации : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Документ read. - Москва : РИОР [и др.], 2021. - 400 с. - (Высшее образование: Бакалавриат; Магистратура). - URL: https://znanium.com/read?id=367588 (дата обращения: 21.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01759-3. - 978-5-16-013801-5. - 978-5-16-106478-8. - Текст : электронный.

5. Коваленко, В. В. Проектирование информационных систем : учеб. пособие для студентов (бакалавров и специалистов) вузов и магистров по направлению 09.03.03 "Приклад. информатика" (профиль "Приклад. информатика в экономике") / В. В. Коваленко. - 2-е изд., перераб. и доп. - Документ Read. - Москва : ФОРУМ [и др.], 2021. - 356 с. : ил., табл. - (Высшее образование. Бакалавриат). - Прил. - URL: https://znanium.com/read?id=361782 (дата обращения: 21.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-00091-637-7. - 978-5-16-107012-3. - Текст : электронный.

6. Конюх, В. Л. Проектирование автоматизированных систем производства : учеб. пособие для вузов по направлению "Автоматизир. технологии и производства" / В. Л. Конюх. - Документ read. - Москва : Курс [и др.], 2019. - 312 с. - Прил. - URL: https://znanium.com/read?id=355804 (дата обращения: 19.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-905554-53-7. - 978-5-16-009624-7. - 978-5-16-100905-5. - Текст : электронный.

7. Нестеров, С. А. Основы информационной безопасности : учеб. пособие / С. А. Нестеров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 322 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/206279 (дата обращения: 21.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-4067-2. - Текст : электронный.

8. Остроух, А. В. Проектирование информационных систем : монография / А. В. Остроух, Н. Е. Суркова. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2021. - 162 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/175513 (дата обращения: 03.03.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-8377-8. - Текст : электронный.

9. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. - Изд. 4-е, стер. - Документ Reader. - Санкт-Петербург : Лань, 2022. - 124 с. -

(Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/217445 (дата обращения: 21.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-44201-0. - Текст : электронный.
Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник по направлению подгот. "Информ. безопасность" / М. В. Тумбинская, М. В. Петровский. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 344 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/256133 (дата обращения: 21.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45046-6 : 0-00. - Текст : электронный.

6.2. Дополнительная литература

10. Бабаш, А. В. Актуальные вопросы защиты информации : монография / А. В. Бабаш, Е. К. Баранова. - Документ read. - Москва : РИОР [и др.], 2021. - 112 с. - (Научная мысль). - URL: https://znanium.com/read?id=375285 (дата обращения: 03.03.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01680-0. - 978-5-16-106277-7. - Текст : электронный.

11. Бильфельд, Н. В. Современные средства реализации автоматизированных систем. Работа с Google таблицами : учеб. пособие / Н. В. Бильфельд, Ю. И. Володина. - Документ read. - Москва : Риор [и др.], 2022. - 172 с. - (Высшее образование). - URL: https://znanium.ru/read?id=399264 (дата обращения: 17.01.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01721-0. - 978-5-16-106016-2. - Текст : электронный.

12. Ворона, В. А. Теоретические основы обеспечения безопасности объектов информатизации : учеб. пособие для вузов по направлению "Информ. безопасность" / В. А. Ворона, В. А. Тихонов, Л. В. Митрякова. - Москва : Горячая линия -Телеком, 2016. - 304 с. : ил. - (Учебное пособие для высших учебных заведений). - ISBN 978-5-9912-0524-5 : 588-50. - Текст : непосредственный.

13. Клименко, И. С. Информационная безопасность и защита информации. Модели и методы управления : монография / И. С. Клименко. - Документ read. - Москва : Инфра-М, 2022. - 180 с. - (Научная мысль). - URL: https://znanium.com/read?id=397337 (дата обращения: 02.03.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-108124-2. - Текст : электронный.

14. Коломейченко, А. С. Информационные технологии : учеб. пособие / А. С. Коломейченко, Н. В. Польшакова, О. В. Чеха. - Изд. 3-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 211 с. - Основ. термины и понятия. - Основ. сокращения. - URL: https://reader.lanbook.com/book/264086#1 (дата обращения: 21.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45293-4. - Текст : электронный.

15. Конфликтно-активное управление проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей : монография / В. И. Новосельцев, С. С. Кочедыков, Д. Е. Орлова, К. А. Плющик ; под ред. В. И. Новосельцева. - Документ read. - Москва : ИНФРА-М, 2023. - 235 с. - (Научная мысль). - Прил. - URL: https://znanium.com/read?id=426480 (дата обращения: 02.03.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-111199-4. - Текст : электронный.

16. Модели и способы взаимодействия пользователя с киберфизическим интеллектуальным пространством : монография / И. В. Ватаманюк, Д. К. Левоневский, Д. А. Малов [и др.] ; С.-Петерб. ин-т информатики и автоматизации РАН. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 174 с. - URL: https://reader.lanbook.com/book/206672 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-3877-8. - Текст : электронный.

17. Олифер, В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - Москва : Горячая линия -Телеком, 2016. - 644 с. : ил. - Прил. - ISBN 978-5-9912-0420-0 : 823-90. - Текст : непосредственный.

18. Остроух, А. В. Системы искусственного интеллекта : монография / А. В. Остроух, Н. Е. Суркова. - Изд. 4-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2024. - 228 с. -

URL: https://reader.lanbook.com/book/379988 (дата обращения: 25.01.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-47478-3. - Текст : электронный.

19. Поддержка принятия решений при проектировании систем защиты информации : монография / В. В. Бухтояров, М. Н. Жукова, В. В. Золотарев [и др.]. - Документ read. - Москва : ИНФРА-М, 2020. - 131 с. - (Научная мысль). - URL: https://znanium.com/read?id=343296 (дата обращения: 19.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-100714-3. - Текст : электронный.

20. Советов, Б. Я. Интеллектуальные системы и технологии : учеб. для студентов вузов по направлению подгот. 230400 "Информ. системы и технологии" / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. - Москва : Академия, 2013. - 319 с. : схем. - (Высшее профессиональное образование. Бакалавриат. Информатика и вычислительная техника). - ISBN 978-5-7695-9572-1 : 600-00. - Текст : непосредственный.

Сычев, Ю. Н. Защита информации и информационная безопасность : учеб. пособие для студентов высш. учеб. заведений по направлению подгот. 10.03.01. "Информационная безопасность" (квалификация (степень) "бакалавр") / Ю. Н. Сычев. - Документ read. - Москва : ИНФРА-М, 2022. - 201 с. - (Высшее образование - бакалавриат). - Прил. - URL: https://znanium.com/read?id=388766 (дата обращения: 26.03.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-107471-8. - Текст : электронный.

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

Таблица 5 - Программное обеспечение практики

№ 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

Практика проводится в структурных подразделениях университета, предназначенных для проведения практической подготовки, или в профильных организациях на основе договоров между организацией, осуществляющей деятельность по образовательной программе соответствующего профиля (далее - организация), и университетом.

Для выполнения программы практики обучающийся должен быть обеспечен рабочим местом в структурном подразделении организации, где он проходи практику.

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 6 - 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 7 - Показатели и критерии оценивания планируемых результатов освоения компетенций и результатов обучения

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации ИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации	**Умеет верно и в полном объеме:** применять принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации; разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации. **Уверенно владеет:** навыками обоснования требований к системе информационной безопасности на основе принципов, требований и структуры системы обеспечения информационной безопасности и защиты информации; навыками разработки технического задания на создание системы обеспечения информационной безопасности.	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: применять принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации; разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации. **Владеет с незначительными замечаниями:** навыками обоснования требований к системе информационной безопасности на основе принципов, требований и структуры системы обеспечения информационной безопасности и защиты информации; навыками разработки технического задания на создание системы обеспечения информационной безопасности.	Пороговый / 70-85,9 баллов/ Хорошо
		Умеет на базовом уровне, с ошибками: применять принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации; разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации. **Владеет на базовом уровне, с ошибками:** навыками обоснования требований к системе информационной безопасности на основе принципов, требований и структуры системы обеспечения информационной безопасности и защиты информации; навыками разработки технического задания на создание системы обеспечения информационной безопасности.	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно
		Не умеет на базовом уровне: применять принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации; разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации. **Не владеет на базовом уровне:** навыками обоснования требований к системе информационной безопасности на основе принципов, требований и структуры системы обеспечения информационной безопасности и защиты информации; навыками разработки технического задания на создание системы обеспечения информационной безопасности.	Допороговый / менее 61 балла/ Неудовлетвори-тельно
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной	ИОПК-2.1. Понимает принципы системного анализа и применяет их для проектирования системы обеспечения информационной безопасности ИОПК-2.2. Проектирует систему обеспечения	**Умеет верно и в полном объеме:** применять принципы системного анализа в профессиональной деятельности; разрабатывать проекты систем обеспечения информационной безопасности и технические проекты защищённых информационных систем. **Уверенно владеет:** навыками разработки технических проектов системы обеспечения информационной безопасности, ее компонентов и подсистем.	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: применять принципы системного анализа в профессиональной деятельности; разрабатывать проекты систем обеспечения информационной безопасности и технические проекты защищённых информационных систем.	Пороговый / 70-85,9 баллов/ Хорошо

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
безопасности	информационной безопасности, ее компоненты и подсистемы ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем	**Владеет с незначительными замечаниями:** навыками разработки технических проектов системы обеспечения информационной безопасности, ее компонентов и подсистем.	
		Умеет на базовом уровне, с ошибками: применять принципы системного анализа в профессиональной деятельности; разрабатывать проекты систем обеспечения информационной безопасности и технические проекты защищённых информационных систем. **Владеет на базовом уровне, с ошибками:** навыками разработки технических проектов системы обеспечения информационной безопасности, ее компонентов и подсистем.	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно
		Не умеет на базовом уровне: применять принципы системного анализа в профессиональной деятельности; разрабатывать проекты систем обеспечения информационной безопасности и технические проекты защищённых информационных систем. **Не владеет на базовом уровне:** навыками разработки технических проектов системы обеспечения информационной безопасности, ее компонентов и подсистем.	Допороговый / менее 61 балла/ Неудовлетвори-тельно
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ИОПК-3.1. Применяет нормативные правовые акты, методические документы при подготовке распорядительных документов по обеспечению информационной безопасности, в том числе при разработке ИАС ИОПК-3.2. Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности	**Умеет верно и в полном объеме:** применять нормативные правовые акты, методические документы при подготовке распорядительных документов; а также разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности. **Уверенно владеет:** навыками применения и разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.	Повышенный / 86-100 баллов/ Отлично
		Умеет с незначительными замечаниями: применять нормативные правовые акты, методические документы при подготовке распорядительных документов; а также разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности. **Владеет с незначительными замечаниями:** навыками применения и разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.	Пороговый / 70-85,9 баллов/ Хорошо
		Умеет на базовом уровне, с ошибками: применять нормативные правовые акты, методические документы при подготовке распорядительных документов; а также разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности. **Владеет на базовом уровне, с ошибками:** навыками применения и разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно
		Не умеет на базовом уровне: применять нормативные правовые акты, методические документы при подготовке распорядительных документов; а также разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности. **Не владеет на базовом уровне:** навыками применения и разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.	Допороговый / менее 61 балла/ Неудовлетвори-тельно
ПК-1. Способен провести обследование и анализ	ИПК-1.1. Проводит предпроектное обследование и анализ деятельности подразделений	**Умеет верно и в полном объеме:** Производить изучение служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Выявлять информационные потребности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Производить формализацию предметной области с целью создания ИАС (ПС 06.031, ТФ С/01.7). Составлять техническое задание на разработку ИАС (ПС 06.031, ТФ С/01.7). Готовить проектную документацию на создаваемые ИАС (ПС 06.031, ТФ С/01.7). Строить	Повышенный / 86-100 баллов/ Отлично

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
деятельности подразделений предприятия, и на их основе выбрать технологии и основные компоненты создаваемых интеллектуальных и информационно-аналитических систем	предприятия и выявляет их потребности, в том числе с применением интеллектуального анализа данных; ИПК 1.2. Применяет знания принципов функционирования, а также конфигураций и состава информационно-аналитических и экспертных систем для обоснования выбора технологий и компонент создаваемых интеллектуальных и информационно-аналитических систем	инфологическую модель предметной области (ПС 06.031, ТФ С/02.7). Описывать функциональную часть ИАС (ПС 06.031, ТФ С/02.7). Выбирать эффективную технологию функционирования ИАС на базе моделирования (ПС 06.031, ТФ С/02.7). Производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7). Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности (ПС 06.031, ТФ С/02.7). Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации (ПС 06.031, ТФ С/02.7). Выбирать состав комплекса средств защиты информации в ИАС (ПС 06.031, ТФ С/02.7) **Уверенно выполняет трудовые действия:** Реализация типовых методик изучения служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Изучение процессов функционирования автоматизируемых подразделений в целях определения их информационных потребностей (ПС 06.031, ТФ С/01.7). Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС (ПС 06.031, ТФ С/01.7). Формирование функциональной части ИАС (ПС 06.031, ТФ С/02.7). Формирование технологии функционирования ИАС (ПС 06.031, ТФ С/02.7). Формирование конфигурации и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7). Формирование комплекса мер защиты информации при создании ИАС (ПС 06.031, ТФ С/02.7)	
		Умеет с незначительными замечаниями: Производить изучение служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Выявлять информационные потребности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Производить формализацию предметной области с целью создания ИАС (ПС 06.031, ТФ С/01.7). Составлять техническое задание на разработку ИАС (ПС 06.031, ТФ С/01.7). Готовить проектную документацию на создаваемые ИАС (ПС 06.031, ТФ С/01.7). Строить инфологическую модель предметной области (ПС 06.031, ТФ С/02.7). Описывать функциональную часть ИАС (ПС 06.031, ТФ С/02.7). Выбирать эффективную технологию функционирования ИАС на базе моделирования (ПС 06.031, ТФ С/02.7). Производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7). Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности (ПС 06.031, ТФ С/02.7). Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации (ПС 06.031, ТФ С/02.7). Выбирать состав комплекса средств защиты информации в ИАС (ПС 06.031, ТФ С/02.7) **Выполняет трудовые действия с незначительными замечаниями:** Реализация типовых методик изучения служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Изучение процессов функционирования автоматизируемых подразделений в целях определения их информационных потребностей (ПС 06.031, ТФ С/01.7). Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС (ПС 06.031, ТФ С/01.7). Формирование функциональной части ИАС (ПС 06.031, ТФ С/02.7). Формирование технологии функционирования ИАС (ПС 06.031, ТФ С/02.7). Формирование конфигурации и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7). Формирование комплекса мер защиты информации при создании ИАС (ПС 06.031, ТФ С/02.7)	Пороговый / 70-85,9 баллов/ Хорошо
		Умеет на базовом уровне, с ошибками: Производить изучение служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Выявлять информационные потребности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Производить формализацию предметной области с целью создания ИАС (ПС 06.031, ТФ С/01.7). Составлять техническое задание на разработку ИАС (ПС 06.031, ТФ С/01.7). Готовить проектную документацию на создаваемые ИАС (ПС 06.031, ТФ С/01.7). Строить инфологическую модель предметной области (ПС 06.031, ТФ С/02.7). Описывать функциональную часть ИАС (ПС 06.031, ТФ С/02.7). Выбирать эффективную технологию функционирования ИАС на базе моделирования (ПС 06.031, ТФ С/02.7). Производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7). Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности (ПС 06.031, ТФ С/02.7). Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации (ПС 06.031, ТФ С/02.7). Выбирать состав комплекса средств защиты информации в ИАС (ПС 06.031, ТФ С/02.7)	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: Реализация типовых методик изучения служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Изучение процессов функционирования автоматизируемых подразделений в целях определения их информационных потребностей (ПС 06.031, ТФ С/01.7). Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС (ПС 06.031, ТФ С/01.7). Формирование функциональной части ИАС (ПС 06.031, ТФ С/02.7). Формирование технологии функционирования ИАС (ПС 06.031, ТФ С/02.7). Формирование конфигурации и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7). Формирование комплекса мер защиты информации при создании ИАС (ПС 06.031, ТФ С/02.7)	
		Не умеет на базовом уровне: Производить изучение служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Выявлять информационные потребности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Производить формализацию предметной области с целью создания ИАС (ПС 06.031, ТФ С/01.7). Составлять техническое задание на разработку ИАС (ПС 06.031, ТФ С/01.7). Готовить проектную документацию на создаваемые ИАС (ПС 06.031, ТФ С/01.7). Строить инфологическую модель предметной области (ПС 06.031, ТФ С/02.7). Описывать функциональную часть ИАС (ПС 06.031, ТФ С/02.7). Выбирать эффективную технологию функционирования ИАС на базе моделирования (ПС 06.031, ТФ С/02.7). Производить сравнительный анализ вариантов конфигураций и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7). Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности (ПС 06.031, ТФ С/02.7). Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации (ПС 06.031, ТФ С/02.7). Выбирать состав комплекса средств защиты информации в ИАС (ПС 06.031, ТФ С/02.7) **Не умеет выполнять трудовые действия на базовом уровне:** Реализация типовых методик изучения служебной деятельности автоматизируемых подразделений (ПС 06.031, ТФ С/01.7). Изучение процессов функционирования автоматизируемых подразделений в целях определения их информационных потребностей (ПС 06.031, ТФ С/01.7). Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС (ПС 06.031, ТФ С/01.7). Формирование функциональной части ИАС (ПС 06.031, ТФ С/02.7). Формирование технологии функционирования ИАС (ПС 06.031, ТФ С/02.7). Формирование конфигурации и состава обеспечивающей части ИАС (ПС 06.031, ТФ С/02.7). Формирование комплекса мер защиты информации при создании ИАС (ПС 06.031, ТФ С/02.7)	Допороговый / менее 61 балла/ Недовлетвори-тельно
ПК-3. Способен оценить угрозы безопасности информации автоматизированной системы и обосновать необходимость её защиты	ИПК-3.1. Строит модель угроз безопасности информации, обрабатываемой автоматизированной системы; ИПК-3.2. Обосновывает необходимость защиты информации в интеллектуальных и информационно-аналитических системах.	**Умеет верно и в полном объеме:** Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами (ПС 06.033, ТФ D/01.7). Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем (ПС 06.033, ТФ D/01.7). Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации (ПС 06.033, ТФ D/01.7). Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем (ПС 06.033, ТФ D/01.7). Использовать рисковую методологию управления защитой информации в автоматизированной системе (ПС 06.033, ТФ D/01.7). Определять класс защищенности автоматизированных систем и ее составных частей (ПС 06.033, ТФ D/01.7). Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе (ПС 06.033, ТФ D/02.7). Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Систематизировать результаты проведенных исследований (ПС 06.033, ТФ D/02.7). Анализировать возможные уязвимости информационных систем (ПС 06.033, ТФ D/02.7). Выявлять известные уязвимости информационных систем (ПС 06.033, ТФ D/02.7). Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах (ПС 06.033, ТФ D/02.7) **Уверенно выполняет трудовые действия:** Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите (ПС 06.033, ТФ D/01.7). Выявление степени участия персонала в обработке защищаемой информации (ПС 06.033, ТФ D/01.7).	Повышенный / 86-100 баллов/ Отлично

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
		Планирование мероприятий по обеспечению защиты информации в автоматизированной системе (ПС 06.033, ТФ D/01.7). Определение требуемого класса (уровня) защищенности автоматизированной системы (ПС 06.033, ТФ D/01.7). Обоснование необходимости использования криптографических средств защиты информации (ПС 06.033, ТФ D/01.7). Разработка отчетных документов и разделов технических заданий (ПС 06.033, ТФ D/01.7). Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7). Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7). Определение оценки возможностей внешних и внутренних нарушителей (ПС 06.033, ТФ D/02.7). Разработка модели угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации (ПС 06.033, ТФ D/02.7). Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации в автоматизированных системах (ПС 06.033, ТФ D/02.7)	
		Умеет с незначительными замечаниями: Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами (ПС 06.033, ТФ D/01.7). Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем (ПС 06.033, ТФ D/01.7). Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации (ПС 06.033, ТФ D/01.7). Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем (ПС 06.033, ТФ D/01.7). Использовать рисковую методологию управления защитой информации в автоматизированной системе (ПС 06.033, ТФ D/01.7). Определять класс защищенности автоматизированных систем и ее составных частей (ПС 06.033, ТФ D/01.7). Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе (ПС 06.033, ТФ D/02.7). Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Систематизировать результаты проведенных исследований (ПС 06.033, ТФ D/02.7). Анализировать возможные уязвимости информационных систем (ПС 06.033, ТФ D/02.7). Выявлять известные уязвимости информационных систем (ПС 06.033, ТФ D/02.7). Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах (ПС 06.033, ТФ D/02.7) **Выполняет трудовые действия с незначительными замечаниями:** Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите (ПС 06.033, ТФ D/01.7). Выявление степени участия персонала в обработке защищаемой информации (ПС 06.033, ТФ D/01.7). Планирование мероприятий по обеспечению защиты информации в автоматизированной системе (ПС 06.033, ТФ D/01.7). Определение требуемого класса (уровня) защищенности автоматизированной системы (ПС 06.033, ТФ D/01.7). Обоснование необходимости использования криптографических средств защиты информации (ПС 06.033, ТФ D/01.7). Разработка отчетных документов и разделов технических заданий (ПС 06.033, ТФ D/01.7). Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7). Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7). Определение оценки возможностей внешних и внутренних нарушителей (ПС 06.033, ТФ D/02.7). Разработка модели угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации (ПС 06.033, ТФ D/02.7). Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации в автоматизированных	Пороговый / 70-85,9 баллов/ Хорошо

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
		системах (ПС 06.033, ТФ D/02.7)	
		Умеет на базовом уровне, с ошибками: Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами (ПС 06.033, ТФ D/01.7). Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем (ПС 06.033, ТФ D/01.7). Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации (ПС 06.033, ТФ D/01.7). Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем (ПС 06.033, ТФ D/01.7). Использовать рисковую методологию управления защитой информации в автоматизированной системе (ПС 06.033, ТФ D/01.7). Определять класс защищенности автоматизированных систем и ее составных частей (ПС 06.033, ТФ D/01.7). Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе (ПС 06.033, ТФ D/02.7). Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Систематизировать результаты проведенных исследований (ПС 06.033, ТФ D/02.7). Анализировать возможные уязвимости информационных систем (ПС 06.033, ТФ D/02.7). Выявлять известные уязвимости информационных систем (ПС 06.033, ТФ D/02.7). Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах (ПС 06.033, ТФ D/02.7) **Выполняет трудовые действия на базовом уровне, с ошибками:** Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите (ПС 06.033, ТФ D/01.7). Выявление степени участия персонала в обработке защищаемой информации (ПС 06.033, ТФ D/01.7). Планирование мероприятий по обеспечению защиты информации в автоматизированной системе (ПС 06.033, ТФ D/01.7). Определение требуемого класса (уровня) защищенности автоматизированной системы (ПС 06.033, ТФ D/01.7). Обоснование необходимости использования криптографических средств защиты информации (ПС 06.033, ТФ D/01.7). Разработка отчетных документов и разделов технических заданий (ПС 06.033, ТФ D/01.7). Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7). Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7). Определение оценки возможностей внешних и внутренних нарушителей (ПС 06.033, ТФ D/02.7). Разработка модели угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации (ПС 06.033, ТФ D/02.7). Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации в автоматизированных системах (ПС 06.033, ТФ D/02.7)	Пороговый / 61-69,9 баллов/ Удовлетвори-тельно
		Не умеет на базовом уровне: Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами (ПС 06.033, ТФ D/01.7). Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем (ПС 06.033, ТФ D/01.7). Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации (ПС 06.033, ТФ D/01.7). Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем (ПС 06.033, ТФ D/01.7). Использовать рисковую методологию управления защитой информации в автоматизированной системе (ПС 06.033, ТФ D/01.7). Определять класс защищенности автоматизированных систем и ее составных частей (ПС 06.033, ТФ D/01.7). Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе (ПС 06.033, ТФ D/02.7). Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Систематизировать результаты проведенных исследований (ПС	Допороговый / менее 61 балла/ Недовлетвори-тельно

Формируемые компетенции	Индикаторы достижения компетенции	Критерии оценивание	Уровень освоения компетенции/ оценка
		06.033, ТФ D/02.7). Анализировать возможные уязвимости информационных систем (ПС 06.033, ТФ D/02.7). Выявлять известные уязвимости информационных систем (ПС 06.033, ТФ D/02.7). Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах (ПС 06.033, ТФ D/02.7) **Не умеет выполнять трудовые действия на базовом уровне** Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите (ПС 06.033, ТФ D/01.7). Выявление степени участия персонала в обработке защищаемой информации (ПС 06.033, ТФ D/01.7). Планирование мероприятий по обеспечению защиты информации в автоматизированной системе (ПС 06.033, ТФ D/01.7). Определение требуемого класса (уровня) защищенности автоматизированной системы (ПС 06.033, ТФ D/01.7). Обоснование необходимости использования криптографических средств защиты информации (ПС 06.033, ТФ D/01.7). Разработка отчетных документов и разделов технических заданий (ПС 06.033, ТФ D/01.7). Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7). Определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем (ПС 06.033, ТФ D/02.7). Определение оценки возможностей внешних и внутренних нарушителей (ПС 06.033, ТФ D/02.7). Разработка модели угроз безопасности информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы (ПС 06.033, ТФ D/02.7). Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации (ПС 06.033, ТФ D/02.7). Определение структурно-функциональных характеристик информационной системы в соответствии с требованиями нормативных правовых документов в области защиты информации в автоматизированных системах (ПС 06.033, ТФ D/02.7).	

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

1. Какие основные документы ФСТЭК по разработке систем информационной безопасности Вы можете назвать? (ОПК-3)

2. Какие отечественные и международные ГОСТы Вы применяли в своей работе? (ОПК-3)

3. Какие нормативно-правовые документы Вы использовали при проведении анализа системы информационной безопасности предприятия? (ОПК-3)

4. Какие инструменты моделирования бизнес-процессов предприятия Вы использовали при формировании отчёта по практике? (ОПК-2, ПК-1)

5. Какие сильные и слабые стороны в системе защиты информации предприятия были выявлены в ходе прохождения практики? (ОПК-1, ОПК-2, ПК-1, ПК-3)

6. Какие проблемы в системе безопасности предприятия были выявлены в процессе исследования? Какие рекомендации можно предложить для их решения? (ОПК-2, ПК-3)

7. Какие требования к защите информации в ИАС установлены законодательством? (ОПК-3)

8. Какие требования к архитектуре ИАС устанавливаются нормативами? (ОПК-2, ОПК-3)

9. Какие процедуры обновления и модернизации автоматизированных систем описаны в специализированной документации? (ОПК-1, ОПК-3)

10. Что представляет собой предложенная вами система комплексной безопасности предприятия? (ОПК-1, ОПК-2, ПК-1)

8.2. Критерии итоговой оценки результатов практики

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

Таблица 8 - 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.

Для обучающихся, не прошедших практику по уважительным причинам, организуется ее проведение в свободное от учебы время.

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.