НЕГОСУДАРСТВЕННОЕ АККРЕДИТОВАННОЕ НЕКОММЕРЧЕСКОЕ ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«АКАДЕМИЯ МАРКЕТИНГА И СОЦИАЛЬНО-ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – ИМСИТ»

(г. Краснодар)

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИННОВАЦИЙ

КАФЕДРА МАТЕМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Рекомендовано
кафедрой математики

и вычислительной техники
протокол № 3 от 13.10 2023 г
Зав. кафедрой доцент
Исикова Н.П.

УТВЕРЖДАЮ
Проректор по учебной работе,
доцент
_____ Н.И. Севрюгина
2023г.

Б2.О.04(П)

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ:

ЭКСПЛУАТАЦИОННОЙ ПРАКТИКИ

для обучающихся направления

10.03.01 Информационная безопасность

Направленность «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

квалификация (степень) выпускника

«Бакалавр»

Краснодар

2023

Рабочая программа производственной практики: Эксплуатационная практика для обучающихся направления 10.03.01 Информационная безопасность / сост. кандидат технических наук, доцент Капустин С.А. – Краснодар, ИМСИТ, 2023.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. № 1427.

Рабочая программа рассмотрена и рекомендована на заседании кафедры Математики и вычислительной техники от 13.10. 2023 г., протокол № 3

Зав. кафедрой математики и вычислительной
техники, к.э.н., доцент Н.П. Исикова

Рабочая программа утверждена на заседании Научно-методического совета Академии ИМСИТ протокол № 3 от 20.11.2023 г.

Председатель Научно-методического совета,
профессор Н.Н. Павелко

Согласовано:

Проректор по качеству образования,
доцент К.В. Писаренко

Рецензенты:

Видовский Л.А., д.т.н., профессор, профессор кафедры информационных систем и программирования КубГТУ

Глебов О.В., директор АО «ЮГ-СИСТЕМА ПЛЮС»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Производственная практика (эксплуатационная) практика является составной частью основной образовательной программы профессиональной подготовки бакалавров.

Программа практики включает методические указания по ее прохождению, требования к содержанию, рекомендации по успешному выполнению учебно-практических задач.

Содержание программы производственной (эксплуатационной) практики основано на компетентностном подходе к обучению студентов и составлено в соответствии с ФГОС ВО, основной образовательной программой по направлению подготовки 10.03.01 Информационная безопасность.

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, указанная практика как тип учебной практики является одной из составляющих раздела Б2 учебного плана бакалавриата. Она представляет собой вид учебных занятий, непосредственно ориентированный на ознакомительную практику студентов.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Цель и задачи практики

Практика обеспечивает соответствие уровня теоретической подготовки практической направленности в системе обучения и будущей деятельности выпускника.

Цель практики:

– закрепление, расширение, углубление и систематизация знаний, полученных при изучении обязательных дисциплин базовой части учебного плана;

– освоение современных технологий и технических средств, применяемых в области информационной безопасности;

– совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и

отчетных документов по результатам профессиональной деятельности и практики;

– обеспечение возможности применения студентами теоретических знаний для решения практических задач;

– развитие организаторских способностей и развитие исполнительских и лидерских навыков обучающихся;

– формирование и развитие практических навыков в профессиональной сфере использования технологий и технических средств, применяемых в области информационной безопасности;

– развитие у обучающихся компетенций, а также формирования опыта самостоятельной исследовательской и аналитической деятельности в изучении практического материала;

– формирование общего представления студентов о будущей профессиональной деятельности и развитие интереса к профессии.

Производственная (эксплуатационная) практика базируется на дисциплинах:

– Б1.О.30	– Организационное и правовое обеспечение информационной безопасности
– Б1.О.35	– Защита информации от утечки по техническим каналам
– Б1.О.36	– Безопасность операционных систем
– Б1.О.37	– Безопасность компьютерных сетей
– Б1.О.39	– Программно-аппаратные средства защиты информации
– Б1.О.40	– Основы управления информационной безопасностью
– Б1.В.03	– Системы охраны и инженерной защиты информации
– Б1.В.04	– Защита информационных процессов в компьютерных системах
– Б1.В.06	– Проектирование защищенных автоматизированных систем

Основные задачи производственной (эксплуатационной) практики:

– формирование общепрофессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за учебной ознакомительной практикой;

– освоение современных технологий и технических средств, применяемых в области информационной безопасности;

– совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики.

Область профессиональной деятельности выпускника

Соответствие выделенной частично *(или полностью)* ОТФ (обобщенной трудовой функции) профессиональной деятельности выпускников, на основе установленных профессиональным стандартом для ОТФ уровня квалификации и требований раздела ФГОС «Требования к образованию и обучению» в наборе профессиональных компетенций по дисциплине.

Освоение производственной (эксплуатационной) практики обеспечивает подготовку бакалавров по направлению подготовки 10.03.01 Информационная безопасность, области профессиональной деятельности и сферы профессиональной деятельности**,** которых включают: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере): 06.030 Специалист по защите информации в телекоммуникационных системах и сетях, 06.032 Специалист по безопасности компьютерных систем и сетей, 06.033 Специалист по защите информации в автоматизированных системах, 06.034 Специалист по технической защите информации.

Область профессиональной деятельности:

– совершенствование и применение средств защиты информации в автоматизированных системах;

– определение угроз информационной безопасности в автоматизированных системах;

– администрирование подсистем защиты информации в операционных системах;

– мониторинг и аудит защищенности информации в автоматизированных системах;

– разработка организационно-распорядительных документов по защите информации в автоматизированных системах;

– проведение контроля защищенности информации от несанкционированного доступа;

– профессиональная деятельность в сфере защиты информации.

Объекты профессиональной деятельности выпускника

Освоение производственной (эксплуатационной) практики обеспечивает подготовку бакалавров по направлению 10.03.01 Информационная безопасность, **объектами профессиональной деятельности**, которых являются:

– системы обработки данных;

– автоматизированные системы различного назначения;

– средства защиты информации;

– объекты, на которых осуществляется обработка информации ограниченного доступа.

Освоение производственной (эксплуатационной) практики обеспечивает подготовку бакалавров по направлению 10.03.01 Информационная безопасность, которые готовятся к решению **задач профессиональной деятельности следующих типов**: эксплуатационный, проектно-технологический, экспериментально-исследовательский, организационно-управленческий.

1.2 Вид практики, способ и форма (формы) проведения практики

Вид практики – производственная практика.

Тип практики – эксплуатационная.

Способы проведения практики – стационарная, выездная.

Формы проведения практики – дискретно: путем чередования в календарном учебном графике периодов учебного времени для проведения практик с периодами учебного времени для проведения теоретических занятий.

Место (места) проведения практики – структурные подразделения Академии маркетинга и социально-информационных технологий.

Лицам с ограниченными возможностями здоровья предоставляются места практики по их желанию с учетом их индивидуальных возможностей

1.3 Объем практики в зачетных единицах и ее продолжительность в неделях или в академических часах

Время проведения практики определяется календарным учебным графиком по направлению подготовки 10.03.01 Информационная безопасность направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Общая трудоемкость Производственной практики (технологическая) составляет для очной формы обучения 3 зачетные единицы (108 часов), 2 недели, в том числе:

4 курс			Итого
7 семестр	8 семестр	Всего	
0	3	3	3

Для заочной формы обучения 3 зачетные единицы (108 часов), 2 недели, в том числе:

Курс 5	Итого
3	3

Таблица 1.1 – Объем Производственной практики (технологическая)

Вид учебной работы	Очная форма обучения		Заочная форма обучения	
	4 курс		5 курс	
	7 семестр	8 семестр	1 сессия	2 сессия
Общая трудоемкость (часы, зачетные единицы)		108 (3)		108 (3)
Контактная работа обучающихся с руководителем (контактные часы), всего		72,3		72,3
Контактная работа по промежуточной аттестации (КА)		0,3		0,3
Иные виды работы во время практики, включая самостоятельную работу (СР), всего:		35,7		
Вид итогового контроля по практике		Зачет с оценкой		Зачет с оценкой

1.4 Место практики в структуре образовательной программы

Практика реализуется в рамках обязательной части Блока 2. Практика основной профессиональной образовательной программы.

Прохождение практики предполагает предварительное освоение следующих дисциплин образовательной программы:

- Б1.О.30 – Организационное и правовое обеспечение информационной безопасности
- Б1.О.35 – Защита информации от утечки по техническим каналам
- Б1.О.36 – Безопасность операционных систем
- Б1.О.37 – Безопасность компьютерных сетей
- Б1.О.39 – Программно-аппаратные средства защиты информации
- Б1.О.40 – Основы управления информационной безопасностью
- Б1.В.03 – Системы охраны и инженерной защиты информации
- Б1.В.04 – Защита информационных процессов в компьютерных системах
- Б1.В.06 – Проектирование защищенных автоматизированных систем

Прохождение практики необходимо как предшествующее для следующих дисциплин образовательной программы:

- Б1.В.07 Порядок проведения аттестации объектов информатизации
- Б1.В.08 Комплексная защита объектов информатизации
- Б2.О.05(П) Производственная практика: Преддипломная практика
- Б3.01(Д) Выполнение и защита выпускной квалификационной работы

В результате прохождения практики студент бакалавриата должен приобрести следующие компетенции:

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их

значение для обеспечения объективных потребностей личности, общества и государства;

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

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;

ОПК-4.1: Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;

ОПК-4.3: Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;

2 ОРГАНИЗАЦИЯ ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ЭКСПЛУАТАЦИОННАЯ)

Производственная практика является одним из видов учебной работы, когда студент обязан выполнить практические и индивидуальные задания, подготовить и защитить отчет по практике.

Руководство производственной практикой осуществляет руководитель научно-исследовательской лаборатории.

Обучающимся перед началом практики выдают задание на практику установленного образца. Данный документ служит основанием для отражения информации, связанной с характеристикой работы студента в период практики и отзывом на него руководителя практики от предприятия. Руководитель практики от академии на данном бланке по итогам сдачи отчета оформляет краткий отзыв на работу и выставляет оценку.

2.1 Обязанности руководителя практики от кафедры

Руководитель производственной практики:

– составляет программу учебной практики;

– разрабатывает темы индивидуальных заданий;

– осуществляет методическое обеспечение практики;

– контролирует выполнение заданий и консультирует студентов

При прохождении практики руководители от образовательной организации и организации (объект практики) контролируют:

– фактические сроки пребывания студентов на практике;

– наличие документов, определяющих порядок прохождения практики (приказы о зачислении на практику, планы-графики, документы, удостоверяющие проведение инструктажа по технике безопасности и др.);

– соблюдение графиков выполнения работы по сбору материалов;

– условия труда, быта и отдыха студентов.

Объем и содержание отчета должны соответствовать программе практики. Отчет проверяет и подписывает руководитель практики от организации, после чего он дает отзыв о прохождении студентом практики.

Подписи руководителей от организации в отчете (на титульном листе отчета) и отзыве должны быть заверены печатью организации.

По возвращению с практики студент сдает руководителю практики от академии отчет для проверки полноты, правильности и качества его выполнения. Защита отчетов по практике организуется кафедрой не позднее 7 дней после завершения практики или начала учебного года.

Защита любого вида практики оценивается в виде дифференцированного зачета с оценкой по 5-ти бальной оценке (зачтено с оценкой «отлично», зачтено с оценкой «хорошо», зачтено с оценкой «удовлетворительно», не зачтено с оценкой «неудовлетворительно»). Оценка проставляется в зачетной книжке. Студент, не выполнивший программу практики, получивший отрицательный отзыв о работе или неудовлетворительную оценку при защите, считается не выполнившим учебный план.

2.2 Обязанности студента

При прохождении практики обучающийся должен соблюдать правила охраны труда, техники безопасности и производственной санитарии в организации, изучить научно-методическую литературу по исследуемой проблеме, участвовать в работе по заданию кафедры и руководителя практики от академии.

Изучив программу практики и собрав необходимый материал для выполнения отчета, обучающийся должен обобщить и отразить результаты работы в отчете о практике.

2.3 Обязанности руководителя практики от предприятия

Руководитель практики от организации:

согласовывает индивидуальные задания, содержание и планируемые результаты практики;

предоставляет рабочие места обучающимся;

обеспечивает безопасные условия прохождения практики обучающимся, отвечающие санитарным правилам и требованиям охраны труда;

проводит инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка.

Руководитель должен ознакомить студента с Правилами внутреннего распорядка дня и контролировать их соблюдение.

Предоставить студенту рабочее место, обеспечивающее наибольшую эффективность прохождения практики в соответствии с утвержденной программой и заданием кафедры. Обеспечить работу студента с руководителем практики от организации.

Создать необходимые условия для приобретения студентом в период практики навыков самостоятельной работы по избранному направлению подготовки.

Предоставить студенту-практиканту возможность пользоваться специальной литературой, инструктивными материалами, положениями, уставом и другими документами организации.

Вносить предложения о поощрении отличившегося на работе студента либо наложения дисциплинарного взыскания при нарушении Правил внутреннего распорядка дня и сообщить об этом ректору образовательной организации. После окончания практики дать краткую характеристику работы студента.

3 СОДЕРЖАНИЕ ПРАКТИКИ

3.1 Структура и содержание Производственной практики (эксплуатационной)

Содержанием производственной практики является выполнение задания по практике, которое выдается руководителями практики от академии совместно с руководителем практики от предприятия (таблица 3.1).

Таблица 3.1 – График прохождения Производственной практики (эксплуатационная)

	Содержание раздела	Трудоемкость в часах	Форма текущего контроля	Формируемые компетенции
	Подготовительный этап			
1	Установочная конференция: цели и задачи учебной практики; инструктаж по технике безопасности; получение задания на практику (в том числе – индивидуальные варианты); требования к оформлению документов (отчет, дневник и пр.)	6	Мониторинг результатов	ОПК-1
	Содержательный этап			
2	Знакомство с содержанием деятельности подразделения по обеспечению информационной безопасности и проводимыми в нем мероприятиями. Изучение нормативных правовых актов по обеспечению информационной безопасности (политика безопасности профильной организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	30	Мониторинг результатов практических работ	ОПК-5 ОПК-10
3	Самостоятельное проведение мониторинга и (или) производственного контроля эффективности применения средств защиты информации в ТКС. Организация работы 2-3 человек и руководство их работой в процессе формулирования предложений по совершенствованию системы защиты информации в ТКС.	30	Мониторинг результатов практических работ	ОПК-1 ОПК-5 ОПК-6 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.3

	Создание плана работы коллектива из 3 – 4 человек, реализующего политику безопасности в ТКС. Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. Формирование систематизированной инструкции по эксплуатации конкретного средства защиты информации в конкретной ТКС. Представление результатов руководителю практики от организации.			
4	Самостоятельное проведение уценки угроз информационной безопасности, возможных каналов утечек конфиденциальных данных в ТКС. Оценка рисков информационной безопасности. Самостоятельная подготовка рекомендаций по повышению уровня информационной безопасности предприятия. Организация работы 2-3 человек и руководство их работой в процессе подготовки рекомендаций по проведению регламентных работ по обнаружению уязвимостей ТКС. Самостоятельное составление рекомендаций по отказоустойчивой эксплуатации защищённых ТКС. Представление перечня средств и мер по обеспечению отказоустойчивости системы. Представление результатов руководителю практики от организации.	30	Мониторинг результатов практических работ	ОПК-1 ОПК-5 ОПК-6 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.3
Отчетный этап				
	Подготовка и оформление отчета по практике.	12	Защита отчета по практике	ОПК-1

Подготовительный этап (установочная конференция в образовательной организации) включает следующие вопросы:

– конкретизация направления практики,

– формулировка конкретных целей и задач практики

– ознакомление с отчетной документацией по итогам практики.

– беседа с руководителем практики от предприятия.

– инструктаж по технике безопасности.

– ознакомление с правила ми внутреннего трудового распорядка предприятия.

– определение рабочего места практиканта.

Инструктаж обучающихся является важнейшим мероприятием по организации практики, от которого во многом зависит качество практики в целом, учебная и производственная дисциплина обучающихся и т. д.

Инструктаж имеет целью:

– информировать обучающихся о сроках, целях и задачах практики;

– довести до студентов примерное распределение фонда рабочего времени в период практики;

– информировать обучающихся о местах прохождения практики и о руководителях практики от академии.

Содержательный этап включает выполнение заданий, изложенных в методических материалах к практическим работам, а также выполнение индивидуального задания по варианту, назначенному руководителем практики от кафедры.

Отчетный этап определяет защиту отчета по практике, выполненного в соответствии с заданием на практику.

Составленный по итогам практики отчет обучающийся сдает на проверку руководителю, подписанным руководителем практики от организации.

После проверки отчета руководителем практики от образовательной организации заведующий кафедрой назначает комиссию, по защите результатов практики, состоящую из числа преподавателей кафедры, а также с возможным привлечением работодателей.

Защита результатов практики проводится в виде устного выступления (5-7 мин.) перед комиссией.

Члены комиссии оценивают представленную работу по следующим критериям:

1. Качество выполнения практических работ.
2. Выполнение индивидуального задания.
3. Оформление отчета (грамотность, соответствие требованиям оформления, качество иллюстративного материала, логичность и полнота материалов отчета).

На основании данных критериев комиссия экспертным путем дает оценку уровня сформированности необходимых компетенций. Выставляют одну из оценок – зачтено (с оценкой «отлично»), зачтено (с оценкой «хорошо»), зачтено (с оценкой «удовлетворительно»), не зачтено (с оценкой «неудовлетворительно»).

Структура отчета по практике, следующая:

- титульный лист;
- содержание;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложения (при необходимости).

Титульный лист является первой страницей работы и служит источником информации для идентификации работы (Приложение А).

Оглавление отражает заявленные задачи и последовательность изложения материала.

Во введении необходимо указать цель и выделить задачи, которые необходимо решить для достижения поставленной цели исследования.

Основная часть должна раскрывать суть, методы и результаты выполненной работы.

Заключение должно быть лаконичным, доказательным и убедительным, содержать итоговый вывод по всей работе.

Правила оформления отчета по практике приведены в приложении 3.

4 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате прохождения Производственной (эксплуатационной) практики у обучающихся должны быть сформированы компетенции, таблица 4.1.

Таблица 4.1 – Планируемые результаты обучения

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-1.1: Классифицирует угрозы информационной безопасности в соответствии с нормативными документами	**Знать:** - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации; - нормативно-правовые аспекты обеспечения информационной безопасности РФ.	**Уметь:** - выявлять угрозы информационной безопасности; - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности.	**Владеть:** - навыками классификации угроз; - навыками выявления уязвимостей технических каналов связи информационных систем.
ОПК-1.2: Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации	**Знать:** - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность.	**Уметь:** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты.	**Владеть:** - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий.
ОПК-1.3: Определяет угрозы информационной	**Знать:** - методы повышения уровня	**Уметь:** - формализовать сведения для	**Владеть:** - общими приемами организации поиска;

безопасности для различных систем	защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности.	запросов; - выбирать тип запроса; - составлять простые и составные запросы.	- алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур.
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-5.1: Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	**Знать:** - правовые основы организации защиты конфиденциальной информации; - задачи органов защиты информации.	**Уметь:** - применять действующую законодательную базу в области обеспечения информационной безопасности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.	**Владеть:** - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.
ОПК-5.2: Формулирует основные	**Знать:** - правовые нормы и стандарты по защите	**Уметь:** - применять действующую	**Владеть:** - навыками работы с нормативными

требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - принципы формирования политики информационной безопасности в автоматизированных системах.	законодательную базу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.	правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.
ОПК-5.3: Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	**Знать:** - правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; - основные отечественные и зарубежные стандарты в области информационной безопасности; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем.	**Уметь:** - применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по	**Владеть:** - навыками работы с нормативными правовыми актами; - навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках.

		требованиям безопасности информации.	
ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации	**Знать:** - модели угроз и модели нарушителя.	**Уметь:** - разрабатывать модели угроз объекта информатизации.	**Владеть:** - навыками разработки модели угроз и модели нарушителя объекта информатизации.
ОПК-6.2: Определяет политику контроля доступа работников к информации ограниченного доступа	**Знать:** - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - угрозы безопасности; - модели нарушителя объекта информатизации.	**Уметь:** - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа.	**Владеть** - навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа; - навыками создания локальных нормативных актов.
ОПК-6.3: Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации	**Знать:** - требования руководящих документов по физической защите объектов информатизации; - требования по пропускному режиму в организации.	**Уметь:** - использовать средства физической защиты объекта информатизации.	**Владеть:** - навыками организации и контроля пропускного режима.
ОПК-6.4: Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного	**Знать:** - требования руководящих документов регламентирующих защиту информации ограниченного доступа.	**Уметь:** - использовать требования руководящих документов регламентирующих защиту информации ограниченного доступа.	**Владеть:** - навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного

доступа в организации			доступа.
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах	**Знать:** - основы криптографии, методы защиты; - классификацию криптографических методов; - основы шифрования с помощью скремблеров; - основы шифрования с помощью ассиметричных алгоритмов; - основы шифрования перспективными методами; - основы программной реализации криптографических преобразований.	**Уметь:** - выполнять шифрование криптографическими методами; - определять целесообразность применения тех или иных методов защиты; - анализировать статистику распределения данных после шифрования.	**Владеть:** - навыками шифрования в режиме ручного расчета; - навыками оценки сходимости методов преобразования; - навыками автоматизации этапов криптографического преобразования.
ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов	**Знать**: - классификацию методов шифрования; - модель криптосистемы с открытым ключом; - требования к качественной хеш-функции; - виды криптографических протоколов.	**Уметь**: - решать задачи криптографической защиты информации с использованием блочных и поточных систем; - решать задачи с использованием криптографических систем с открытым ключом; - решать задачи с использованием	**Владеть**: - навыками определения метода шифрования; -навыками автоматизации этапов криптографического преобразования.

		криптографических хеш-функций и протоколов.	
ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации	**Знать**: - основные виды угроз безопасности; - возможные каналы утечки конфиденциальной информации по техническим каналам; - принципы организации защиты информации от утечки по техническим каналам; - способы защиты информации от утечки по техническим каналам на объектах информатизации.	**Уметь**: - выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации; - определять каналы утечки информации; - организовывать мероприятия, направленные на защиту информации. - защищать информацию от утечки по техническим каналам на объектах информатизации.	**Владеть**: - способами защиты информации от утечки по техническим каналам на объектах информатизации; - навыками применения технических средств защиты информации; - навыками определения каналов утечки; - навыками планирования, контроля.
ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации	**Знать**: - угрозы информационной безопасности объекта информатизации.	**Уметь**: - оценивать угрозы информационной безопасности объекта информатизации.	**Владеть**: - способами предотвращения угрозам информационной безопасности объекта информатизации.
ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	**Знать**: - средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.	**Уметь**: - использовать средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - применять известные методики оценки угроз; - принимать технические меры, направленные на повышение защищенности и снижения рисков	**Владеть**: - навыками использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - методами проведения анализа угроз информационной безопасности.

		нарушения безопасности телекоммуникационных систем.	
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-10.1: Реализует требования политик безопасности на объектах информатизации	**Знать**: - требования политик безопасности на объектах информатизации; - систему хранения и обработки информации; - принципы идентификации записей.	**Уметь**: - применять политики безопасности на объектах информатизации; - организовывать выполнение мер по обеспечению информационной безопасности.	**Владеть**: - навыками применения политик безопасности на объектах информатизации; - навыками управления; - навыками создания локально-нормативных документов.
ОПК-10.2: Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	**Знать**: - основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы атак; - основные принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях; - сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации; - принципы функционирования	**Уметь**: - конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности; - выявлять слабости защиты ОС, ВС и СУБД и использовать их для вскрытия защиты; - планировать программно-аппаратную подсистему политики безопасности организации; - применять и администрировать средства программно-аппаратной защиты информации. - производить анализ эффективности программно-	**Владеть**: - навыками установки и настройки программно-аппаратных средств защиты информации в соответствии с заданными политиками безопасности; - методами администрирования операционных систем и баз данных; - методами защиты информации в операционных системах и в пользовательских приложениях; - способами выявления основных вредоносных программ и их нейтрализацией; - навыками анализа и администрирования подсистем защиты

	основных типов вредоносных программ, способы их выявления и нейтрализации.	аппаратных средств защиты информации в компьютерных сетях; - оценивать оптимальность выбора программно-аппаратных средств.	современных ОС, ВС и СУБД; - навыками использования межсетевых экранов и систем обнаружения вторжений.
ОПК-10.3: Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	**Знать**: - принципы построения компьютерных сетей, операционных систем; - стек сетевых протоколов операционных систем, стек протоколов сетевого оборудования; - порядок реализации методов и средств межсетевого экранирования; - принципы функционирования сетевых протоколов, включающих криптографические алгоритмы; - методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; - принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации; - нормативные правовые акты в области защиты	**Уметь**: - оценивать угрозы безопасности информации в компьютерных сетях, операционных системах, БД; - обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях; - выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях, ОС; - проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях, операционных системах; - конфигурировать средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях.	**Владеть**: - навыками определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях; - навыками разработки порядка применения программно-аппаратных средств защиты информации в компьютерных сетях; - навыками настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации; - навыками установки и настройки средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях.

	информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях.		
ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	**Знать**: - информационную инфраструктуру и информационные ресурсы, подлежащие защите.	**Уметь**: - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.	**Владеть**: - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите.
ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	**Знать**: - показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.	**Уметь**: - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.	**Владеть**: - навыками оценки систем и отдельных методов и средств защиты информации.
ОПК-12.3: Оценивает информационные риски в автоматизированны х системах	**Знать**: - информационные риски в автоматизированных системах.	**Уметь**: - оценивать информационные риски в автоматизированных системах.	**Владеть**: - навыками оценки информационных рисков в автоматизированных системах.
ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений	**Знать**: - основные методы управления информационной безопасностью; - основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов; - основные отечественные и	**Уметь**: - проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня	**Владеть**: - навыками управления информационной безопасности; - навыками подготовки исходных данных для проектирования подсистем; - навыками оценки эффективности проектных решений;

	зарубежные стандарты в области защиты информации; -основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); - угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах; - основные показатели технико-экономического обоснования соответствующих проектных решений.	защищенности; - исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности; -проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации; - разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений.	- навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений.
ОПК-4.1: Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем	**Знать**: - подлежащие защите информационные ресурсы автоматизированных систем.	**Уметь**: - определять подлежащие защите информационные ресурсы автоматизированных систем.	**Владеть**: - навыками определения подлежащих защите информационных ресурсов автоматизированных систем.
ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в	**Знать**: - принципы и методы обеспечения защиты информации в автоматизированной системе.	**Уметь**: - составлять комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в	**Владеть**: - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты

автоматизированной системе		автоматизированной системе.	информации в автоматизированной системе.
ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации	**Знать**: - принципы и методы обеспечения защиты информации в автоматизированной системе.	**Уметь**: - составлять комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе.	**Владеть**: - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе.
ОПК-4.1.4: Организует работу персонала автоматизированной системы с учетом требований по защите информации	**Знать**: - требования по защите информации.	**Уметь**: - разрабатывать организационно-распорядительные документы по защите информации.	**Владеть**: - навыками разработки организационно-распорядительных документов по обеспечения защиты информации в автоматизированной системе.
ОПК-4.3: Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-4.3.1: Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы	**Знать**: - принципы автономной наладки технических и программных средств системы защиты информации автоматизированной системы; - порядок эксплуатации средств антивирусной защиты; - порядок обеспечения	**Уметь**: - устанавливать программные и технические средства в соответствии с технической документацией; -производить настройку параметров работы технических и программных средств; - осуществлять автономную наладку	**Владеть**: - навыками установки антивирусной защиты; - навыками настройки встроенных средств защиты информации программного обеспечения; - навыками проверки работоспособности отдельных программных, программно-

	безопасности при эксплуатации технических и программных средств; - порядок администрирования технических и программных средств системы защиты информации автоматизированной системы.	технических и программных средств системы защиты информации автоматизированной системы.	аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем.
ОПК-4.3.2: Применяет программные средства обеспечения безопасности данных	**Знать**: - порядок применения программных средства обеспечения безопасности данных; - перечень информации, подлежащей резервному копированию; - методику проведения резервного копирования; - принципы восстановления информации в автоматизированных системах.	**Уметь**: - применять программные средства обеспечения безопасности данных; - применять типовые программные средства резервирования и восстановления информации в автоматизированных системах; - настраивать систему резервного копирования; - проверять корректность резервной копии.	**Владеть**: - навыками применения программных средства обеспечения безопасности данных; - навыками фильтрации информации, подлежащей резервному копированию; - навыками применения методик резервного копирования и восстановления.
ОПК-4.3.3: Управляет полномочиями пользователей автоматизированной системы	**Знать**: - порядок разграничения доступа к информационным ресурсам.	**Уметь**: - применять политики безопасности в автоматизированной системе.	**Владеть**: - навыками управления полномочиями пользователей автоматизированной системы.

5 КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ (ЭКСПЛУАТАЦИОННОЙ)

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Промежуточная аттестация по учебной практике осуществляется в форме зачета с оценкой. Для получения зачета обучающийся представляет отчет, который выполняется по результатам прохождения практики с учетом (анализом) результатов проведенных работ и отзывом руководителя практики.

5.1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Основными этапами формирования универсальных и общепрофессиональных компетенций при прохождении производственной практики (технологической) являются последовательное прохождение содержательно связанных между собой этапов практики. Выполнение каждого этапа предполагает овладение обучающимися необходимыми элементами компетенций на уровне знаний, умений и навыков (таблица 5.1).

Таблица 5.1 – Критерии определения сформированности компетенций на различных этапах их формирования

Критерии оценивания этапов формирования компетенции	Уровни сформированности компетенций		
	Низкий (пороговый)	Средний	Высокий
	Компетенция сформирована. Демонстрируется недостаточный уровень самостоятельности практического навыка	Компетенция сформирована. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка	Компетенция сформирована. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
Уровень знаний	Теоретическое содержание освоено частично, есть несущественные пробелы, неточности и недочеты при выполнении заданий	Теоретическое содержание освоено полностью, без пробелов, некоторые практические навыки сформированы на достаточном уровне	Теоретическое содержание освоено полностью, на высоком уровне
Уровень умений	Необходимые умения, предусмотренные программой практики, в основном сформированы	Некоторые практические навыки сформированы на достаточном уровне	Практические навыки, предусмотренные программой практики, сформированы полностью
Уровень овладения навыками и (или) опыта деятельности	Необходимые практические навыки, предусмотренные программой практики, в основном освоены	Некоторые практические навыки освоены на достаточном уровне	Практические навыки, предусмотренные программой практики, освоены полностью

Итоговая оценка, полученная с учетом оценивания компетенций на различных этапах их формирования, показывает успешность освоения компетенций обучающимися.

Процесс прохождения практики обеспечивает формирование сразу несколько компетенций, критерии оценки целесообразно формировать в два этапа.

1-й этап: определение критериев оценки отдельно по каждой формируемой компетенции. Сущность 1-го этапа состоит в определении критериев для оценивания отдельно взятой компетенции на основе

продемонстрированного студентом уровня овладения соответствующими знаниями, умениями и навыками.

2-й этап: определение критериев для оценки уровня обученности по итогам практики на основе комплексного подхода к уровню сформированости всех компетенций, обязательных к формированию в процессе ее прохождения. Сущность 2-го этапа определения критерия оценки по практике заключена в определении подхода к оцениванию на основе ранее полученных данных об уровне сформированности каждой компетенции, обязательной к выработке в процессе прохождения этапа практики.

В качестве основного критерия при оценке итогов прохождения практики является наличие у обучающегося сформированных компетенций. Показатели оценивания компетенций и шкалы оценки приведены в таблице 5.2:

Зачтено (с оценкой «отлично»), (90 – 100 баллов) выставляют обучающемуся, который:

– выполнил весь объем работы, предусмотренный программой практики и индивидуальным заданием;

– соблюдал трудовую дисциплину, подчинялся действующим на предприятии правилам внутреннего трудового распорядка, систематически вел дневник, в котором записывал объем выполненной работы за каждый день практики;

– своевременно предоставил отчет о прохождении Производственной практики и отзыв-характеристику руководителя практики от предприятия, оформленный в соответствии с требованиями программы практики;

– содержание разделов отчета по практике соответствует требуемой структуре отчета, имеет четкое построение, логическую последовательность изложения материала, доказательность выводов и обоснованность рекомендаций;

– в докладе демонстрирует отличные знания и умения, предусмотренные программой практики, аргументировано и в логической последовательности излагает материал, использует точные краткие формулировки.

Зачтено (с оценкой «хорошо»), (70 – 89 баллов) выставляют обучающемуся, который:

– выполнил весь объем работы, предусмотренный программой практики и индивидуальным заданием;

– соблюдал трудовую дисциплину, подчинялся действующим на предприятии правилам внутреннего трудового распорядка, систематически вел дневник, в котором записывал объем выполненной работы за каждый день практики;

– своевременно представил отчет о прохождении практики и отзыв-характеристику руководителя практики от предприятия, оформленный в соответствии с требованиями программы практики;

– содержание разделов отчета по практике в основном соответствует требуемой структуре отчета, однако имеет отдельные отклонения и неточности в построении, логической последовательности изложения материала, выводов и рекомендаций;

– в докладе демонстрирует твердые знания программного материала, грамотно и, по существу, излагает его, не допускает существенных неточностей в ответах, правильно применяет теоретические положения при анализе практических ситуаций.

Зачтено (с оценкой «удовлетворительно») (51 – 69 баллов) выставляют обучающемуся, который:

– выполнил весь объем работы, предусмотренный программой практики и индивидуальным заданием;

– соблюдал трудовую дисциплину, подчинялся действующим на предприятии правилам внутреннего трудового распорядка, систематически

вел дневник, в котором записывал объем выполненной работы за каждый день практики;

– предоставил отчет о прохождении практики и отзыв-характеристику руководителя практики от предприятия, оформленный в соответствии с требованиями программы практики;

– содержание разделов отчета по практике, в основном, соответствует требуемой структуре отчета, однако нарушена логическая последовательность изложения материала, выводы и рекомендации некорректны;

– в докладе демонстрирует удовлетворительные знания и умения, предусмотренные программой практики.

Не зачтено (с оценкой «неудовлетворительно») (0-50 баллов) выставляют обучающемуся, который:

– выполнил весь объем работы, предусмотренный программой практики и индивидуальным заданием;

– не соблюдал трудовую дисциплину, не подчинялся действующим на предприятии правилам внутреннего трудового распорядка, периодически вел дневник, в котором записывал объем выполненной работы практики;

– содержание разделов отчета по практике, в основном, соответствует требуемой структуре отчета, однако нарушена логическая последовательность изложения материала, выводы и рекомендации некорректны.

Таблица 5.2 – Измерительная шкала для оценки уровня сформированности компетенций по производственной практике (технологическая)

Не зачтено (с оценкой «неудовлетворительно») или отсутствие сформированности компетенций	Зачтено (с оценкой «удовлетворительно») или низкой уровень освоения компетенции	Зачтено (с оценкой «хорошо») или средний уровень освоения компетенции	Зачтено (с оценкой «отлично») или высокий уровень освоения компетенции
1 этап			
Студент демонстрирует неспособность применять соответствующие знания, умения и навыки при выполнении задания по практике. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах прохождения практики.	Студент демонстрирует наличие базовых знаний, умений и навыков при выполнении задания по практике, но их уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне.	Студент демонстрирует наличие соответствующих знаний, умений и навыков при выполнении задания по практике на достаточном уровне. Наличие сформированной компетенции на достаточном уровне следует оценивать как положительное и устойчиво закрепленное в практическом навыке.	Студент демонстрирует наличие соответствующих знаний, умений и навыков при выполнении задания по практике на повышенном уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой активности практического применения к изменяющимся условиям профессиональной задачи позволяет дать высокую оценку.
2 этап			
Уровень освоение программы практики, при котором у обучающегося не сформировано более 50% компетенций. Если практика выступает в качестве итогового этапа формирования компетенции оценка «неудовлетворительно» выставляется при отсутствии сформированности хотя бы одной	При наличии более 50% сформированных компетенций по практике, имеющим возможность до формирования компетенций на последующих этапах обучения. Для практик итогового формирования компетенций ставится оценка «удовлетворительно», если сформированы более 60% компетенций.	Для определения уровня освоения промежуточной практики на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных компетенций, из которых не менее 75% оценены отметкой «хорошо».	Оценка «отлично» по практике с промежуточным освоением компетенций, ставится при 100% подтверждении наличия компетенций, либо при 90% сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения практики с итоговым

компетенции	При наличии более 50 – 69% сформированных компетенций.	Оценивание итоговой практики на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций, причем не менее 60% компетенций должны быть сформированы на повышенном уровне, то есть с оценкой «хорошо». Наличие 70-89% сформированных компетенций.	формированием компетенций оценка «отлично» ставится при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% компетенций. При 90 – 100% подтверждении уровня сформированности компетенций.

Таблица 5.3 – Критерии оценивания уровня сформированности компетенций по производственной практике (технологическая)

Планируемые результаты обучения /Уровень сформированности компетенций	Критерии оценивания			
	«Неудовлетворительно» / нулевой уровень	«Удовлетворительно» /низкий уровень	«Хорошо» / средний уровень	«Отлично» / высокий уровень
ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ ОПК-1; ОПК-5; ОПК-6; ОПК-9; ОПК-10; ОПК-12; ОПК-4.1; ОПК-4.3				
Теоретические показатели				
ОПК-1.1: Классифицирует угрозы информационной безопасности в соответствии с нормативными документами ОПК-1.2: Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности	Обучающийся **не знает:** - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации; - нормативно-правовые аспекты обеспечения	Обучающийся **частично знает:** - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации;	Обучающийся **знает:** - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации; - нормативно-правовые	Обучающийся полностью **знает** - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации;

Российской Федерации ОПК-1.3: Определяет угрозы информационной безопасности для различных систем ОПК-5.1: Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ОПК-5.2: Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.3: Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	информационной безопасности РФ; - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность; - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности; - правовые основы организации защиты конфиденциальной информации; - задачи органов защиты информации; - правовые нормы и стандарты по защите конфиденциальной информации, персональных данных и охране	- нормативно-правовые аспекты обеспечения информационной безопасности РФ; - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность; - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности; - правовые основы организации защиты конфиденциальной информации; - задачи органов защиты информации; - правовые нормы и	аспекты обеспечения информационной безопасности РФ; - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность; - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности; - правовые основы организации защиты конфиденциальной информации; - задачи органов защиты информации;	- нормативно-правовые аспекты обеспечения информационной безопасности РФ; - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность; - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности; - правовые основы

ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-6.2: Определяет политику контроля доступа работников к информации ограниченного доступа ОПК-6.3: Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации ОПК-6.4: Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем	результатов интеллектуальной деятельности в организации; - принципы формирования политики информационной безопасности в автоматизированных системах; - правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; - основные отечественные и зарубежные стандарты в области информационной безопасности; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - модели угроз и модели нарушителя; - модели разграничения	стандарты по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - принципы формирования политики информационной безопасности в автоматизированных системах; - правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; - основные отечественные и зарубежные стандарты в области информационной безопасности; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - основные требования,	- правовые нормы и стандарты по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - принципы формирования политики информационной безопасности в автоматизированных системах; - правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; - основные отечественные и зарубежные стандарты в области информационной безопасности; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и	организации защиты конфиденциальной информации; - задачи органов защиты информации; - правовые нормы и стандарты по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - принципы формирования политики информационной безопасности в автоматизированных системах; - правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; - основные отечественные и зарубежные стандарты в области информационной

шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов	доступа к информации ограниченного доступа; - требования руководящих документов по физической защите объектов информатизации; - требования по пропускному режиму в организации; - требования руководящих документов регламентирующих защиту информации ограниченного доступа; - основы криптографии, методы защиты; - классификацию криптографических методов; - основы шифрования с помощью ассиметричных алгоритмов; - классификацию методов шифрования; - модель криптосистемы с открытым ключом; - способы защиты информации от утечки по техническим каналам на объектах информатизации; - угрозы информационной безопасности объекта информатизации; - средства защиты	предъявляемые к сотрудникам защиты информации ограниченного доступа; - модели угроз и модели нарушителя; - модели разграничения доступа к информации ограниченного доступа; - требования руководящих документов по физической защите объектов информатизации; - требования по пропускному режиму в организации; - требования руководящих документов регламентирующих защиту информации ограниченного доступа; - основы криптографии, методы защиты; - классификацию криптографических методов; - основы шифрования с помощью ассиметричных алгоритмов; - классификацию методов шифрования; - модель криптосистемы с открытым ключом;	систем; - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - модели угроз и модели нарушителя; - модели разграничения доступа к информации ограниченного доступа; - требования руководящих документов по физической защите объектов информатизации; - требования по пропускному режиму в организации; - требования руководящих документов регламентирующих защиту информации ограниченного доступа; - основы криптографии, методы защиты; - классификацию криптографических методов; - основы шифрования с помощью ассиметричных алгоритмов; - классификацию методов шифрования;	безопасности; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - модели угроз и модели нарушителя; - модели разграничения доступа к информации ограниченного доступа; - требования руководящих документов по физической защите объектов информатизации; - требования по пропускному режиму в организации; - требования руководящих
ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации				
ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации				
ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации				
ОПК-10.1: Реализует требования политик безопасности на объектах информатизации				
ОПК-10.2: Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности				
ОПК-10.3: Применяет средства защиты информации в типовых операционных системах, системах				

управления базами данных, компьютерных сетях ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-12.3: Оценивает информационные риски в автоматизированных системах ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в	информации от утечки по техническим каналам; - состав, назначение и технические характеристики программно-аппаратных средств защиты информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - информационные риски в автоматизированных системах; - принципы и методы обеспечения защиты информации в автоматизированной системе; - порядок применения программных средства обеспечения безопасности данных; - порядок разграничения	- способы защиты информации от утечки по техническим каналам на объектах информатизации; - угрозы информационной безопасности объекта информатизации; - средства защиты информации от утечки по техническим каналам; - состав, назначение и технические характеристики программно-аппаратных средств защиты информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - информационные риски в автоматизированных	- модель криптосистемы с открытым ключом; - способы защиты информации от утечки по техническим каналам на объектах информатизации; - угрозы информационной безопасности объекта информатизации; - средства защиты информации от утечки по техническим каналам; - состав, назначение и технические характеристики программно-аппаратных средств защиты информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	документов регламентирующих защиту информации ограниченного доступа; - основы криптографии, методы защиты; - классификацию криптографических методов; - основы шифрования с помощью ассиметричных алгоритмов; - классификацию методов шифрования; - модель криптосистемы с открытым ключом; - способы защиты информации от утечки по техническим каналам на объектах информатизации; - угрозы информационной безопасности объекта информатизации; - средства защиты информации от утечки по

автоматизированной системе ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации ОПК-4.1.4: Организует работу персонала автоматизированной системы с учетом требований по защите информации ОПК-4.3.1: Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы ОПК-4.3.2: Применяет программные средства обеспечения безопасности данных ОПК-4.3.3: Управляет полномочиями пользователей автоматизированной системы	доступа к информационным ресурсам.	системах; - принципы и методы обеспечения защиты информации в автоматизированной системе; - порядок применения программных средства обеспечения безопасности данных; - порядок разграничения доступа к информационным ресурсам.	- информационные риски в автоматизированных системах; - принципы и методы обеспечения защиты информации в автоматизированной системе; - порядок применения программных средства обеспечения безопасности данных; - порядок разграничения доступа к информационным ресурсам.	техническим каналам; - состав, назначение и технические характеристики программно-аппаратных средств защиты информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - информационные риски в автоматизированных системах; - принципы и методы обеспечения защиты информации в автоматизированной системе; - порядок применения программных средства обеспечения безопасности данных;

				- порядок разграничения доступа к информационным ресурсам.
Практические показатели				
ОПК-1.1: Классифицирует угрозы информационной безопасности в соответствии с нормативными документами ОПК-1.2: Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации ОПК-1.3: Определяет угрозы информационной безопасности для различных систем ОПК-5.1: Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ОПК-5.2: Формулирует	Обучающийся **не умеет:** - выявлять угрозы информационной безопасности; - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты; - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы; - применять действующую законодательную базу в области обеспечения информационной безопасности; - классифицировать	Обучающийся **частично умеет:** - выявлять угрозы информационной безопасности; - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты; - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы; - применять действующую законодательную базу в	Обучающийся **умеет:** - выявлять угрозы информационной безопасности; - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты; - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы; - применять действующую законодательную базу в области обеспечения	Обучающийся **умеет на высоком уровне:** - выявлять угрозы информационной безопасности; - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты; - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые

основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.3: Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-6.2: Определяет политику контроля доступа работников к информации ограниченного доступа ОПК-6.3: Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации ОПК-6.4: Разрабатывает проекты инструкций,	защищаемую информацию по видам тайны и степеням конфиденциальности; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - применять действующую законодательную базу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;	области обеспечения информационной безопасности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - применять действующую законодательную базу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - разрабатывать проекты локальных правовых актов, инструкций,	информационной безопасности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - применять действующую законодательную базу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и	и составные запросы; - применять действующую законодательную базу в области обеспечения информационной безопасности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - применять действующую законодательную базу по защите конфиденциальной информации, персональных данных

регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	- применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа; - разрабатывать модели угроз объекта информатизации; - применять политику разграничения доступа к	регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности	организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;	и охране результатов интеллектуальной деятельности в организации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - разрабатывать

ОПК-10.1: Реализует требования политик безопасности на объектах информатизации ОПК-10.2: Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности ОПК-10.3: Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-12.3: Оценивает информационные риски в автоматизированных системах ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования	информации ограниченного доступа; - использовать средства физической защиты объекта информатизации; - выполнять шифрование криптографическими методами; - решать задачи криптографической защиты информации с использованием блочных и поточных систем; - решать задачи с использованием криптографических систем с открытым ключом; - решать задачи с использованием криптографических хеш-функций и протоколов; - защищать информацию от утечки по техническим каналам на объектах информатизации; - оценивать угрозы информационной безопасности объекта информатизации; - конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками	информации; - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа; - разрабатывать модели угроз объекта информатизации; - применять политику разграничения доступа к информации ограниченного доступа; - использовать средства физической защиты объекта информатизации; - выполнять шифрование криптографическими методами; - решать задачи криптографической защиты информации с использованием блочных и поточных систем; - решать задачи с использованием криптографических систем с открытым	- составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа; - разрабатывать модели угроз объекта информатизации; - применять политику разграничения доступа к информации ограниченного доступа; - использовать средства физической защиты объекта информатизации; - выполнять шифрование криптографическими методами; - решать задачи криптографической защиты информации с использованием блочных и поточных систем; - решать задачи с использованием криптографических систем с открытым	проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа; - разрабатывать модели угроз объекта информатизации; - применять политику разграничения доступа к информации ограниченного

соответствующих проектных решений	безопасности; - оценивать информационные риски в автоматизированных системах; - определять подлежащие защите информационные ресурсы автоматизированных систем; - составлять комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - разрабатывать организационно-распорядительные документы по защите информации; - применять программные средства обеспечения безопасности данных; - применять политики безопасности в автоматизированной системе.	ключом; - решать задачи с использованием криптографических хеш-функций и протоколов; - защищать информацию от утечки по техническим каналам на объектах информатизации; - оценивать угрозы информационной безопасности объекта информатизации; - конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности; - оценивать информационные риски в автоматизированных системах; - определять подлежащие защите информационные ресурсы автоматизированных систем; - составлять комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения	ключом; - решать задачи с использованием криптографических хеш-функций и протоколов; - защищать информацию от утечки по техническим каналам на объектах информатизации; - оценивать угрозы информационной безопасности объекта информатизации; - конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности; - оценивать информационные риски в автоматизированных системах; - определять подлежащие защите информационные ресурсы автоматизированных систем; - составлять комплексы правил, процедур, практических приемов, принципов и методов,	доступа; - использовать средства физической защиты объекта информатизации; - выполнять шифрование криптографическими методами; - решать задачи криптографической защиты информации с использованием блочных и поточных систем; - решать задачи с использованием криптографических систем с открытым ключом; - решать задачи с использованием криптографических хеш-функций и протоколов; - защищать информацию от утечки по техническим каналам на объектах информатизации; - оценивать угрозы информационной безопасности объекта
ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем				
ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе				
ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации				
ОПК-4.1.4: Организует работу персонала автоматизированной системы с учетом требований по защите информации				
ОПК-4.3.1: Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы				
ОПК-4.3.2: Применяет программные средства обеспечения безопасности				

данных ОПК-4.3.3: Управляет полномочиями пользователей автоматизированной системы		защиты информации в автоматизированной системе; - разрабатывать организационно-распорядительные документы по защите информации; - применять программные средства обеспечения безопасности данных; - применять политики безопасности в автоматизированной системе.	средств обеспечения защиты информации в автоматизированной системе; - разрабатывать организационно-распорядительные документы по защите информации; - применять программные средства обеспечения безопасности данных; - применять политики безопасности в автоматизированной системе.	информатизации; - конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности; - оценивать информационные риски в автоматизированных системах; - определять подлежащие защите информационные ресурсы автоматизированных систем; - составлять комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - разрабатывать организационно-распорядительные документы по защите

				информации; - применять программные средства обеспечения безопасности данных; - применять политики безопасности в автоматизированной системе.
Практико-ориентированные показатели (навыки)				
ОПК-1.1: Классифицирует угрозы информационной безопасности в соответствии с нормативными документами ОПК-1.2: Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации ОПК-1.3: Определяет угрозы информационной безопасности для различных систем ОПК-5.1: Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по	Обучающийся **не владеет:** - навыками классификации угроз; - навыками выявления уязвимостей технических каналов связи информационных систем; - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий; - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур; - навыками работы с нормативными правовыми актами;	Обучающийся **частично владеет:** - навыками классификации угроз; - навыками выявления уязвимостей технических каналов связи информационных систем; - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий; - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками	Обучающийся **владеет на среднем уровне:** - навыками классификации угроз; - навыками выявления уязвимостей технических каналов связи информационных систем; - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий; - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур;	Обучающийся **владеет на высоком уровне:** - навыками классификации угроз; - навыками выявления уязвимостей технических каналов связи информационных систем; - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий; - общими приемами организации поиска;

обеспечению информационной безопасности в организации ОПК-5.2: Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.3: Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-6.2: Определяет политику контроля доступа работников к информации ограниченного доступа ОПК-6.3: Формулирует требования, предъявляемые к физической защите объекта и	- навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - навыками работы с нормативными правовыми актами;	программирования поисковых процедур; - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации, персональных данных и	- навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;	- алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур; - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов,

пропускному режиму в организации	- навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; - навыками разработки модели угроз и модели нарушителя объекта информатизации; - навыками контроля политики разграничения доступа к информации ограниченного доступа; - навыками организации и контроля пропускного режима; - навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа; - навыками автоматизации этапов криптографического преобразования; - способами защиты информации от утечки по техническим каналам на	охране результатов интеллектуальной деятельности в организации; - навыками работы с нормативными правовыми актами; - навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; - навыками разработки модели угроз и модели нарушителя объекта информатизации; - навыками контроля политики разграничения доступа к информации ограниченного доступа; - навыками организации и контроля пропускного режима; - навыками разработки проектов инструкций, регламентов, положений и приказов,	- навыками работы с нормативными правовыми актами; - навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; - навыками разработки модели угроз и модели нарушителя объекта информатизации; - навыками контроля политики разграничения доступа к информации ограниченного доступа; - навыками организации и контроля пропускного режима; - навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа; - навыками автоматизации этапов	регламентирующих работу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - навыками работы с нормативными правовыми актами; - навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; - навыками разработки модели угроз и модели нарушителя объекта информатизации; - навыками контроля политики разграничения доступа к
ОПК-6.4: Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации				
ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах				
ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов				
ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации				
ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации				
ОПК-9.5: Использует средства				

защиты информации от утечки по техническим каналам и контроля эффективности защиты информации ОПК-10.1: Реализует требования политик безопасности на объектах информатизации ОПК-10.2: Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности ОПК-10.3: Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-12.3: Оценивает информационные риски в	объектах информатизации; - способами предотвращения угрозам информационной безопасности объекта информатизации; - навыками использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - навыками применения политик безопасности на объектах информатизации; - навыками установки и настройки программно-аппаратных средств защиты информации в соответствии с заданными политиками безопасности; - навыками установки и настройки средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите;	регламентирующих защиту информации ограниченного доступа; - навыками автоматизации этапов криптографического преобразования; - способами защиты информации от утечки по техническим каналам на объектах информатизации; - способами предотвращения угрозам информационной безопасности объекта информатизации; - навыками использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - навыками применения политик безопасности на объектах информатизации; - навыками установки и настройки программно-аппаратных средств защиты информации в соответствии с заданными политиками	криптографического преобразования; - способами защиты информации от утечки по техническим каналам на объектах информатизации; - способами предотвращения угрозам информационной безопасности объекта информатизации; - навыками использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - навыками применения политик безопасности на объектах информатизации; - навыками установки и настройки программно-аппаратных средств защиты информации в соответствии с заданными политиками безопасности; - навыками установки и настройки средств защиты информации в типовых операционных системах, системах	информации ограниченного доступа; - навыками организации и контроля пропускного режима; - навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа; - навыками автоматизации этапов криптографического преобразования; - способами защиты информации от утечки по техническим каналам на объектах информатизации; - способами предотвращения угрозам информационной безопасности объекта информатизации; - навыками

автоматизированных системах ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации ОПК-4.1.4: Организует работу персонала автоматизированной системы с учетом требований по защите информации ОПК-4.3.1: Осуществляет автономную наладку технических и программных средств системы защиты информации	- навыками оценки информационных рисков в автоматизированных системах; - навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений; - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - навыками разработки организационно-распорядительных документов по обеспечения защиты информации в автоматизированной системе; - навыками проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	безопасности; - навыками установки и настройки средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - навыками оценки информационных рисков в автоматизированных системах; - навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений; - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе;	управления базами данных, компьютерных сетях; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - навыками оценки информационных рисков в автоматизированных системах; - навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений; - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - навыками разработки организационно-распорядительных документов по обеспечения защиты информации в	использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - навыками применения политик безопасности на объектах информатизации; - навыками установки и настройки программно-аппаратных средств защиты информации в соответствии с заданными политиками безопасности; - навыками установки и настройки средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - навыками определения информационной

автоматизированной системы ОПК-4.3.2: Применяет программные средства обеспечения безопасности данных ОПК-4.3.3: Управляет полномочиями пользователей автоматизированной системы	автоматизированных систем; - навыками управления полномочиями пользователей автоматизированной системы.	- навыками разработки организационно-распорядительных документов по обеспечения защиты информации в автоматизированной системе; - навыками проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем; - навыками управления полномочиями пользователей автоматизированной системы.	автоматизированной системе; - навыками проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем; - навыками управления полномочиями пользователей автоматизированной системы.	инфраструктуры и информационных ресурсов организации, подлежащих защите; - навыками оценки информационных рисков в автоматизированных системах; - навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений; - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - навыками разработки организационно-распорядительных документов по обеспечения защиты информации в

				автоматизированной системе; - навыками проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем; - навыками управления полномочиями пользователей автоматизированной системы.

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 5.4 – Примерный перечень заданий производственной практики (технологической) 4 курс 8 семестр ОФО, 5 курс 10 семестр ЗФО

Разделы (этапы) практики	Суть этапа практики	Комплект заданий, позволяющий оценить уровень знаний, умений и навыков	Контролируемые компетенции
Организация практики, подготовительный этап, включающий инструктаж по технике безопасности	Получение задания от руководителя практики, ознакомление с документами на практику	Распределение фонда рабочего времени в период практики; Получение программы практики и индивидуального задания	ОПК-1
Содержательный этап	Выполнение практических работ	Знакомство с содержанием деятельности подразделения по обеспечению информационной безопасности и проводимыми им мероприятиями. Изучение нормативных правовых актов организации по обеспечению информационной безопасности (политика безопасности организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	ОПК-5 ОПК-10
Содержательный этап	Выполнение индивидуального задания (Варианты заданий разрабатываются и утверждаются кафедрой за 1 месяц до начала практик.)	Самостоятельное проведение мониторинга и (или) производственного контроля эффективности применения средств защиты информации в ТКС. Организация работы 2-3 человек и руководство их работой в процессе формулирования предложений по совершенствованию системы защиты информации в ТКС. Создание плана работы коллектива из 3 – 4 человек, реализующего	ОПК-1 ОПК-5 ОПК-6 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.3

		политику безопасности в ТКС. Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. Формирование систематизированной инструкции по эксплуатации конкретного средства защиты информации в конкретной ТКС. Самостоятельное проведение уценки угроз информационной безопасности, возможных каналов утечек конфиденциальных данных в ТКС. Оценка рисков информационной безопасности. Самостоятельная подготовка рекомендаций по повышению уровня информационной безопасности предприятия. Организация работы 2-3 человек и руководство их работой в процессе подготовки рекомендаций по проведению регламентных работ по обнаружению уязвимостей ТКС. Самостоятельное составление рекомендаций по отказоустойчивой эксплуатации защищённых ТКС. Представление перечня средств и мер по обеспечению отказоустойчивости системы. Представление результатов руководителю практики от организации.	
Отчетный этап	Выработка по итогам прохождения практики выводов и предложений, оформление отчета по практике и его защита	Формулирование основных выводов Написание текста отчета Оформление отчета по практике и представление на проверку руководителю Подготовка к защите отчета по практике	ОПК-1

5.3 Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

Таблица 5.6 – Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности обучающихся в результате прохождения практики (учебно-лабораторной)

Формы контроля	Оценочное средство	Процедура оценивания (краткая характеристика оценочного средства)
Текущий контроль	Наблюдение	Средство контроля, которое является основным методом при текущем контроле, проводится с целью измерения частоты, длительности, топологии действий студентов, обычно в естественных условиях с применением не интерактивных методов
Рубежный контроль	Индивидуальное задание (разделы отчета по практике)	Частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся
Промежуточный контроль	Защита отчета по практике	Отчет является специфической формой письменных работ, позволяющей студенту обобщить свои знания, умения и навыки, приобретенные за время прохождения учебных практик. Отчеты по практике готовятся индивидуально. Цель каждого отчета – осознать и зафиксировать компетенции, приобретенные студентом в результате освоения теоретических курсов и полученные им при прохождении практики

6 УСЛОВИЯ РЕАЛИЗАЦИИ ПРАКТИКИ ДЛЯ ОБУЧАЮЩИХСЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для студентов из числа лиц с ограниченными возможностями здоровья практика проводится Академией с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья.

При проведении практики обеспечивается соблюдение следующих общих требований:

– проведение практики для лиц с ограниченными возможностями здоровья в одной аудитории совместно со студентами, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для них в процессе обучения;

– присутствие в аудитории ассистента, оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем);

– пользование необходимыми обучающимся техническими средствами при выполнении практических и других работ в соответствии с учебным планом с учетом их индивидуальных особенностей;

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья образовательная среда Академии обеспечивает выполнение следующих требований при организации учебной практики:

а) для слепых:

– задания и иные материалы для аттестации зачитываются ассистентом;

– письменные задания надиктовываются обучающимся ассистенту;

б) для слабовидящих:

– задания и иные учебно-методические материалы оформляются увеличенным шрифтом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

– обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

– по их желанию аттестационные испытания проводятся в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

– письменные задания надиктовываются ассистенту;

– по их желанию все аттестационные испытания проводятся в устной форме.

7 УЧЕБНО-МЕТОДИЧЕСКОЕ, ИНФОРМАЦИОННОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ЭКСПЛУАТАЦИОННАЯ)

7.1 Основная литература

1. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты : практическое руководство / А. А. Петров. - 2-е изд. - Москва : ДМК Пресс, 2023. - 451 с. - ISBN 978-5-89818-453-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/2106222. – Режим доступа: по подписке.
2. 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.
3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598. – Режим доступа: по подписке.
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. - Москва : Форум, 2021. - 416 с. - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://ibooks.ru/bookshelf/361273/reading. – Режим доступа: по подписке.
5. Мельников, В. П., Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. — Москва : КноРус, 2023. — 371 с. — ISBN 978-5-406-11960-0. — URL: https://book.ru/book/950148. — Текст : электронный.
6. Николаев, Н. С., Управление информационной безопасностью : учебник / Н. С. Николаев. — Москва : КноРус, 2021. — 188 с. — ISBN 978-5-406-07325-4. — URL: https://book.ru/book/939841. — Текст : электронный.
7. Организационно-правовое обеспечение информационной безопасности : учебник / под ред. А. А. Александрова, М. П. Сычева. - Москва : МГТУ им. Баумана, 2018. - 292 с. - ISBN 978-5-7038-4723-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/2010603. – Режим доступа: по подписке.
8. Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства : учебное пособие / В. В. Бондарев. - Москва : МГТУ им. Баумана, 2017. - 227 с. - ISBN 978-5-7038-4757-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/2010601. – Режим доступа: по подписке.
9. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. — 2-е изд., эл. / В.Ф. Шаньгин. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-

5-89818-506-0. - URL: https://ibooks.ru/bookshelf/392204/reading. - Текст: электронный.
10. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления / И.С. Клименко. - Москва : Инфра-М, 2021. - 180 с. - ISBN 978-5-16-015149-6. - URL: https://ibooks.ru/bookshelf/378012/reading. - Текст: электронный.

7.2 Дополнительная литература

1. 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.
2. 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.
3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-5-89818-506-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2107178. – Режим доступа: по подписке.
4. Крамаров С.О. Криптографическая защита информации / С.О. Крамаров, Е.Н. Тищенко, С.В. Соколов. - Москва : ИЦ РИОР, 2021. - 324 с. - ISBN 978-5-369-01716-6. - URL: https://ibooks.ru/bookshelf/361333/reading. - Текст: электронный.
5. Крылов, Г. О., Базовые понятия информационной безопасности : учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. — Москва : Русайнс, 2023. — 257 с. — ISBN 978-5-466-01996-4. — URL: https://book.ru/book/946979. — Текст : электронный.
6. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»
7. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
8. Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»

9. ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»
10. ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»
11. ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»
12. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»
13. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
14. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»
15. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»
16. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер»
17. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»
18. ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности»
19. ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология. Уровни целостности систем и программных средств»
20. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»
21. ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и

средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
22. ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки»
23. ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»
24. ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»
25. ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»
26. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»
27. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»
28. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»
29. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
30. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хеширования»
31. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2008)
32. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» (СТО БР ИББС-1.1-2007)
33. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО

БР ИББС-1.0-2008» (СТО БР ИББС-1.2-2009)

34. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» (РС БР ИББС-2.0-2007)
35. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0» (РС БР ИББС-2.1-2007)
36. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» (РС БР ИББС-2.2-2009)
37. Описание формы предоставления результатов оценки уровня информационной безопасности организаций банковской системы Российской Федерации

7.3 Периодические издания

1. Электронный научный журнал Вычислительные методы и программирование. Новые вычислительные технологии ISSN 1726-3522, doi 10.26089/NumMet.Journal. -Режим доступа http://num-meth.srcc.msu.ru/
2. Журнал Фундаментальная и прикладная математика. – М.: Изд-во МГУ. – Режим доступа http://mech.math.msu.su/~fpm/
3. Журнал Continuum. Математика. Информатика. Образование- Елец: Изд-во Елецкий государственный университет им. И.А. Бунина. Режим доступа: https://elibrary.ru/contents.asp?titleid=58830
4. Журнал Прикладная информатика. М.: Изд-во Московский финансово-промышленный университет "Синергия". – Режим доступа: https://elibrary.ru/contents.asp?titleid=25599
5. Научно-технический журнал «Информационные технологии и вычислительные системы». – М.: Изд-во «Новые технологии». ISSN 1684-6400. Режим доступа: http://www.novtex.ru/IT/
6. Научно-технический журнал «Информационные ресурсы России». – М.: Федеральное государственное бюджетное учреждение Российское энергетическое агентство Министерства энергетики Российской Федерации. Режим доступа: https://elibrary.ru/contents.asp?titleid=8741

7.4 Интернет-ресурсы

1. Интернет университет информационных технологий [Электронный ресурс]. Режим доступа: http://www.intuit.ru/
2. Российиский портал открытого образования « Российский образовательный портал» [Электронный ресурс]. Режим доступа:.http://www.openet.edu.ru/
3. Естественно-научный образовательный портал [Электронный ресурс] Режим доступа: http://www.en.edu.ru/
4. Федеральный портал «Инженерное образование», журнал «Инженерное образование» [Электронный ресурс] Режим доступа: http://www.techno.edu.ru/
5. Федеральный центр информационно-образовательных ресурсов [Электронный ресурс] Режим доступа: http://fcior.edu.ru/
6. Единое окно доступа к образовательным ресурсам [Электронный ресурс]. Режим доступа: http://window.edu.ru/
7. Все для учебы [Электронный ресурс]. Режим доступа: http://www.studfiles.ru/
8. Банк рефератов [Электронный ресурс] Режим доступа: http://www.bestreferat.ru/
9. Электронная библиотечная система Znanium[Электронный ресурс] Режим доступа: http://new.www.znanium.com/
10. Электронные ресурсы Академии ИМСИТ [Электронный ресурс] – Режим доступа: http://eios.imsit.ru/
11. Электронная библиотечная система BOOK.ru [Электронный ресурс] – Режим доступа: http://www.book.ru
12. http://www.iprbookshop.ru – ЭБС «IPRbooks».
13. http://www.biblioclub.ru – университетская библиотека онлайн
14. http://www.iqlib.ru – интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия.
15. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
16. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
17. Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
18. Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
19. Справочный центр Astra Linux – Режим доступа: https://wiki.astralinux.ru/
20. База знаний Astra – Режим доступа: https://wiki.astralinux.ru/kb
21. Компания «Код Безопасности» [официальный сайт]. Режим доступа: https://www.securitycode.ru/

7.5 Программное обеспечение

Преподавание и подготовка студентов предполагает использование стандартного программного обеспечения для персонального компьютера:

1. ОС – Windows 10 Pro RUS. Подписка Microsoft Imagine Premium – Invoce № 9554097373 от 22 июля 2019г.
2. ОС – Astra Linux SE
3. Программное обеспечение по лицензии GNU GPL:
4. 7-Zip, LibreOffice, Maxima, Mozilla Firefox.
5. Microsoft Visio профессиональный 2016. Подписка Microsoft Imagine Premium – Invoce № 9554097373 от 22 июля 2019г

Таблица 7.1 – Перечень электронно-библиотечных систем

№	Наименование ресурса	Наименование документа с указанием реквизитов	Срок действия документа
1	ЭБС Znanuim	ООО «ЗНАНИУМ». Договор № 463 эбс от 16.09.2022 г Срок действия - до 27.09.2023	с 28.09.2022 г. по 27.09.2023 г.
2	Научная электронная библиотека eLibrary (ринц)	ООО «Научная электронная библиотека» (г. Москва). Лицензионное соглашение № 7241 от 24.02.12 г.	бессрочно
3	ЭБС IBooks	ООО «Айбукс». Договор № 27-01/23К от 27.01.2023 г	с 27.01.2023 по 27.01.2023 г.
4	ЭБС Book.ru	ООО «КноРус медиа». Договор №18507666 от 29 Августа 2022 г.	с 29.08.2022 г. по 09.09.2023 г.

7.6 Перечень профессиональных баз данных и информационных справочных систем:

1. Кодекс – Профессиональные справочные системы – URL: https://kodeks.ru
2. РОССТАНДАРТ Федеральное агентство по техническому регулированию и метрологии – URL: https://www.gost.ru/portal/gost/
3. ИСО Международная организация по стандартизации – URL: https://www.iso.org/ru/home.html
4. ABOUT THE UNIFIED MODELING LANGUAGE SPECIFICATION – URL: https://www.omg.org/spec/UML
5. ARIS BPM Community – URL: https://www.ariscommunity.com
6. Global CIO Официальный портал ИТ-директоров – URL: http://www.globalcio.ru

7.7 Перечень средств материально-технического обеспечения для учебной практики

Таблица 7.2 – Перечень средств материально-технического обеспечения для учебной практики

Лаборатория программно-аппаратных средств защиты информации Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение, коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН	350010, Краснодарский край, г. Краснодар, Центральный административный округ, ул. Зиповская, 5, 1 этаж, 89,2 кв.м, №88	оперативное управление	Агабекян Раиса Левоновна, Хамидов Нуради Нурадиевич, Баум Ирина Дмитриевна, Косяков Владимир Анатольевич	Выписка из Единого государственного реестра недвижимости об объекте недвижимости от 11.12.2023 г. №КУВИ-001/2023-279076982, бессрочно

40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт.,				

стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.				
Кабинет информационной безопасности. Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение	350010, Краснодарский край, г. Краснодар, Центральный административный округ, ул. Зиповская, 5, 1 этаж, 41,6 кв.м, №84	оперативное управление	Агабекян Раиса Левоновна, Хамидов Нуради Нурадиевич, Баум Ирина Дмитриевна, Косяков Владимир Анатольевич	Выписка из Единого государственного реестра недвижимости об объекте недвижимости от 11.12.2023 г. №КУВИ-001/2023-279076982, бессрочно
Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся) Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.	350010, Краснодарский край, г. Краснодар, Центральный административный округ, ул. Зиповская, 5, 1 этаж, 163 кв.м, №103	оперативное управление	Агабекян Раиса Левоновна, Хамидов Нуради Нурадиевич, Баум Ирина Дмитриевна, Косяков Владимир Анатольевич	Выписка из Единого государственного реестра недвижимости об объекте недвижимости от 11.12.2023 г. №КУВИ-001/2023-279076982, бессрочно
Серверная, кабинет отдела инженерного обеспечения и системного	350049, Краснодарский край, г.	практическая подготовка	Общество с ограниченной ответственност	Договор о практической подготовке

администрирования Стол – 1 шт., кресло офисное – 1 шт., сервер – 2 шт., сервер виртуализации HYPER-V - 1 шт., персональный компьютер с выходом в интернет – 1 шт., многофункциональное устройство– 1 шт., соответствующее программное обеспечение	Краснодар, Центральный административный округ, ул. им. Котовского, д 76/2, к.11, 30 кв.м, №22		ью «Поставщик коммерческой информации»	обучающихся от 24.05 2023 г. № 106, срок действия до 31.08.2028 г.

Приложение А
Образец титульного листа отчета по производственной практике

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

Институт информационных технологий и инноваций

Отчет по производственной (эксплуатационной) практике
в Академии маркетинга и информационных технологий (ИМСИТ) г. Краснодар

Направление 10.03.01 Информационная безопасность

Отчет выполнил
обучающийся 4 курса,
группы_____

Иванов Иван Иванович

Руководитель практики от академии
к.т.н., доцент
«___»_____20 г .

Руководитель практики от организации

Отчет защищен с оценкой_____
«_____» _____ 2023 г.

Краснодар
2023

Приложение Б

Образец задания на учебную практику

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

Институт информационных технологий и инноваций

Утверждаю
Заведующий кафедрой
_____
«____» _____20__г.

ЗАДАНИЕ
на производственную (эксплуатационную) практику

Обучающемуся 4 курса группы _____ Иванову Ивану Ивановичу

Основные вопросы, подлежащие разработке:

Срок представления отчета «_____» _____ 202 г.

Дата выдачи задания «_____» _____ 202 г.
Руководитель

Задание получил «_____» _____ 202 г.

Обучающийся / Иванов И.И. /

Приложение В
(обязательное)
Бланк направления на практику

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

Н А П Р А В Л Е Н И Е

на_____
_____
_____в 20__ / 20__ учебном году
обучающегося института информационных технологий и инноваций
_____ курса, группы _____
_____ формы обучения направления 10.03.01 Информационная безопасность (очной/заочной)

Фамилия _____
Имя _____ Отчество _____
Наименование предприятия (базы практики) _____
_____
_____

КАЛЕНДАРНЫЕ СРОКИ ПРОХОЖДЕНИЯ ПРАКТИКИ

По учебному плану: начало _____ конец _____
Дата прибытия на практику «____»_____ 20__ г.
Дата убытия с места практики «____» _____ 20__ г.

Заведующий кафедрой Исикова Наталья Павловна, к.э.н., доцент

РУКОВОДИТЕЛЬ ПРАКТИКИ ОТ АКАДЕМИИ

кафедра _____ звание _____
Фамилия _____
Имя _____ Отчество _____

ХАРАКТЕРИСТИКА РАБОТЫ ОБУЧАЮЩЕГОСЯ ПО ИТОГАМ ПРАКТИКИ

_____
_____
_____
_____
_____
Подпись руководителя от академии _____
«____»_____ 20__ г.
Оценка защиты отчета на кафедре _____

ОТЗЫВ

РУКОВОДИТЕЛЯ ПРАКТИКИ ОТ ПРЕДПРИЯТИЯ

_____
_____

КАЛЕНДАРНЫЕ СРОКИ ПРОХОЖДЕНИЯ ПРАКТИКИ

Дата прибытия на практику «____»_____ 20_ __ г.
Дата убытия с места практики «____» _____ 20_ __ г.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Должность _____
Фамилия _____
Имя _____ Отчество _____

Подпись _____
«____»_____ 20_ __ г.

м.п.

Приложение Г
Образец отзыва руководителя на производственную практику

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

Институт информационных технологий и инноваций

ОТЗЫВ РУКОВОДИТЕЛЯ НА ПРОИЗВОДСТВЕННУЮ (ЭКСПЛУАТАЦИОННУЮ) ПРАКТИКУ ОБУЧАЮЩЕГОСЯ

Направление подготовки 10.03.01 Информационная безопасность (профиль) «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Наименование предприятия (базы практики) НАН ЧОУ ВО Академия ИМСИТ
Сформированность компетенций у выпускника по итогам выполнения заданий на практику

Этапы работы (виды деятельности) при прохождении практики	Код формируемых компетенций	Уровень сформированности компетенций*
Подготовительный этап:	ОПК-1	
Содержательный этап:	ОПК-1 ОПК-5 ОПК-6 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.3	
Выполнение индивидуального задания:	ОПК-1 ОПК-5 ОПК-6 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1	

	ОПК-4.3	
Отчетный этап: Составление отчета по учебной практике Заполнение дневника практики	ОПК-1	

**Отметить «Нулевой», «Низкий», «Средний», «Высокий»*

Соответствие отчета по практике требованиям

Наименование требования	Заключение о соответствии требованиям*
1. Качество подобранного материала для проведения исследования	
1.1 Наличие источников информации в соответствии с заданием	
1.2 Наличие актуальных первичных данных, материалов	
2. Качественная оценка проведенного исследования собранных материалов	
2.1 Оценка требований к содержательной части отчета, соответствие заданию	
2.2 Оценка степени самостоятельности проведенного исследования	
2.3 Оценка качества проведенного исследования собранных материалов, данных	
3. Выполнение общих требований к проведению практики	
3.1 Выполнение требований руководителя по своевременному выполнению задания	
3.2 Выполнение требований к оформлению отчета по практике	

Достоинства содержательной части отчета по практике:

Ошибки и недостатки содержательной части отчета по практике:

_____

_____

Отчет защищен с оценкой

Зачтено с оценкой

« _____» ___ _____ 202___ г.

Руководитель практики от академии ____ _____ (.)

«__»_____202_г.

Приложение Д
Образец индивидуального задания
Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ» (г. Краснодар)

Институт информационных технологий и инноваций

Индивидуальное задание, выполняемое в период проведения учебной практики

Направление подготовки 10.03.01 Информационная безопасность направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Обучающемуся_____

Сроки прохождения практики
с «___»_____20_г. по «___»_____ 20_г.

Цель учебной практики, в соответствии с основной профессиональной образовательной программой по направлению подготовки 10.03.01 Информационная безопасность направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» – достижении обучающимися следующих результатов: закрепление, расширение и систематизация знаний, умений и навыков полученных при изучении теоретического материала; формирование у обучающихся в соответствии с объектами, областью и видами профессиональной деятельности навыков аналитической и научно-исследовательской работы в профессиональной области, регламентируемыми ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. № 1427.

Перечень вопросов (заданий, поручений) для прохождения учебной практики:

№п/п	Этапы работы (виды деятельности) при прохождении практики	Код формируемых компетенций	Сроки	Отметка руководителя от академии
1	Организация практики подготовительный этап, включающий заполнение плана прохождения практики, знакомство с	ОПК-1		

	средой разработки			
2	Содержательный этап,	ОПК-1 ОПК-5 ОПК-6 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.3		
4	Отчетный этап Составление отчета по практике	ОПК-1		

Ознакомлен _202 г.

Руководитель практики от академии .
«__»_____202 г.

Согласовано:
Руководитель практики от организации (расшифровка подписи руководителя)
«__»_____202 г. МП

Приложение Е

Образец дневника практики

ДНЕВНИК ПРОХОЖДЕНИЯ
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ЭКСПЛУАТАЦИОННАЯ)

_____

(фамилия, имя, отчество)

Обучающегося 3 курса, _____ группы

Направление подготовки 10.03.01 Информационная безопасность направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Место прохождения практики_____
Сроки практики: с ___ по ___.

_____

(должность, фамилия, инициалы)

Дата (период)	Содержание проведенной работы	Результат работы	Оценки, замечания и предложения по работе

Обучающийся _____(подпись, дата)
Руководитель практики от академии _____(подпись, дата)
Руководитель практики от организации _____(подпись, дата)

Приложение Ж
Образец календарного плана

Календарный план прохождения учебной практики

Обучающимся 4 курса _____факультета _____(ф.и.о.)

1		
2		
3		
4		
5		
6		
7		
8		

Обучающийся _____ (подпись, дата)

Руководитель практики от академии _____(подпись)
Руководитель практики от организации _____ (подпись, печать)

Приложение 3
Требования к оформлению отчета по производственной (эксплуатационной) практике

Текст отчета должен быть оформлен в соответствии с требованиями ГОСТ 7.32-2017 Отчет о научно-исследовательской работе. Структура и правила оформления и основными требованиями, предъявляемыми к оформлению отчета по практике

Отчет по практике оформляется на русском языке. В тексте категорически запрещается применять:

– обороты разговорной речи, техницизмы, профессионализмы;
– для одного и того же понятия различные научно- технические термины (синонимы), а также иностранные слова и термины при наличии равнозначных слов и терминов на русском языке;
– произвольные словообразования;
– сокращения слов, кроме установленных правилами русской орфографии, соответствующими государственными стандартами, а также перечнем принятых сокращений в данном документе (помещаемом перед содержанием пояснительной записки);
– сокращать обозначения единиц физических величин, если они употребляются без цифр, за исключением единиц физических величин в головках и боковиках таблиц и расшифровках буквенных обозначений, входящих в формулы и рисунки.

В тексте документа числовые значения величин с обозначением единиц физических величин и единиц счета следует писать цифрами, а числа без обозначения единиц физических величин и единиц счета от единицы до девяти – словами.

Согласно ГОСТу 7.32-2017 СИБИД. Отчет о научно-исследовательской работе. Структура и правила оформления; ГОСТу Р 7.0.5-2008 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления, а также требования к оформлению отчетов по практике, Академии ИМСИТ, текст печатается на одной стороне листа бумаги стандартного формата А4.

Страницы текста отчета по практике и включенные в нее иллюстрации и таблицы должны соответствовать формату А4 по ГОСТ 9327. Допускается применение формата А3 при наличии большого количества таблиц и иллюстраций данного формата.

Работа должна быть выполнена любым печатным способом на одной стороне листа белой бумаги формата А4 через полтора интервала.

Цвет шрифта должен быть черным, размер шрифта – не менее 12 пт (рекомендуется использовать 14 пт). Рекомендуемый тип шрифта для основного текста работы – Times New Roman. Полужирный шрифт применяют только для заголовков разделов и подразделов, заголовков структурных элементов. Использование курсива допускается для обозначения объектов (биология, геология, медицина, нанотехнологии, генная инженерия и др.) и написания терминов (например, in vivo, in vitro) и иных объектов и терминов на латыни.

Для акцентирования внимания может применяться выделение текста с помощью шрифта иного начертания, чем шрифт основного текста, но того же кегля и гарнитуры. Разрешается для написания определенных терминов, формул, теорем применять шрифты разной гарнитуры.

Текст работы следует печатать, соблюдая следующие размеры полей: левое – 30 мм, правое – 15 мм, верхнее и нижнее – 20 мм. Абзацный отступ должен быть одинаковым по всему тексту работы и равен 1,25 см.

Вне зависимости от способа выполнения работы качество напечатанного текста и оформления иллюстраций, таблиц, распечаток программ должно удовлетворять требованию их четкого воспроизведения.

При выполнении работы необходимо соблюдать равномерную плотность и четкость изображения по всей работе. Все линии, буквы, цифры и знаки должны иметь одинаковую контрастность по всему тексту работы.

Фамилии, наименования учреждений, организаций, фирм, наименования изделий и другие имена собственные в работе приводят на языке оригинала. Допускается транслитерировать имена собственные и приводить наименования организаций в переводе на язык работы с добавлением (при первом упоминании) оригинального названия по ГОСТ 7.79.

Сокращения слов и словосочетаний на русском, белорусском и иностранных европейских языках оформляют в соответствии с требованиями ГОСТ 7.11, ГОСТ 7.12.

Наименования структурных элементов работы: "СПИСОК ИСПОЛНИТЕЛЕЙ", "РЕФЕРАТ", "СОДЕРЖАНИЕ", "ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ", "ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ", "ВВЕДЕНИЕ", "ЗАКЛЮЧЕНИЕ", "СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ", "ПРИЛОЖЕНИЕ" служат заголовками структурных элементов работы.

Заголовки структурных элементов следует располагать в середине строки без точки в конце, прописными буквами, не подчеркивая. Каждый структурный элемент и каждый раздел основной части работы начинают с новой страницы.

Основную часть работы следует делить на разделы, подразделы и пункты. Пункты при необходимости могут делиться на подпункты. Разделы и

подразделы работы должны иметь заголовки. Пункты и подпункты могут не иметь заголовков.

Заголовки разделов и подразделов основной части работы следует начинать с абзацного отступа и размещать после порядкового номера, печатать с прописной буквы, полужирным шрифтом, не подчеркивать, без точки в конце. Пункты и подпункты могут иметь только порядковый номер без заголовка, начинающийся с абзацного отступа, а могут иметь заголовок после порядкового номера, печатать с прописной буквы, обычным шрифтом, не подчеркивать, без точки в конце.

Если заголовок включает несколько предложений, их разделяют точками. Переносы слов в заголовках не допускаются.

Страницы работы следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту работы, включая приложения. Номер страницы проставляется в центре нижней части страницы без точки. Приложения, которые приведены в работе и имеющие собственную нумерацию, допускается не перенумеровать.

Титульный лист включают в общую нумерацию страниц работы. Номер страницы на титульном листе не проставляют.

Иллюстрации и таблицы, расположенные на отдельных листах, включают в общую нумерацию страниц работы. Иллюстрации и таблицы на листе формата А3 учитывают как одну страницу.

Разделы должны иметь порядковые номера в пределах всей работы, обозначенные арабскими цифрами без точки и расположенные с абзацного отступа. Подразделы должны иметь нумерацию в пределах каждого раздела. Номер подраздела состоит из номеров раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится. Разделы, как и подразделы, могут состоять из одного или нескольких пунктов.

Если работа не имеет подразделов, то нумерация пунктов в нем должна быть в пределах каждого раздела и номер пункта должен состоять из номеров раздела и пункта, разделенных точкой. В конце номера пункта точка не ставится.

Если работа имеет подразделы, то нумерация пунктов должна быть в пределах подраздела и номер пункта должен состоять из номеров раздела, подраздела и пункта, разделенных точками.

Пример – Приведен фрагмент нумерации раздела, подраздела и пунктов работы:

3 Принципы, методы и результаты разработки и ведения классификационных систем ВИНИТИ

3.1 Рубрикатор ВИНИТИ

3.1.1 Структура и функции рубрикатора

3.1.2 Соотношение Рубрикатора ВИНИТИ и ГРНТИ

3.1.3 Место рубрикатора отрасли знания в рубрикационной системе ВИНИТИ

Если раздел или подраздел состоит из одного пункта, то пункт не нумеруется.

Если текст работы подразделяется только на пункты, они нумеруются порядковыми номерами в пределах работы.

Пункты при необходимости могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта: 4.2.1.1, 4.2.1.2, 4.2.1.3 и т.д.

Внутри пунктов или подпунктов могут быть приведены перечисления. Перед каждым элементом перечисления следует ставить тире. При необходимости ссылки в тексте работы на один из элементов перечисления вместо тире ставят строчные буквы русского алфавита со скобкой, начиная с буквы "а" (за исключением букв е, з, й, о, ч, ъ, ы, ь). Простые перечисления отделяются запятой, сложные - точкой с запятой.

При наличии конкретного числа перечислений допускается перед каждым элементом перечисления ставить арабские цифры, после которых ставится скобка.

Перечисления приводятся с абзацного отступа в столбик.

Пример 1

Информационно-сервисная служба для обслуживания удаленных пользователей включает следующие модули:

- удаленный заказ,

- виртуальная справочная служба,

- виртуальный читальный зал.

Пример 2

Работа по оцифровке включала следующие технологические этапы:

а) первичный осмотр и структурирование исходных материалов,

б) сканирование документов,

в) обработка и проверка полученных образов,

г) структурирование оцифрованного массива,

д) выходной контроль качества массивов графических образов.

Пример 3

8.2.3 Камеральные и лабораторные исследования включали разделение всего выявленного видового состава растений на четыре группы по степени использования их копытными:

1) случайный корм,

2) второстепенный корм,

3) дополнительный корм,

4) основной корм.

Пример 4

7.6.4 Разрабатываемое сверхмощное устройство можно будет применять в различных отраслях реального сектора экономики:

- в машиностроении:

1) для очистки отливок от формовочной смеси;

2) для очистки лопаток турбин авиационных двигателей;

3) для холодной штамповки из листа;

- в ремонте техники:

1) устранение наслоений на внутренних стенках труб;

2) очистка каналов и отверстий небольшого диаметра от грязи.

Заголовки должны четко и кратко отражать содержание разделов, подразделов. Если заголовок состоит из двух предложений, их разделяют точкой.

В работе рекомендуется приводить ссылки на использованные источники. При нумерации ссылок на документы, использованные при составлении работы, приводится сплошная нумерация для всего текста работы в целом или для отдельных разделов. Порядковый номер ссылки (отсылки) приводят арабскими цифрами в квадратных скобках в конце текста ссылки. Порядковый номер библиографического описания источника в списке использованных источников соответствует номеру ссылки.

Ссылаться следует на документ в целом или на его разделы и приложения.

При ссылках на стандарты и технические условия указывают их обозначение, при этом допускается не указывать год их утверждения при условии полного описания стандарта и технических условий в списке использованных источников в соответствии с ГОСТ 7.1.

Примеры

1 ..... приведено в работах [1] - [4].

2 ..... по ГОСТ 29029.

3 ..... в работе [9], раздел 5.

Иллюстрации (чертежи, графики, схемы, компьютерные распечатки, диаграммы, фотоснимки) следует располагать в работе непосредственно после текста, где они упоминаются впервые, или на следующей странице (по

возможности ближе к соответствующим частям текста работы). На все иллюстрации в работе должны быть даны ссылки. При ссылке необходимо писать слово "рисунок" и его номер, например: "в соответствии с рисунком 2" и т.д.

Чертежи, графики, диаграммы, схемы, помещаемые в работе, должны соответствовать требованиям стандартов Единой системы конструкторской документации (ЕСКД).

Количество иллюстраций должно быть достаточным для пояснения излагаемого текста работы. Не рекомендуется в отчете по практике приводить объемные рисунки.

Иллюстрации, за исключением иллюстраций, приведенных в приложениях, следует нумеровать арабскими цифрами сквозной нумерацией. Если рисунок один, то он обозначается: Рисунок 1.

Пример – Рисунок 1 – Схема прибора

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения: Рисунок А.3.

Допускается нумеровать иллюстрации в пределах раздела работы. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой: Рисунок 2.1.

Иллюстрации при необходимости могут иметь наименование и пояснительные данные (подрисуночный текст). Слово "Рисунок", его номер и через тире наименование помещают после пояснительных данных и располагают в центре под рисунком без точки в конце.

Пример – Рисунок 2 – Оформление таблицы

Если наименование рисунка состоит из нескольких строк, то его следует записывать через один межстрочный интервал. Наименование рисунка приводят с прописной буквы без точки в конце. Перенос слов в наименовании графического материала не допускается.

Цифровой материал должен оформляться в виде таблиц. Таблицы применяют для наглядности и удобства сравнения показателей. Таблицу следует располагать непосредственно после текста, в котором она упоминается впервые, или на следующей странице. все таблицы в работе должны быть ссылки. При ссылке следует печатать слово "таблица" с указанием ее номера.

Наименование таблицы, при ее наличии, должно отражать ее содержание, быть точным, кратким. Наименование следует помещать над таблицей слева, без абзацного отступа в следующем формате: Таблица Номер таблицы – Наименование таблицы. Наименование таблицы приводят с прописной буквы без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через один межстрочный интервал.

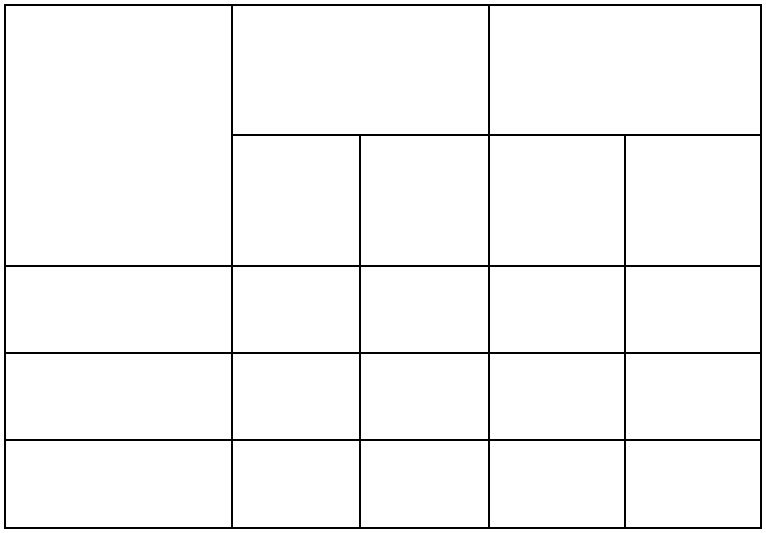
Таблицу с большим количеством строк допускается переносить на другую страницу. При переносе части таблицы на другую страницу слово "Таблица", ее номер и наименование указывают один раз слева над первой частью таблицы, а над другими частями также слева пишут слова "Продолжение таблицы" и указывают номер таблицы.

При делении таблицы на части допускается ее головку или боковик заменять соответственно номерами граф и строк. При этом нумеруют арабскими цифрами графы и (или) строки первой части таблицы. Таблица оформляется в соответствии с таблицей 1.

Таблица 1 – Заголовок таблицы

Таблица _____ - _____

номер наименование таблицы



Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Таблицы каждого приложения обозначаются отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Если в работе одна таблица, она должна быть обозначена "Таблица 1" или "Таблица А.1" (если она приведена в приложении А).

Допускается нумеровать таблицы в пределах раздела при большом объеме работы. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой: Таблица 2.3.

Заголовки граф и строк таблицы следует печатать с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков таблиц точки не ставятся. Названия заголовков и подзаголовков таблиц указывают в единственном числе.

Таблицы слева, справа, сверху и снизу ограничивают линиями. Разделять заголовки и подзаголовки боковика и граф диагональными линиями не допускается. Заголовки граф выравнивают по центру, а заголовки строк – по левому краю.

Горизонтальные и вертикальные линии, разграничивающие строки таблицы, допускается не проводить, если их отсутствие не затрудняет пользование таблицей.

Текст, повторяющийся в строках одной и той же графы и состоящий из одиночных слов, заменяют кавычками. Ставить кавычки вместо повторяющихся цифр, буквенно-цифровых обозначений, знаков и символов не допускается.

Если текст повторяется, то при первом повторении его заменяют словами "то же", а далее кавычками. В таблице допускается применять размер шрифта меньше, чем в тексте работы.

Титульный лист является первой страницей отчет по практике, предшествующей основному тексту. Размеры полей титульного листа те же, что и для текста работы (приложение Б).

Каждую запись содержания оформляют как отдельный абзац, выровненный по ширине.

Номера страниц указывают выровненными по правому краю поля.

Слово «СОДЕРЖАНИЕ» записывают прописными буквами в виде заголовка и располагают симметрично тексту (приложение Г).

Наименования, включенные в содержание, записывают с абзаца.

Наименования разделов записываются прописными буквами, подразделов и пунктов основной части отчет по практике – с прописной буквы с указанием номеров разделов и подразделов.

Цифры, обозначающие номера страниц (листов), с которых начинается раздел отчет по практике, следует располагать на расстоянии 15 мм от края листа, соблюдая разрядность цифр. Слово «стр.» не пишется.

Для удобства редактирования текста, рекомендуется выполнять содержание в невидимой таблице, так как тестовую часть содержания выравнивают по ширине, а страницы по правому нижнему краю.

Список использованных источников представляет собой библиографическое описание использованных источников, который должен включать не менее 25 источников, расположенных в алфавитном порядке.

Отчет по практике обязательно может содержать приложения, которые выделяются как структурная единица документа словом ПРИЛОЖЕНИЕ, расположенным по центру отдельного листа.

В приложения выносятся формы отчетности по исследуемому вопросу, на основании которых выполнялись расчеты, а также другой объемный аналитический материал (графики, таблицы, рисунки, копии подлинных документов и т.п.).

Каждое приложение начинается с новой страницы с указанием наверху по справа страницы «Приложение», которое должно иметь обозначение (заглавными буквами русского алфавита, начиная с А, кроме Ё, З, Й, О, Ч, Ь, Ы, Ъ) и заголовок.

Заголовок приложения записывают отдельной строкой по центру симметрично относительно текста с прописной буквы, без точки в конце.

При вынесении материала в приложение следует группировать связанные по смыслу таблицы и рисунки в одно приложение.