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
Н.П. Исикова

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

Б2.О.05(П)

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ:

ПРЕДДИПЛОМНОЙ 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: Преддипломной практики 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 (преддипломная) 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 (преддипломной) 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
– Б1.В.07	– Порядок проведения аттестации объектов информатизации
– Б1.В.08	– Комплексная защита объектов

	информатизации
– Б2.О.04(П)	– Производственная практика: Эксплуатационная практика

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 (преддипломной) 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 (преддипломной) 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 (преддипдомной) 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 – преддипломная.

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)		0,5		0,5
Иные виды работы во время практики, включая самостоятельную работу (СР), всего:		35,5		35,5
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
– Б1.В.07	– Порядок проведения аттестации объектов информатизации
– Б1.В.08	– Комплексная защита объектов информатизации
– Б2.О.04(П)	– Производственная практика: Эксплуатационная практика

Прохождение практики необходимо как предшествующее для следующих дисциплин образовательной программы:

– Б3.01(Д)	Выполнение и защита выпускной квалификационной работы

В результате прохождения практики студент бакалавриата должен приобрести следующие компетенции:

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-3: Способен использовать необходимые математические методы для решения задач профессиональной деятельности;

ОПК-4: Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;

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-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

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-4.2: Способен администрировать операционные системы, системы управления базами данных, вычислительные сети;

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;

ОПК-4.4: Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем;

ПК-1: Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем;

ПК-2: Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности;

ПК-3: Способен обеспечивать безопасную обработку данных в автоматизированных системах;

ПК-4: Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении;

ПК-5: Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла;

ПК-6: Способен документально оформлять работы по обеспечению информационной безопасности;

ПК-7: Способен определять уровень защищённости автоматизированных систем;

ПК-8: Способен выполнять задачи по выявлению уязвимых узлов автоматизированной системы;

ПК-9: Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах;

ПК-10: Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности.

2 ОРГАНИЗАЦИЯ ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНАЯ)

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 (преддипломной)

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 (преддипломная)

	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	УК-1 ОПК-2
	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-2 ОПК-5
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 проведения мониторинга безопасности ТКС. Создание плана работы коллектива	30	Мониторинг результатов практических работ	УК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-8 ОПК-9

	из 3 – 4 человек, реализующего политику безопасности в ТКС. Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. Мониторинг состояния информационной безопасности. Самостоятельное проведение анализа результатов проведенного мониторинга информационной безопасности. Представление результатов руководителю практики от организации.			ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-4.4 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10
4	Организация работы 2-3 человек и руководство их работой в процессе работ по обеспечению информационной безопасности. 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 повышению уровня информационной безопасности предприятия. Самостоятельное составление краткосрочного плана работ по обеспечению безопасности организации, эксплуатирующей ТКС. Организация работы 2-3 человек и руководство их работой в процессе составления краткосрочного и долгосрочного прогнозов. Представление своего прогноза с обоснованием руководителю практики от организации. Представление результатов руководителю практики от организации.	30	Мониторинг результатов практических работ	УК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-8 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-4.4 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10
Отчетный этап				

	Подготовка и оформление отчета по практике.	12	Защита отчета по практике	УК-1 ОПК-2

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 (преддипломной) практики у обучающихся должны быть сформированы компетенции, таблица 4.1.

Таблица 4.1 – Планируемые результаты обучения

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
УК-1.1: Анализирует задачу, выделяя ее базовые составляющие	**Знать:** - основные этапы развития технологии программирования; - принципы построения программных систем.	**Уметь:** - пользоваться понятийным аппаратом методов разработки программных систем; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы функционирования программных систем; - выполнять операции импорта/экспорта данных при работе с программными средами.	**Владеть:** - базовыми элементами технологии разработки; - программными приемами декларативного описания предметной области; - навыками структуризации знаний и его программирования.
УК-1.2: Определяет и ранжирует информацию, требуемую для решения поставленной задачи	**Знать:** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения.	**Уметь:** - разрабатывать техническое задание на проектирование программного обеспечения; - принимать обоснованные решения по выбору архитектуры программного	**Владеть:** - правилами ранжирования информации; - процедурами упорядочения элементов.

		обеспечения, среды программирования, стандартов разработки.	
УК-1.3: Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	**Знать:** - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности.	**Уметь:** - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы.	**Владеть:** - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур.
ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-2.1: Ищет информацию в глобальной информационной сети Интернет	**Знать:** - существующие системы глобального поиска - варианты использования поисковых систем внутри профессионального сервиса - правила формирования запросов на основе ключевых словосочетаний на русском и английском языке - основы использования расширенных параметров поиска.	**Уметь:** - производить поиск в различных поисковых системах - уточнять поисковый запрос с учетом предварительной выдачи данных - анализировать источники данных и производить расширенный поиск в том числе на англоязычных ресурсах.	**Владеть:** - технологией формирования поискового запроса на основе ключевых слов - навыками анализа результатов работы поисковых систем (топ выдачи) - навыками поиска и сопоставления результатов на русском и английском языке, в том числе с разнородным контентом.

ОПК-2.2: Подготавливает документы в среде типовых офисных пакетов	**Знать:** - основы работы и разновидности офисных пакетов - основы подготовки документов и отчетных форм на основе текста - основы подготовки документов на основе электронных таблиц - основы подготовки презентаций.	**Уметь:** - создавать и дорабатывать документы на основе текста - производить вычисления, строить графики и визуализировать данные на базе электронных таблиц - разрабатывать презентации для повышения наглядности при демонстрации ключевых показателей деятельности.	**Владеть** - навыками работы с текстом с расширенным форматированием - навыками составления электронных таблиц с организацией вычислений - навыками создания презентаций для демонстрации результатов работы и повышения их наглядности.
ОПК-2.3: Определяет состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств	**Знать:** - основы аппаратного обеспечения вычислительной техники - разновидности типов оперативной и постоянной памяти, центрального процессора, материнской платы и видеокарты - способы диагностики и получения данных о составе и параметрах оборудования.	**Уметь:** - проводить получение данных об аппаратном обеспечении персонального компьютера - оценивать быстродействие с учетом имеющегося оборудования - определять совместимость периферийного оборудования с основной вычислительной платформой.	**Владеть:** - навыками получения данных в режиме программного опроса оборудования - навыками определения состава вычислительной системы на основе интегрированного и периферийного оборудования на уровне визуального анализа - навыками оценки номинального быстродействия ПК.
ОПК-2.4: Применяет технические и программные средств тестирования с целью определения исправности компьютера и оценки его производительности	**Знать:** - основные разновидности и средства программной диагностики работы компьютера - основы оценки производительности ПК на базе прикладных решений - типовые нештатные ситуации, предполагающие	**Уметь:** - оценивать текущую производительность ПК, сопоставлять ее с номинальной - выявлять нештатные ситуации программных или аппаратных элементов вычислительной системы - использовать	**Владеть:** - навыками оценки производительности компьютеры - навыками локализации неисправностей на различных уровнях - навыками применения актуальных технических и программных средств

	локализацию неисправности в работе программных или аппаратных элементов вычислительной системы.	прикладные средства для контроля состояния системы.	тестирования с целью локализации исправности системы.
ОПК-3: Способен использовать необходимые математические методы для решения задач профессиональной деятельности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-3.1: Использует методы аналитической геометрии и векторной алгебры при решении прикладных задач	**Знать:** -основные приемы решения математических задач; - утверждения для обоснования выбираемых методов математического анализа и их следствия.	**Уметь:** - применять инструментарий математического анализа при решении задач; -анализировать способы решения поставленных задач.	**Владеть:** - навыками решения основных математических задач; - инструментами сбора и обработки необходимых данных для математической постановки и решения задач; - навыками анализа и интерпретации результатов решения задач.
ОПК-3.2: Использует типовые модели и методы математического анализа при решении стандартных прикладных задач	**Знать:** - основные понятия о погрешности вычислений; - основные требования, предъявляемые к вычислительным схемам (корректность, устойчивость, сходимость).	**Уметь:** - пользоваться учебной и научной литературой; - обоснованно выбрать численный метод; - разработать алгоритм решения поставленной задачи.	**Владеть** - методами применения стандартных методов; - навыками применения моделей вычислительной математики для решения прикладных задач.
ОПК-3.3: Выполняет типовые расчеты с использованием основных формул дифференциального и интегрального исчисления	**Знать:** - основные методы и алгоритмы численного интегрирования и дифференцирования; - методы и алгоритмы теории обработки результатов эксперимента.	**Уметь:** - применять полученные знания к численному решению задач практики; - оценивать адекватность полученного численного решения, его сходимость и необходимый ресурс	**Владеть:** - основными методами численного решения задач оптимизации; - методами оценки адекватности полученного численного решения, его сходимости и необходимого ресурса времени.

		времени.	
ОПК-3.4: Использует расчетные формулы и таблицы при решении стандартных вероятностно-статистических задач	**Знать:** - содержание основных понятий дискретной математики; - основные приемы работы с комбинаторными объектами, булевыми функциями, графами; - возможности использования дискретной математики в будущей профессиональной деятельности.	**Уметь:** - использовать дискретную математику при проектировании сетей, разработке программного обеспечения; - решать стандартные задачи по дискретной математике; - использовать знания по дискретной математике в решении стандартных задач профессиональной деятельности.	**Владеть:** - навыками и приемами исследования и моделирования прикладных задач методами дискретной математики; - навыками работы с математическими методами и моделями компьютерной математики в рамках своей профессиональной деятельности.
ОПК-3.5: Решает задачи профессиональной области с применением дискретных моделей	**Знать:** - виды ресурсов и ограничений для решения профессиональных задач; - основные методы оценки разных способов решения задач, действующее законодательство и правовые нормы, регулирующие профессиональную деятельность.	**Уметь:** - проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; - анализировать альтернативные варианты для достижения намеченных результатов; - использовать нормативно-правовую документацию в сфере профессиональной деятельности.	**Владеть:** - методиками разработки цели и задач проекта, - методами оценки потребности в ресурсах, продолжительности и стоимости проекта; - навыками работы с нормативно-правовой документацией.
ОПК-4: Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-4.1: Решает базовые прикладные физические задачи	**Знать:** - базовые физические законы; - модели для решения задач профессиональной деятельности.	**Уметь:** - самостоятельно проводить анализ поставленной задачи; - формулировать задачу с использованием	**Владеть:** - навыками решения базовых прикладных задач.

		соответствующих физических законов; - осуществлять поиск возможных методов ее решения, выбирать и обосновывать наиболее рациональный метод.	
ОПК-4.2: Анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях	**Знать:** - принципы действия основных электрических устройств и электронных приборов, их эквивалентные схемы; - характеристики и параметры; - методы измерения параметров и расчета цепей.	**Уметь:** - выбирать и рассчитывать режимы работы элементов электронных устройств в схемах; - рассчитывать электрическую схему.	**Владеть:** - методами экспериментального исследования параметров и характеристик электронных приборов; - методами расчета электрических цепей.
ОПК-4.3: Анализирует процессы, протекающие в линейных и нелинейных электрических цепях	**Знать:** - современные средства автоматизированного проектирования ЭС; - интерфейс, библиотеки, функциональные возможности современных САПР; - методы моделирования электронных средств в САПР.	**Уметь:** - применять современные средства автоматизированного проектирования ЭС; - строить и анализировать временные диаграммы, передаточные и частотные характеристики в САПР; - использовать функциональные возможности САПР при исследовании и анализе параметров и характеристик ЭС.	**Владеть:** - методами моделирования электронных средств в САПР; - средствами САПР для моделирования и построения передаточных характеристик и временных диаграмм электронных устройств, расчета электрических цепей.
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,	**Знать:** - правовые основы организации защиты конфиденциальной	**Уметь:** - применять действующую законодательную	**Владеть:** - навыками работы с нормативными правовыми актами;

инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	информации; - задачи органов защиты информации.	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.	- 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 требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	**Знать:** - 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.	**Уметь:** - 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.	**Владеть:** - 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.

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 требованиям безопасности информации.	**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.
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 доступа в организации	**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.
ОПК-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-8.1: Составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов	**Знать:** - основы составления рефератов по результатам поиска на основе научно-технической документации - нормативную и методическую базу	**Уметь:** - работать с научно-технической литературой - находить нормативные и методические документы, регламентирующие порядок действий;	**Владеть:** - технологией работы с актуальной нормативно-правовой базой - навыками реферирования научно- технической литературы.

	профессиональной области.	- составлять рефераты по результатам обзора.	
ОПК-8.2: Систематизирует научную информацию в области информационной безопасности	**Знать:** - основы систематизации данных в профессиональной предметной области; - актуальные источники, регламентирующие порядок обеспечения информационной безопасности.	**Уметь:** - систематизировать данные в профессиональной предметной области; - выделять актуальные источники, регламентирующие порядок обеспечения информационной безопасности.	**Владеть:** - навыками систематизации данных в профессиональной предметной области; - навыками ранжирования научных данных с учетом современных требований нормативно-правовой базы.
ОПК-8.3: Использует информационно-справочные системы при поиске информации в области профессиональной деятельности	**Знать:** - основные информационно-справочные системы, содержащие документы профессиональной области; - правила выделения необходимой информации с учетом параметрических поисковых запросов.	**Уметь:** - работать с информационно-справочными системами, содержащими документы профессиональной области; - составлять параметрические поисковые запросы при поиске информации в справочной системе.	**Владеть:** - навыками работы с основными информационно-справочными системами, содержащими документы профессиональной области; - навыками выделения необходимой информации с учетом параметрических поисковых запросов.
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	**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.

	алгоритмов; - основы шифрования перспективными методами; - основы программной реализации криптографических преобразований.		
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 криптографических хеш-функций и протоколов.	**Владеть**: - навыками определения метода шифрования; -навыками автоматизации этапов криптографического преобразования.
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	**Знать**: - угрозы информационной безопасности	**Уметь**: - оценивать угрозы информационной безопасности объекта	**Владеть**: - способами предотвращения угрозам

объекта информатизации	объекта информатизации.	информатизации.	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 нарушения безопасности телекоммуникационн ых систем.	**Владеть**: - навыками использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - методами проведения анализа угроз информационной безопасности.
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	**Знать**: - основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы	**Уметь**: - конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками	**Владеть**: - навыками установки и настройки программно-аппаратных средств защиты информации в соответствии с

политиками безопасности	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 основных типов вредоносных программ, способы их выявления и нейтрализации.	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-аппаратных средств защиты информации в компьютерных сетях; - оценивать оптимальность выбора программно-аппаратных средств.	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 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,	**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	**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

	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 информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях.	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.	компьютерных сетей, использующих криптографическую защиту информации; - навыками установки и настройки 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	**Знать**: - показатели качества и критерии оценки систем и	**Уметь**: - анализировать показатели качества и критерии оценки	**Владеть**: - навыками оценки систем и отдельных методов и средств

систем и отдельных методов и средств защиты информации	отдельных методов и средств защиты информации.	систем и отдельных методов и средств защиты информации.	защиты информации.
ОПК-12.3: Оценивает информационные риски в автоматизированных 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 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	**Уметь**: - проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня 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.	**Владеть**: - навыками управления информационной безопасности; - навыками подготовки исходных данных для проектирования подсистем; - навыками оценки эффективности проектных решений; - навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений.

	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 автоматизированной системе	**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-4.1.3: 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-4.2: Способен администрировать операционные системы, системы управления базами данных, вычислительные сети			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			

ОПК-4.2.1: Настраивает операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации	**Знать:** - разновидности и принципы построения современных операционных систем - основы использования систем управления базами данных - основы построения и настройки вычислительных сетей.	**Уметь:** - устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности.	**Владеть:** - навыками оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности.
ОПК-4.2.2: Применяет программные средства обеспечения безопасности данных	**Знать:** - основные типы неисправностей в автоматизированных системах, методы и способы их устранения.	**Уметь:** - документировать действия в журналах безопасности автоматизированных систем; - вести журналы технического обслуживания автоматизированных систем.	**Владеть:** - навыками анализа документации, журналов аудита и безопасности автоматизированных систем локальных и распределенных; - навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания.
ОПК-4.2.3: Управляет полномочиями пользователей автоматизированной системы	**Знать:** - классификацию инцидентов информационной безопасности - критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах.	**Уметь:** - вести журнал регистрации инцидентов информационной безопасности в автоматизированных системах с указанием степени важности инцидента.	**Владеть:** - навыками анализа событий, связанных с защитой информации в автоматизированных системах - навыками составления отчетов по журналам регистрации инцидентов информационной безопасности.
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 безопасности при эксплуатации технических и программных средств; - порядок администрирования технических и программных средств системы защиты информации автоматизированной системы.	**Уметь**: - устанавливать программные и технические средства в соответствии с технической документацией; -производить настройку параметров работы технических и программных средств; - осуществлять автономную наладку технических и программных средств системы защиты информации автоматизированной системы.	**Владеть**: - навыками установки антивирусной защиты; - навыками настройки встроенных средств защиты информации программного обеспечения; - навыками проверки работоспособности отдельных программных, программно-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	**Уметь**: - применять программные средства обеспечения безопасности данных; - применять типовые программные средства резервирования и восстановления информации в автоматизированных системах; - настраивать систему резервного копирования; - проверять корректность	**Владеть**: - навыками применения программных средства обеспечения безопасности данных; - навыками фильтрации информации, подлежащей резервному копированию; - навыками применения методик резервного копирования и восстановления.

	автоматизированных системах.	резервной копии.	
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.
ОПК-4.4: Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ОПК-4.4.1: Применяет инструментальные средства контроля защищенности информации в автоматизированных системах	**Знать:** - состав, назначение и основные характеристики современных инструментальных средств контроля защищенности информации в автоматизированных системах.	**Уметь:** - применять инструментальные средства контроля защищенности информации в автоматизированных системах.	**Владеть:** - навыками использования инструментальных средств контроля защищенности информации в автоматизированных системах.
ОПК-4.4.2: Документирует действия по устранению неисправностей в работе системы защиты информации автоматизированной системы	**Знать**: - основные типы неисправностей в автоматизированных системах, методы и способы их устранения.	**Уметь**: - документировать действия в журналах безопасности автоматизированных систем, вести журналы технического обслуживания автоматизированных систем.	**Владеть**: - навыками анализа документации, журналов аудита и безопасности автоматизированных систем локальных и распределенных; навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания.
ОПК-4.4.3: Регистрирует события, связанные с защитой информации в автоматизированных системах	**Знать**: - классификацию инцидентов информационной безопасности, критерии отнесения событий к инцидентам информационной	**Уметь**: - вести журнал регистрации инцидентов информационной безопасности в автоматизированных системах с указанием степени	**Владеть**: - навыками анализа событий, связанных с защитой информации в автоматизированных системах, составлять отчеты по журналам регистрации

	безопасности в автоматизированных системах.	важности инцидента.	инцидентов информационной безопасности.
ПК-1: Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-1.1: Производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности	**Знать**: - классификацию угроз информационной безопасности (ИБ) в автоматизированных системах (АС); - причины, виды и каналы утечки информации в АС; - способы защиты операционных систем, классификацию систем защиты программного обеспечения (ПО); - методы идентификации и установления подлинности пользователей и объектов, типы аутентификации и межсетевых экранов, способы их реализации; - классификацию компьютерных вирусов, виды антивирусных программ; - средства анализа защищённости АС; - перечень мероприятий по защите информации от вирусов; - этапы внедрения и отладки программно-аппаратных средств защиты информации в АС.	**Уметь**: - реализовывать контроль доступа средствами АС и аудит потоков данных; - использовать средства аутентификации АС; применять одноразовые пароли, шифрование паролей и данных, определять уязвимые места в прикладном ПО, устанавливать программы защиты приложений, контролировать ресурсы оборудования АС; - использовать антивирусное ПО, специальные средства контроля и фильтрации доступа (сетевые экраны); - использовать средства анализа защищённости АС (сканеры безопасности); -системы обнаружения сетевых атак; - применять средства защиты информации в АС, проводить анализ информационных рисков.	**Владеть**: - навыками внедрения и отладки программных средств защиты АС; - установки и эксплуатации средств анализа защищённости АС (сканеров безопасности), систем обнаружения сетевых атак; - реализации контроля доступа и аудита, использования антивирусного ПО, настройки специальных средств контроля и фильтрации доступа (сетевых экранов); - определения уязвимых мест в прикладном ПО, контроля ресурсов оборудования АС.
ПК-1.2: Соотносит	**Знать**:	**Уметь**:	**Владеть**:

функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности	- технические характеристики и особенности функционирования программно-аппаратных средств ЗИ в АС; - перечень и объём мероприятий по обеспечению безопасности и защищённости АС, виды угроз АС, типы, виды, назначение средств защиты информации в АС; - состав, характеристики, назначение, функции оборудования АС; - классификацию антивирусного ПО, способы настройки сетевых экранов.	- проводить анализ угроз, рисков АС, осуществлять выбор оборудования и средств защиты АС в соответствии с решаемыми АС задачами, классифицировать средства защиты исходя из функционала АС, определять состав средств защиты для обеспечения выполнения задач АС; - применять программные средства защиты сетевого оборудования, антивирусные программные комплексы, настраивать режимы работы межсетевых экранов.	- навыками анализа функциональных возможностей оборудования и средств защиты АС, технических характеристик сетевого оборудования и программно-аппаратных средств ЗИ в АС; - выбора и эксплуатации средств ЗИ в АС в соответствии с функциональными задачами АС, настройки сетевых экранов, установки ПО, разработки защищённых сайтов.
ПК-1.3: Выполняет регламентные работы по эксплуатации средств защиты информации	**Знать**: - типы регламентных работ, классификацию программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; - технические характеристики и правила эксплуатации средств защиты информации (СЗИ); - эксплуатационную документацию, возможные угрозы и методики определения рисков, порядок настройки сетевого и	**Уметь**: - проводить анализ защищенности АС; - использовать программные и аппаратные средств анализа защищённости АС, системы обнаружения сетевых атак, антивирусное ПО, настраивать межсетевое оборудование.	**Владеть**: - навыками эксплуатации программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; - программных средств анализа и управления рисками, навыками настройки сетевых экранов, разработки защищенных сайтов.

	программного оборудования и режимы функционирования.		
ПК-1.4: Устраняет неисправности при эксплуатации средств защиты информации	**Знать**: - назначение и классификацию программно-аппаратных средств АС; - особенности функционирования ПО АС; классификацию программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; - технические характеристики и правила эксплуатации средств защиты информации (СЗИ); - эксплуатационную документацию.	**Уметь**: - проводить мониторинг безопасности АС; - обнаруживать уязвимые места в функционировании ПО и аппаратного оборудования АС; - провести настройку ПО и оборудования АС.	**Владеть**: - навыками настройки программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; - программных средств анализа и управления рисками, навыками разработки защищенных сайтов.
ПК-2: Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-2.1: Формулирует критерии безопасности обработки информации в автоматизированных системах	**Знать**: - требования действующих стандартов и рекомендаций, определяющих критерии оценки безопасности АС и этапы анализа рисков и угроз безопасности и уязвимости АС; - классификацию общих критериев, пути организации общих критериев; - требования к разработке должностных	**Уметь**: - применять требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в АС; - разрабатывать служебную и техническую документацию; - применять средства защиты информации в соответствии с заданными требованиями к АС;	**Владеть**: - навыками применения требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в АС; - разработки служебной и технической документации; программных средств защиты информации, разработки

	инструкций; - порядок эксплуатации программно-аппаратных средств защиты АС; - основные принципы построения политики безопасности; - методы и способы защиты информации в АС, методы анализа угроз и оценки рисков информационной безопасности АС.	- проводить анализ информационных рисков.	архитектуры сетевой защиты.
ПК-2.2: Выполняет мероприятия для реализации политики информационной безопасности	**Знать**: - виды угроз и каналы утечки информации, состав, структуру, требования и принципы построения политики безопасности; - модели и типы политик безопасности; - состав, технические характеристики и правила эксплуатации программно-аппаратных средств АС; - основные элементы политики безопасности, методы управления доступом, средства идентификация и аутентификация, анализа регистрационной информации;	**Уметь**: - проводить анализ угроз, рисков; - разрабатывать документацию пользователя, администратора сети, применять тестовые программы; - разрабатывать архитектуры АС, разрабатывать политики безопасности; применять средства защиты информации в АС, проводить анализ защищенности АС, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов.	**Владеть**: - навыками разработки документации пользователя, администратора сети, разработки и применения тестовых программ, описания архитектуры, описания политики безопасности; - навыками защиты информации в компьютерных системах, навыками анализа защищенности АС, применения антивирусных программных комплексов, настройки режимов работы межсетевых экранов.
ПК-2.3: Определяет состав средств, необходимый для	**Знать**: - требования руководящих	**Уметь**: - проводить анализ защищенности	**Владеть**: - навыками определения задач

управления автоматизированными системами и средствами их защиты от НСД	документов по защите АС от НСД; - классификацию средств и АС по уровню защищённости от НСД; - требования к защищённости АС; - показатели и классы защищённости межсетевых экранов от НСД к информации; - классификацию ПО СЗИ, требования руководящих документов к составу и содержанию документаций и испытаний ПО СЗИ; - механизмы управления ключами, шифрованием, администрирования управления доступом, аутентификацией, маршрутизацией; - задачи и методы управления системой защиты АС; - типы, состав, назначение, способы применения современных систем управления защитой АС; - показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем.	локальной вычислительной сети, определять текущее состояние оборудования АС; - применять программно-аппаратные средства ЗИ в АС; - классифицировать программные продукты управления в соответствии с задачами АС, подбирать конфигурацию системы управления безопасности АС; - проводить анализ информационных рисков.	АС, классификации оборудования АС (серверов, АРМ, рабочих станций, сетевое оборудование); - навыками установки ПО серверной и клиентской части, настройки систем управления доступом, эксплуатации программных средств мониторинга и управления средствами безопасности АС; - навыками определения уязвимых мест АС и выбора средств защиты от НСД.

ПК-2.4: Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД	**Знать**: - причины, виды и каналы утечки информации в АС; - типы технических средств.	**Уметь**: - настраивать программы защиты приложений, антивирусное ПО, специальные средства контроля и фильтрации доступа (сетевые экраны); - средства анализа защищённости АС (сканеры безопасности); - системы обнаружения сетевых атак; применять средства защиты информации в АС.	**Владеть**: - навыками настройки средств защиты АС; - установки и эксплуатации средств анализа защищённости АС (сканеров безопасности); - систем обнаружения сетевых атак; - реализации контроля доступа и аудита, установки антивирусного ПО, настройки специальных средств контроля и фильтрации доступа (сетевых экранов), контроля ресурсов оборудования АС.
ПК-2.5: Устанавливает программное обеспечение в соответствии с требованиями по защите информации	**Знать**: - причины, виды и каналы утечки информации в АС; - способы защиты операционных систем, классификацию систем защиты программного обеспечения (ПО); - типы аутентификации и межсетевых экранов, способы их реализации; -виды антивирусных программ; - средства анализа защищённости АС; - алгоритм установки и отладки ПО защиты информации в АС.	**Уметь**: - устанавливать программы защиты приложений, антивирусное ПО, специальные средства контроля и фильтрации доступа (сетевые экраны); - средства анализа защищённости АС (сканеры безопасности); - системы обнаружения сетевых атак; применять средства защиты информации в АС.	**Владеть**: - навыками внедрения и отладки программных средств защиты АС; - установки и эксплуатации средств анализа защищённости АС (сканеров безопасности); - систем обнаружения сетевых атак; - реализации контроля доступа и аудита, установки антивирусного ПО, настройки специальных средств контроля и фильтрации доступа (сетевых экранов), контроля ресурсов оборудования АС.
ПК-3: Способен обеспечивать безопасную обработку данных в автоматизированных системах			
Планируемые результаты обучения, соответствующие индикаторам достижения			

компетенции			
ПК-3.1: Фиксирует возникновение инцидентов информационной безопасности	**Знать:** - понятие инцидент; - классификация и параметры инцидентов информационной безопасности; - регламенты, определяющие порядок управления инцидентами информационной безопасности; - принципы управления инцидентами.	**Уметь:** - определить тип инцидента; - зарегистрировать инцидент информационной безопасности.	**Владеть:** - навыками определения типа инцидента; - навыками управления инцидентами информационной безопасности.
ПК-3.2: Использует методы и средства резервного копирования информации	**Знать:** - методы резервного копирования информации; - типы и характеристики носителей хранения данных; - типы и характеристики используемых платформ; - схемы копирования; - базовые функции резервного копирования информации.	**Уметь:** - определить необходимый тип носителя хранения данных; - использовать оптимальную схему копирования; - применить оптимальный тип резервного копирования.	**Владеть:** - навыками выбора необходимой для копирования информации; - навыками организации процесса резервного копирования.
ПК-3.3: Устраняет уязвимости в автоматизированной системе	**Знать:** - понятие уязвимости, классификация уязвимостей в автоматизированной системе; - поисковые признаки; - методы оценки опасности угроз; - методы устранения угроз.	**Уметь:** - анализировать уязвимости в автоматизированной системе; - выбрать средства для поиска уязвимостей; - устранять уязвимости в автоматизированной системе.	**Владеть:** - навыками анализа уязвимости в автоматизированной системе; - навыками поиска уязвимости; - навыками устранения уязвимости в автоматизированной системе.
ПК-3.4: Соотносит изменения в конфигурации автоматизированной	**Знать:** - основные методы управления защитой информации;	**Уметь:** - анализировать воздействия изменений	**Владеть:** - навыками анализа, оценки информационных

системы с её защищенностью	- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - методы защиты информации от утечки по техническим каналам; - нормативные правовые акты в области защиты информации.	конфигурации автоматизированной системы на ее защищенность; - оценивать информационные риски в автоматизированных системах - классифицировать и оценивать угрозы безопасности информации; - конфигурировать параметры системы защиты информации автоматизированных систем; - применять технические средства контроля эффективности мер защиты информации.	рисков в автоматизированных системах; - навыками настройки системы защиты информации.
ПК-4: Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-4.1: Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем	**Знать:** - методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности; - основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных	**Уметь:** - уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; - уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности; - разрабатывать проекты нормативных	**Владеть:** - навыками разработки политик безопасности различных уровней; - правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации; - навыками работы с нормативными правовыми актами в области информационной безопасности.

	документов; - основные нормативные правовые акты в области обеспечения информационной безопасности.	материалов, регламентирующих работу по защите информации.	
ПК-4.2: Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем	**Знать:** -основные нормативно-правовые акты в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации; - основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.	**Уметь:** - оформлять техническую и проектную документацию по регламентации вопросов создания и эксплуатации автоматизированных систем; - оформлять техническую документацию в соответствии с действующими нормативными документами.	**Владеть:** - навыками ведения документов учета, обработки, хранения и передачи информации, составляющей профессиональную, коммерческую, служебную или иную тайну.
ПК-4.3: Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации	**Знать:** - требования защиты информации; -методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля функциональных характеристик работы системы;	**Уметь:** - формализовать выборки для формирования сообщений; - составлять простые и составные запросы к системам учета; - проводить анализ основных характеристик системы.	**Владеть:** - общими приемами организации поиска; - алгоритмическими схемами оценки характеристик; - навыками анализа ожидаемых и фактических результатов работы системы.
ПК-4.4: Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем	**Знать:** - основные методы управления защитой информации; - основные угрозы безопасности информации и	**Уметь:** - оценивать информационные риски в автоматизированных системах; - классифицировать	**Владеть:** - навыками проведения сравнительного анализа; - навыками проведения

	модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); - методы защиты информации в автоматизированных системах; - варианты конфигураций и их характеристики.	и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы автоматизированных систем; -разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; - конфигурировать параметры системы защиты информации автоматизированных систем.	различных конфигураций; - навыками разработки предложений по совершенствованию систем защиты информации.
ПК-5: Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-5.1: Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности	**Знать:** - реализуемую политику безопасности; - основные характеристики программных и технических средств разработки ПО; - особенности проверки внедряемых решений и средств для обеспечения информационной безопасности.	**Уметь:** - строить модели формирования решений для обеспечения информационной безопасности; -находить возможные решения и средства информационной безопасности; - анализировать возможные несоответствия внедряемых решений.	**Владеть:** - навыком выбора соответствующего решения/ средства для обеспечения информационной безопасности; - навыками разработки средств обеспечения информационной безопасности; - навыками определения соответствия выбранных средств реализуемой политики безопасности.
ПК-5.2: Восстанавливает работоспособность автоматизированных систем после инцидентов информационной	**Знать:** - особенности автоматизированных систем; - виды инцидентов информационной безопасности;	**Уметь:** - определять причину возникновения инцидента информационной безопасности;	**Владеть:** - приемами анализа полноты и корректности ключевых параметров эксплуатации

безопасности	- особенности восстановления автоматизированных систем после инцидентов информационной безопасности.	- анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы автоматизированной системы.	автоматизированных систем; - навыком определения вида инцидента; - навыком восстановления работоспособности автоматизированной системы.
ПК-5.3: Проводит операции вывода защищённых автоматизированных систем из эксплуатации	**Знать:** - содержание и порядок выполнения работ на стадиях создания автоматизированных систем в защищенном исполнении; - технологии повышения защищенности автоматизированных систем из эксплуатации; - особенности вывода защищённых автоматизированных систем из эксплуатации.	**Уметь:** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов автоматизированных систем; - минимизировать последствия ущерба за счет интеграции средств защиты.	**Владеть:** - навыками разработки компонентов автоматизированных систем; - навыками обеспечения совместимого взаимодействия отдельных модулей; - навыками вывода защищённых автоматизированных систем из эксплуатации.
ПК-6: Способен документально оформлять работы по обеспечению информационной безопасности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-6.1: Анализирует полноту и нормативным требованиям руководящих документов, описывающих работы по обеспечению информационной безопасности	**Знать:** - основные нормативно-правовые акты в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации.	**Уметь:** - анализировать полноту и соответствие нормативным требованиям руководящих документов, описывающих работы по обеспечению информационной безопасности.	**Владеть:** - навыками составления перечня руководящих документов, описывающих требования к информационной безопасности; - навыками анализа требований руководящих документов.
ПК-6.2: Формирует	**Знать:**	**Уметь:**	**Владеть:**

отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	-основные нормативно-правовые акты в области информационной безопасности и защиты информации; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности информационных систем; -основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.	- оформлять документацию по регламентации процесса эксплуатации информационной системы с целью обеспечения защиты информации; - оформлять отчётную и техническую документацию в соответствии с действующими нормативными документами.	- навыками составления отчётной и технической документации, описывающей требования к информационной безопасности; - навыками ведения протоколов и журналов учета при изменении конфигурации, осуществлении аудита и мониторинга систем защиты информации информационных систем.
ПК-6.3: Формулирует в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации	**Знать:** - основные нормативно-правовые акты в области информационной безопасности и защиты информации; -методы обеспечения уровня защищённости информации; - принципы построения систем защиты информации.	**Уметь:** - классифицировать и оценивать угрозы безопасности информации для объекта информатизации; - разрабатывать процедуры контроля обеспеченности уровня защищённости информации; - применять действующую законодательную базу в области обеспечения защиты информации.	**Владеть:** - основными криптографическим и методами, алгоритмами и протоколами, используемыми для обеспечения безопасности информации; - способами и средствами защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - принципами построения систем защиты информации.
ПК-6.4: Готовит	**Знать:**	**Уметь:**	**Владеть:**

документы для проведения работ по аттестации объектов информатизации и автоматизированных систем	- порядок организации и проведения аттестации объектов информатизации и информационных систем (ИС); - условия функционирования объектов и ИС; -основные нормативно-правовые акты в области информационной безопасности и защиты информации.	- проверять организационно распорядительную документации по защите информации; - проводить испытания объектов информатизации на соответствие требованиям по защите конфиденциальной информации от утечки; - готовить документы для проведения работ по аттестации объектов информатизации и ИС.	- навыками анализа необходимой документации; - навыками проведения испытаний объектов информатизации и ИС; - навыками подготовки документации для проведения работ по аттестации объектов информатизации и ИС.
ПК-7: Способен определять уровень защищённости автоматизированных систем			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-7.1: Формулирует целевые показатели функционирования защищенных автоматизированных систем	**Знать:** - критерии оценки защищенности автоматизированной системы; - регламент информирования персонала автоматизированной системы о выявленных инцидентах; - регламент учета выявленных инцидентов; - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах.	**Уметь:** - определять источники и причины возникновения инцидентов; - формулировать целевые показатели функционирования защищённых автоматизированных систем; - проводить оценку защищенности автоматизированных систем с помощью типовых программных средств; - рассчитывать и проводить инструментальный контроль показателей эффективности защиты информации.	**Владеть:** - навыками определения источников и причин возникновения инцидентов; - навыками расчёта целевых показателей защищённых автоматизированных систем.
ПК-7.2: Анализирует	**Знать:** - нормативные	**Уметь:** - анализировать	**Владеть:** - навыками

уязвимости автоматизированных систем в соответствии с нормативными документами	документы; - особенности анализа уязвимости автоматизированных систем; - основные виды уязвимости автоматизированных систем.	уязвимости автоматизированных систем в соответствии с требованиями руководящих документов; - минимизировать количество потенциальных несоответствий.	установки директив, определяющих работу автоматизированных систем; - навыками проведения анализа нормативных документов; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.
ПК-7.3: Формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы	**Знать:** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; - основы использования средств защиты информации.	**Уметь:** - организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне.	**Владеть:** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.
ПК-8: Способен выполнять задачи по выявлению уязвимых узлов автоматизированной системы			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-8.1: Разрабатывает методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы	**Знать:** - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; - основные угрозы безопасности информации и модели нарушителя	**Уметь:** - анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации;	**Владеть:** - навыками анализ компонентов автоматизированных систем; - навыками разработки документации.

	в автоматизированных системах; - основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; нормативно-правовые акты в области информационной безопасности и защиты информации.	- разрабатывать методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы; - контролировать эффективность принятых мер по защите информации в автоматизированных системах.	
ПК-8.2: Осуществляет подбор программных средств тестирования защищённости автоматизированной системы в зависимости от предъявляемым к ней требованиям	**Знать:** - принципы построения и функционирования систем и сетей передачи информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах; - принципы построения средств защиты информации от утечки по техническим каналам; - основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных	**Уметь:** - анализировать основные узлы и устройства современных автоматизированных систем; - применять действующую нормативную базу в области обеспечения безопасности информации; - контролировать безотказное функционирование технических средств защиты информации; - составлять методики тестирования систем защиты информации автоматизированных систем; - подбирать программные средства тестирования систем защиты информации автоматизированных систем.	**Владеть:** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз; - навыками анализа основных узлов и устройств современных автоматизированных систем.

	системах; - технические каналы утечки информации; - технические средства контроля эффективности мер защиты информации.		
ПК-8.3: Использует средств инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы	**Знать:** - принципы построения компьютерных систем и сетей; - формальные модели безопасности компьютерных систем и сетей; - принципы построения систем обнаружения компьютерных атак; - методы обработки данных мониторинга безопасности компьютерных систем и сетей; - порядок создания и структура отчета, создаваемого по результатам проверок; - способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; - криптографические протоколы.	**Уметь:** - формализовывать задачу управления безопасностью автоматизированных систем; - применять инструментальные средства проведения мониторинга защищенности автоматизированных систем; - применять методы анализа защищенности компьютерных систем и сетей; - структурировать аналитическую информацию для включения в отчет.	**Владеть:** - навыками выполнения анализа защищенности; - навыками составления отчетов по результатам проверок.
ПК-8.4: Проводит контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы	**Знать:** - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации; - способы и средства защиты информации	**Уметь:** - классифицировать и оценивать угрозы безопасности информации для объекта информатизации; -разрабатывать предложения по совершенствованию системы управления	**Владеть:** - навыками оценки информационных рисков; - навыками экспертизы состояния защищенности информации автоматизированных систем;

	от утечки по техническим каналам и контроля эффективности защиты информации; -принципы построения систем защиты информации.	информационной безопасностью автоматизированных систем; - разрабатывать политики безопасности информации автоматизированных систем; - применять действующую законодательную базу в области обеспечения защиты информации.	- навыками обоснования критериев эффективности функционирования защищенных автоматизированных систем.
ПК-9: Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-9.1: Формулирование правил работы персонала со средствами защиты информации	**Знать:** - нормативно-правовые акты в области информационной безопасности и защиты информации; - регламент информирования персонала автоматизированной системы о выявленных инцидентах.	**Уметь:** - устанавливать и настраивать средства защиты информации; - выявлять степень участия персонала в обработке защищаемой информации; - осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; - обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации.	**Владеть:** - навыками оценки работы технических средств; - навыками анализа эффективности их работы; - навыками разработки регламентов работы.
ПК-9.2: Распределяет	**Знать:** - обязанности и	**Уметь:** - разрабатывать	**Владеть:** - навыками

обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему	полномочия персонала, обслуживающего защищённую автоматизированную систему; - типовые политики безопасности.	политики безопасности на основе обязанностей и полномочий персонала, обслуживающего защищённую автоматизированную систему; - определять критерии, требуемой степени защищенности.	настройки политик безопасности; - распределения полномочий персонала, обслуживающего защищённую автоматизированную систему.
ПК-9.3: Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации	**Знать:** - организацию явного и скрытого контроля за работой пользователей и персонала автоматизированной системы.	**Уметь:** - проводить анализ работы персонала в плане информационной безопасности.	**Владеть:** - навыками сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации; - навыками проведения аудита информационной безопасности.
ПК-10: Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности			
Планируемые результаты обучения, соответствующие индикаторам достижения компетенции			
ПК-10.1: Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации	**Знать:** - типовые инциденты информационной безопасности АС, состав, документацию, характеристики и принцип работы оборудования АС; - классификацию, состав, документацию, способы применения систем и средств защиты информации в АС.	**Уметь:** - классифицировать инциденты информационной безопасности АС; - применять средства защиты информации в АС; - определять уязвимые узлы в системе информационной безопасности; - осуществлять контроль функционирования систем и средств защиты АС;	**Владеть:** - навыками применения программных и аппаратных средств защиты информации в АС; - обнаружения инцидентов и восстановления функционирования оборудования АС; - контроля и анализа результатов выполняемых работ.

		- проводить анализ результатов выполняемых работ.	
ПК-10.2: Обосновывает необходимость модернизации системы защиты информации автоматизированной системы	**Знать:** - модель нарушителя: - порядок оценки угроз безопасности информации.	**Уметь:** - обосновывать необходимость модернизации системы защиты информации автоматизированной системы.	**Владеть:** - навыками разработки модели нарушителя информационной системы.
ПК-10.3: Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности	**Знать:** - меры защиты информации; - типовые инциденты информационной безопасности.	**Уметь:** - выявлять, анализировать и устранять уязвимости информационной системы.	**Владеть:** - навыками устранение причин возникновения инцидентов информационной безопасности.
ПК-10.4: Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем	**Знать:** - задачи и функции систем и средств мониторинга и управления средствами обеспечения безопасности АС; - правила эксплуатации оборудования и программных средств управления средствами защиты АС; - классификацию и способы применения средств и систем защиты АС.	**Уметь:** - проводить анализ защищенности АС; - разрабатывать правила протоколирования результатов мониторинга АС; - настраивать оборудования и программных средств мониторинга и управления средствами защиты АС; - средства и системы защиты АС.	**Владеть:** - навыками анализа защищенности АС; - навыками эксплуатации программных средств мониторинга и управления средствами зашиты АС; - навыками разработки правил протоколирования результатов мониторинга АС; - навыками настройки оборудования и программных средств мониторинга и управления средствами защиты АС.

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

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 (преддипломная)

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 (преддипломная)

Планируемые результаты обучения /Уровень сформированности компетенций	Критерии оценивания			
	«Неудовлетворительно» / нулевой уровень	«Удовлетворительно» /низкий уровень	«Хорошо» / средний уровень	«Отлично» / высокий уровень
УНИВЕРСАЛЬНЫЕ И ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ УК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-8; ОПК-9; ОПК-10; ОПК-12; ОПК-4.1; ОПК-4.2; ОПК-4.3; ОПК-4.4				
Теоретические показатели				
УК-1.1: Анализирует задачу, выделяя ее базовые составляющие УК-1.2: Определяет и ранжирует информацию, требуемую для решения поставленной задачи	Обучающийся **не знает:** - основные этапы развития технологии программирования; - принципы построения программных систем; - этапы разработки	Обучающийся **частично знает:** - основные этапы развития технологии программирования; - принципы построения программных систем; - этапы разработки	Обучающийся **знает:** - основные этапы развития технологии программирования; - принципы построения программных систем; - этапы разработки	Обучающийся полностью **знает** - основные этапы развития технологии программирования; - принципы построения программных систем; - этапы разработки

УК-1.3: Осуществляет поиск информации для решения поставленной задачи по различным типам запросов ОПК-2.1: Ищет информацию в глобальной информационной сети Интернет ОПК-2.2: Подготавливает документы в среде типовых офисных пакетов ОПК-2.3: Определяет состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств ОПК-2.4: Применяет технические и программные средств тестирования с целью определения исправности компьютера и оценки его производительности ОПК-3.1: Использует методы аналитической геометрии и векторной алгебры при решении прикладных задач ОПК-3.2: Использует типовые модели и методы математического анализа при решении стандартных прикладных задач ОПК-3.3: Выполняет типовые	программного обеспечения; - модели жизненного цикла программного обеспечения; - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности; - существующие системы глобального поиска - варианты использования поисковых систем внутри профессионального сервиса - правила формирования запросов на основе ключевых словосочетаний на русском и английском языке - основы использования расширенных параметров поиска; - основы работы и разновидности офисных пакетов - основы подготовки документов и отчетных форм на основе текста	- этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности; - существующие системы глобального поиска - варианты использования поисковых систем внутри профессионального сервиса - правила формирования запросов на основе ключевых словосочетаний на русском и английском языке - основы использования расширенных параметров поиска;	программного обеспечения; - модели жизненного цикла программного обеспечения; - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности; - существующие системы глобального поиска - варианты использования поисковых систем внутри профессионального сервиса - правила формирования запросов на основе ключевых словосочетаний на русском и английском языке - основы использования расширенных	- этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта; - нормативно-правовые аспекты обеспечения информационной безопасности; - существующие системы глобального поиска - варианты использования поисковых систем внутри профессионального сервиса - правила формирования запросов на основе ключевых словосочетаний на русском и английском языке

расчеты с использованием основных формул дифференциального и интегрального исчисления ОПК-3.4: Использует расчетные формулы и таблицы при решении стандартных вероятностно-статистических задач ОПК-3.5: Решает задачи профессиональной области с применением дискретных моделей ОПК-4.1: Решает базовые прикладные физические задачи ОПК-4.2: Анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях ОПК-4.3: Анализирует процессы, протекающие в линейных и нелинейных электрических цепях ОПК-5.1: Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов,	- основы подготовки документов на основе электронных таблиц - основы подготовки презентаций; - основы аппаратного обеспечения вычислительной техники - разновидности типов оперативной и постоянной памяти, центрального процессора, материнской платы и видеокарты - способы диагностики и получения данных о составе и параметрах оборудования; - основные разновидности и средства программной диагностики работы компьютера - основы оценки производительности ПК на базе прикладных решений - типовые нештатные ситуации, предполагающие локализацию неисправности в работе программных или аппаратных элементов вычислительной системы; -основные приемы решения математических задач; - утверждения для обоснования выбираемых методов математического	- основы работы и разновидности офисных пакетов - основы подготовки документов и отчетных форм на основе текста - основы подготовки документов на основе электронных таблиц - основы подготовки презентаций; - основы аппаратного обеспечения вычислительной техники - разновидности типов оперативной и постоянной памяти, центрального процессора, материнской платы и видеокарты - способы диагностики и получения данных о составе и параметрах оборудования; - основные разновидности и средства программной диагностики работы компьютера - основы оценки производительности ПК на базе прикладных решений - типовые нештатные	параметров поиска; - основы работы и разновидности офисных пакетов - основы подготовки документов и отчетных форм на основе текста - основы подготовки документов на основе электронных таблиц - основы подготовки презентаций; - основы аппаратного обеспечения вычислительной техники - разновидности типов оперативной и постоянной памяти, центрального процессора, материнской платы и видеокарты - способы диагностики и получения данных о составе и параметрах оборудования; - основные разновидности и средства программной диагностики работы компьютера - основы оценки производительности ПК на базе прикладных решений	- основы использования расширенных параметров поиска; - основы работы и разновидности офисных пакетов - основы подготовки документов и отчетных форм на основе текста - основы подготовки документов на основе электронных таблиц - основы подготовки презентаций; - основы аппаратного обеспечения вычислительной техники - разновидности типов оперативной и постоянной памяти, центрального процессора, материнской платы и видеокарты - способы диагностики и получения данных о составе и параметрах оборудования; - основные разновидности и средства программной диагностики работы компьютера

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 ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации 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	анализа и их следствия; - основные понятия о погрешности вычислений; - основные требования, предъявляемые к вычислительным схемам (корректность, устойчивость, сходимость); - основные методы и алгоритмы численного интегрирования и дифференцирования; - методы и алгоритмы теории обработки результатов эксперимента; - содержание основных понятий дискретной математики; - основные приемы работы с комбинаторными объектами, булевыми функциями, графами; - возможности использования дискретной математики в будущей профессиональной деятельности; - виды ресурсов и ограничений для решения профессиональных задач; - основные методы оценки разных способов решения задач, действующее законодательство и	ситуации, предполагающие локализацию неисправности в работе программных или аппаратных элементов вычислительной системы; -основные приемы решения математических задач; - утверждения для обоснования выбираемых методов математического анализа и их следствия; - основные понятия о погрешности вычислений; - основные требования, предъявляемые к вычислительным схемам (корректность, устойчивость, сходимость); - основные методы и алгоритмы численного интегрирования и дифференцирования; - методы и алгоритмы теории обработки результатов эксперимента; - содержание основных понятий дискретной	- типовые нештатные ситуации, предполагающие локализацию неисправности в работе программных или аппаратных элементов вычислительной системы; -основные приемы решения математических задач; - утверждения для обоснования выбираемых методов математического анализа и их следствия; - основные понятия о погрешности вычислений; - основные требования, предъявляемые к вычислительным схемам (корректность, устойчивость, сходимость); - основные методы и алгоритмы численного интегрирования и дифференцирования; - методы и алгоритмы теории обработки результатов эксперимента;	- основы оценки производительности ПК на базе прикладных решений - типовые нештатные ситуации, предполагающие локализацию неисправности в работе программных или аппаратных элементов вычислительной системы; -основные приемы решения математических задач; - утверждения для обоснования выбираемых методов математического анализа и их следствия; - основные понятия о погрешности вычислений; - основные требования, предъявляемые к вычислительным схемам (корректность, устойчивость, сходимость); - основные методы и алгоритмы численного интегрирования и дифференцирования;

проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ОПК-8.1: Составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов ОПК-8.2: Систематизирует научную информацию в области информационной безопасности ОПК-8.3: Использует информационно-справочные системы при поиске информации в области профессиональной деятельности 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,	правовые нормы, регулирующие профессиональную деятельность; - базовые физические законы; - модели для решения задач профессиональной деятельности; - принципы действия основных электрических устройств и электронных приборов, их эквивалентные схемы; - характеристики и параметры; - методы измерения параметров и расчета цепей; - современные средства автоматизированного проектирования ЭС; - интерфейс, библиотеки, функциональные возможности современных САПР; - методы моделирования электронных средств в САПР; - правовые основы организации защиты конфиденциальной информации; - задачи органов защиты информации;	математики; - основные приемы работы с комбинаторными объектами, булевыми функциями, графами; - возможности использования дискретной математики в будущей профессиональной деятельности; - виды ресурсов и ограничений для решения профессиональных задач; - основные методы оценки разных способов решения задач, действующее законодательство и правовые нормы, регулирующие профессиональную деятельность; - базовые физические законы; - модели для решения задач профессиональной деятельности; - принципы действия основных электрических устройств и электронных приборов, их эквивалентные схемы;	- содержание основных понятий дискретной математики; - основные приемы работы с комбинаторными объектами, булевыми функциями, графами; - возможности использования дискретной математики в будущей профессиональной деятельности; - виды ресурсов и ограничений для решения профессиональных задач; - основные методы оценки разных способов решения задач, действующее законодательство и правовые нормы, регулирующие профессиональную деятельность; - базовые физические законы; - модели для решения задач профессиональной деятельности; - принципы действия основных электрических	- методы и алгоритмы теории обработки результатов эксперимента; - содержание основных понятий дискретной математики; - основные приемы работы с комбинаторными объектами, булевыми функциями, графами; - возможности использования дискретной математики в будущей профессиональной деятельности; - виды ресурсов и ограничений для решения профессиональных задач; - основные методы оценки разных способов решения задач, действующее законодательство и правовые нормы, регулирующие профессиональную деятельность; - базовые физические законы;

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	- 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 систем; - модели угроз и модели нарушителя; - основные требования, предъявляемые к	- характеристики и параметры; - методы измерения параметров и расчета цепей; - современные средства автоматизированного проектирования ЭС; - интерфейс, библиотеки, функциональные возможности современных САПР; - методы моделирования электронных средств в САПР; - правовые основы 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	устройств и электронных приборов, их эквивалентные схемы; - характеристики и параметры; - методы измерения параметров и расчета цепей; - современные средства автоматизированного проектирования ЭС; - интерфейс, библиотеки, функциональные возможности современных САПР; - методы моделирования электронных средств в САПР; - правовые основы 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	- модели для решения задач профессиональной деятельности; - принципы действия основных электрических устройств и электронных приборов, их эквивалентные схемы; - характеристики и параметры; - методы измерения параметров и расчета цепей; - современные средства автоматизированного проектирования ЭС; - интерфейс, библиотеки, функциональные возможности современных САПР; - методы моделирования электронных средств в САПР; - правовые основы организации защиты конфиденциальной информации; - задачи органов защиты информации;

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 автоматизированной системе ОПК-4.1.3: Организует работу персонала	сотрудникам защиты информации ограниченного доступа; - угрозы безопасности; - модели нарушителя объекта информатизации; - требования руководящих документов по физической защите объектов информатизации; - требования по пропускному режиму в организации; - требования руководящих документов регламентирующих защиту информации ограниченного доступа; - основы составления рефератов по результатам поиска на основе научно-технической документации - нормативную и методическую базу профессиональной области; - основы систематизации данных в профессиональной предметной области - актуальные источники, регламентирующие порядок обеспечения информационной безопасности; - основные информационно-	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; - модели угроз и модели нарушителя; - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - угрозы безопасности; - модели нарушителя объекта информатизации; - требования руководящих документов по физической защите объектов	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; - модели угроз и модели нарушителя; - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - угрозы безопасности; - модели нарушителя объекта	- 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

автоматизированной системы с учетом требований по защите информации	справочные системы, содержащие документы профессиональной области - правила выделения необходимой информации с учетом параметрических поисковых запросов; - 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; - классификацию методов шифрования; - модель криптосистемы с открытым ключом; - требования к качественной хеш-функции; - виды криптографических протоколов; - основные виды угроз безопасности; - возможные каналы утечки	информатизации; - требования по пропускному режиму в организации; - требования руководящих документов регламентирующих защиту информации ограниченного доступа; - основы составления рефератов по результатам поиска на основе научно-технической документации - нормативную и методическую базу профессиональной области; - основы систематизации данных в профессиональной предметной области - актуальные источники, регламентирующие порядок обеспечения информационной безопасности; - основные информационно-справочные системы, содержащие документы профессиональной области - правила выделения	информатизации; - требования руководящих документов по физической защите объектов информатизации; - требования по пропускному режиму в организации; - требования руководящих документов регламентирующих защиту информации ограниченного доступа; - основы составления рефератов по результатам поиска на основе научно-технической документации - нормативную и методическую базу профессиональной области; - основы систематизации данных в профессиональной предметной области - актуальные источники, регламентирующие порядок обеспечения информационной безопасности; - основные	систем; - модели угроз и модели нарушителя; - основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - угрозы безопасности; - модели нарушителя объекта информатизации; - требования руководящих документов по физической защите объектов информатизации; - требования по пропускному режиму в организации; - требования руководящих документов регламентирующих защиту информации ограниченного доступа; - основы составления рефератов по результатам поиска на основе научно-технической документации - нормативную и
ОПК-4.1.4: Организует работу персонала автоматизированной системы с учетом требований по защите информации				
ОПК-4.2.1: Настраивает операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации				
ОПК-4.2.2: Применяет программные средства обеспечения безопасности данных				
ОПК-4.2.3: Управляет полномочиями пользователей автоматизированной системы				
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 ОПК-4.4.1: Применяет инструментальные средства контроля защищенности информации в автоматизированных системах ОПК-4.4.2: Документирует действия по устранению неисправностей в работе системы защиты информации автоматизированной системы ОПК-4.4.3: Регистрирует события, связанные с защитой информации в автоматизированных системах	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; - угрозы информационной безопасности объекта информатизации; - средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - требования политик безопасности на объектах информатизации; - систему хранения и обработки информации; - принципы идентификации записей; - основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы атак; - основные принципы построения подсистем защиты компьютерной	необходимой информации с учетом параметрических поисковых запросов; - 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; - классификацию методов шифрования; - модель криптосистемы с открытым ключом; - требования к качественной хеш-функции; - виды криптографических протоколов; - основные виды угроз безопасности; - возможные каналы	информационно-справочные системы, содержащие документы профессиональной области - правила выделения необходимой информации с учетом параметрических поисковых запросов; - 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; - классификацию методов шифрования; - модель криптосистемы с открытым ключом; - требования к качественной хеш-функции;	методическую базу профессиональной области; - основы систематизации данных в профессиональной предметной области - актуальные источники, регламентирующие порядок обеспечения информационной безопасности; - основные информационно-справочные системы, содержащие документы профессиональной области - правила выделения необходимой информации с учетом параметрических поисковых запросов; - основы криптографии, методы защиты; - классификацию криптографических методов; - основы шифрования с помощью скремблеров; - основы шифрования с помощью ассиметричных

	информации в операционных системах и в пользовательских программных приложениях; - сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации; - принципы функционирования основных типов вредоносных программ, способы их выявления и нейтрализации; - 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	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; - угрозы информационной безопасности объекта информатизации; - средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - требования политик безопасности на объектах информатизации; - систему хранения и обработки информации; - принципы идентификации записей; - основные угрозы компьютерной информации, реализуемые на различных уровнях	- виды криптографических протоколов; - 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; - угрозы информационной безопасности объекта информатизации; - средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - требования политик безопасности на объектах информатизации; - систему хранения и	алгоритмов; - основы шифрования перспективными методами; - основы программной реализации криптографических преобразований; - классификацию методов шифрования; - модель криптосистемы с открытым ключом; - требования к качественной хеш-функции; - виды криптографических протоколов; - 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

	расчетов характеристик программно-аппаратных средств защиты информации; - принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации; - нормативные правовые акты в области защиты информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - информационную инфраструктуру и информационные ресурсы, подлежащие защите; - показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - информационные риски в автоматизированных системах; - основные методы управления	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 основных типов вредоносных программ, способы их выявления и нейтрализации; - принципы построения компьютерных сетей, операционных систем; - стек сетевых протоколов операционных систем, стек протоколов сетевого оборудования; - порядок реализации методов и средств межсетевого экранирования;	обработки информации; - принципы идентификации записей; - 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 основных типов вредоносных программ, способы их выявления и нейтрализации; - принципы построения компьютерных сетей, операционных систем; - стек сетевых	каналам на объектах информатизации; - угрозы информационной безопасности объекта информатизации; - средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - требования политик безопасности на объектах информатизации; - систему хранения и обработки информации; - принципы идентификации записей; - 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

	информационной безопасностью; - основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов; - основные отечественные и 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; - подлежащие защите информационные ресурсы автоматизированных	- 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 информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - информационную инфраструктуру и информационные ресурсы, подлежащие защите;	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 информации; - особенности применения средств защиты информации в типовых операционных	программных приложениях; - сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации; - принципы функционирования основных типов вредоносных программ, способы их выявления и нейтрализации; - 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;

	систем; - принципы и методы обеспечения защиты информации в автоматизированной системе; - требования по защите информации; - разновидности и принципы построения современных операционных систем - основы использования систем управления базами данных - основы построения и настройки вычислительных сетей; - основные типы неисправностей в автоматизированных системах, методы и способы их устранения; - классификацию инцидентов информационной безопасности - критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах; - принципы автономной	- показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - информационные риски в автоматизированных системах; - основные методы управления информационной безопасностью; - основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов; - основные отечественные и 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	системах, системах управления базами данных, компьютерных сетях; - информационную инфраструктуру и информационные ресурсы, подлежащие защите; - показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - информационные риски в автоматизированных системах; - основные методы управления информационной безопасностью; - основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов; - основные отечественные и зарубежные стандарты в области защиты информации; -основные меры по защите информации в автоматизированных	- 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 информации; - особенности применения средств защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - информационную инфраструктуру и информационные ресурсы, подлежащие защите; - показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;

	наладки технических и программных средств системы защиты информации автоматизированной системы; - порядок эксплуатации средств антивирусной защиты; - порядок обеспечения безопасности при эксплуатации технических и программных средств; - порядок администрирования технических и программных средств системы защиты информации автоматизированной системы; - порядок применения программных средства обеспечения безопасности данных; - перечень информации, подлежащей резервному копированию; - методику проведения резервного копирования; - принципы восстановления информации в автоматизированных системах;	оценки защищенности и методы защиты информации в автоматизированных системах; - основные показатели технико-экономического обоснования соответствующих проектных решений; - подлежащие защите информационные ресурсы автоматизированных систем; - принципы и методы обеспечения защиты информации в автоматизированной системе; - требования по защите информации; - разновидности и принципы построения современных операционных систем - основы использования систем управления базами данных - основы построения и настройки вычислительных сетей; - основные типы неисправностей в	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; - подлежащие защите информационные ресурсы автоматизированных систем; - принципы и методы обеспечения защиты информации в автоматизированной системе; - требования по защите информации; - разновидности и принципы построения современных	- информационные риски в автоматизированных системах; - основные методы управления информационной безопасностью; - основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов; - основные отечественные и 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

	- порядок разграничения доступа к информационным ресурсам; - состав, назначение и основные характеристики современных инструментальных средств контроля защищенности информации в автоматизированных системах; - основные типы неисправностей в автоматизированных системах, методы и способы их устранения; - классификацию инцидентов информационной безопасности, критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах.	автоматизированных системах, методы и способы их устранения; - классификацию инцидентов информационной безопасности - критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах; - принципы автономной наладки технических и программных средств системы защиты информации автоматизированной системы; - порядок эксплуатации средств антивирусной защиты; - порядок обеспечения безопасности при эксплуатации технических и программных средств; - порядок администрирования технических и программных средств системы защиты информации	операционных систем - основы использования систем управления базами данных - основы построения и настройки вычислительных сетей; - основные типы неисправностей в автоматизированных системах, методы и способы их устранения; - классификацию инцидентов информационной безопасности - критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах; - принципы автономной наладки технических и программных средств системы защиты информации автоматизированной системы; - порядок эксплуатации средств антивирусной защиты; - порядок обеспечения безопасности при	системах; - основные показатели технико-экономического обоснования соответствующих проектных решений; - подлежащие защите информационные ресурсы автоматизированных систем; - принципы и методы обеспечения защиты информации в автоматизированной системе; - требования по защите информации; - разновидности и принципы построения современных операционных систем - основы использования систем управления базами данных - основы построения и настройки вычислительных сетей; - основные типы неисправностей в автоматизированных системах, методы и способы их устранения;

		автоматизированной системы; - порядок применения программных средства обеспечения безопасности данных; - перечень информации, подлежащей резервному копированию; - методику проведения резервного копирования; - принципы восстановления информации в автоматизированных системах; - порядок разграничения доступа к информационным ресурсам; - состав, назначение и основные характеристики современных инструментальных средств контроля защищенности информации в автоматизированных системах; - основные типы неисправностей в автоматизированных системах, методы и способы их устранения;	эксплуатации технических и программных средств; - порядок администрирования технических и программных средств системы защиты информации автоматизированной системы; - порядок применения программных средства обеспечения безопасности данных; - перечень информации, подлежащей резервному копированию; - методику проведения резервного копирования; - принципы восстановления информации в автоматизированных системах; - порядок разграничения доступа к информационным ресурсам; - состав, назначение и основные характеристики современных инструментальных	- классификацию инцидентов информационной безопасности - критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах; - принципы автономной наладки технических и программных средств системы защиты информации автоматизированной системы; - порядок эксплуатации средств антивирусной защиты; - порядок обеспечения безопасности при эксплуатации технических и программных средств; - порядок администрирования технических и программных средств системы защиты информации автоматизированной системы; - порядок применения

		- классификацию инцидентов информационной безопасности, критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах.	средств контроля защищенности информации в автоматизированных системах; - основные типы неисправностей в автоматизированных системах, методы и способы их устранения; - классификацию инцидентов информационной безопасности, критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах.	программных средства обеспечения безопасности данных; - перечень информации, подлежащей резервному копированию; - методику проведения резервного копирования; - принципы восстановления информации в автоматизированных системах; - порядок разграничения доступа к информационным ресурсам; - состав, назначение и основные характеристики современных инструментальных средств контроля защищенности информации в автоматизированных системах; - основные типы неисправностей в автоматизированных системах, методы и способы их устранения;

				- классификацию инцидентов информационной безопасности, критерии отнесения событий к инцидентам информационной безопасности в автоматизированных системах.
Практические показатели				
УК-1.1: Анализирует задачу, выделяя ее базовые составляющие УК-1.2: Определяет и ранжирует информацию, требуемую для решения поставленной задачи УК-1.3: Осуществляет поиск информации для решения поставленной задачи по различным типам запросов ОПК-2.1: Ищет информацию в глобальной информационной сети Интернет ОПК-2.2: Подготавливает документы в среде типовых офисных пакетов	Обучающийся **не умеет:** - пользоваться понятийным аппаратом методов разработки программных систем; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы функционирования программных систем; - выполнять операции импорта/экспорта данных при работе с программными средами; - разрабатывать техническое задание на проектирование	Обучающийся **частично умеет:** - пользоваться понятийным аппаратом методов разработки программных систем; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы функционирования программных систем; - выполнять операции импорта/экспорта данных при работе с программными средами; - разрабатывать техническое задание на	Обучающийся **умеет:** - пользоваться понятийным аппаратом методов разработки программных систем; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы функционирования программных систем; - выполнять операции импорта/экспорта данных при работе с программными средами; - разрабатывать техническое задание на проектирование	Обучающийся **умеет на высоком уровне:** - пользоваться понятийным аппаратом методов разработки программных систем; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы функционирования программных систем; - выполнять операции импорта/экспорта данных при работе с программными средами;

ОПК-2.3: Определяет состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств ОПК-2.4: Применяет технические и программные средств тестирования с целью определения исправности компьютера и оценки его производительности ОПК-3.1: Использует методы аналитической геометрии и векторной алгебры при решении прикладных задач ОПК-3.2: Использует типовые модели и методы математического анализа при решении стандартных прикладных задач ОПК-3.3: Выполняет типовые расчеты с использованием основных формул дифференциального и интегрального исчисления ОПК-3.4: Использует расчетные формулы и таблицы при решении стандартных вероятностно-статистических задач	программного обеспечения; - принимать обоснованные решения по выбору архитектуры программного обеспечения, среды программирования, стандартов разработки; - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы; - производить поиск в различных поисковых системах - уточнять поисковый запрос с учетом предварительной выдачи данных - анализировать источники данных и производить расширенный поиск в том числе на англоязычных ресурсах; - создавать и дорабатывать документы на основе текста - производить вычисления, строить графики и визуализировать данные на базе электронных таблиц - разрабатывать презентации для повышения наглядности при демонстрации ключевых	проектирование программного обеспечения; - принимать обоснованные решения по выбору архитектуры программного обеспечения, среды программирования, стандартов разработки; - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы; - производить поиск в различных поисковых системах - уточнять поисковый запрос с учетом предварительной выдачи данных - анализировать источники данных и производить расширенный поиск в том числе на англоязычных ресурсах; - создавать и дорабатывать документы на основе текста - производить вычисления, строить графики и	программного обеспечения; - принимать обоснованные решения по выбору архитектуры программного обеспечения, среды программирования, стандартов разработки; - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы; - производить поиск в различных поисковых системах - уточнять поисковый запрос с учетом предварительной выдачи данных - анализировать источники данных и производить расширенный поиск в том числе на англоязычных ресурсах; - создавать и дорабатывать документы на основе текста - производить вычисления, строить графики и визуализировать данные	- разрабатывать техническое задание на проектирование программного обеспечения; - принимать обоснованные решения по выбору архитектуры программного обеспечения, среды программирования, стандартов разработки; - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы; - производить поиск в различных поисковых системах - уточнять поисковый запрос с учетом предварительной выдачи данных - анализировать источники данных и производить расширенный поиск в том числе на англоязычных ресурсах; - создавать и дорабатывать документы на основе

ОПК-3.5: Решает задачи профессиональной области с применением дискретных моделей ОПК-4.1: Решает базовые прикладные физические задачи ОПК-4.2: Анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях ОПК-4.3: Анализирует процессы, протекающие в линейных и нелинейных электрических цепях 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	показателей деятельности; - проводить получение данных об аппаратном обеспечении персонального компьютера - оценивать быстродействие с учетом имеющегося оборудования - определять совместимость периферийного оборудования с основной вычислительной платформой; - оценивать текущую производительность ПК, сопоставлять ее с номинальной - выявлять нештатные ситуации программных или аппаратных элементов вычислительной системы - использовать прикладные средства для контроля состояния системы; - применять инструментарий математического анализа при решении задач; -анализировать способы решения поставленных задач; - пользоваться учебной и научной литературой; - обоснованно выбрать	визуализировать данные на базе электронных таблиц - разрабатывать презентации для повышения наглядности при демонстрации ключевых показателей деятельности; - проводить получение данных об аппаратном обеспечении персонального компьютера - оценивать быстродействие с учетом имеющегося оборудования - определять совместимость периферийного оборудования с основной вычислительной платформой; - оценивать текущую производительность ПК, сопоставлять ее с номинальной - выявлять нештатные ситуации программных или аппаратных элементов вычислительной системы - использовать	на базе электронных таблиц - разрабатывать презентации для повышения наглядности при демонстрации ключевых показателей деятельности; - проводить получение данных об аппаратном обеспечении персонального компьютера - оценивать быстродействие с учетом имеющегося оборудования - определять совместимость периферийного оборудования с основной вычислительной платформой; - оценивать текущую производительность ПК, сопоставлять ее с номинальной - выявлять нештатные ситуации программных или аппаратных элементов вычислительной системы - использовать прикладные средства для	текста - производить вычисления, строить графики и визуализировать данные на базе электронных таблиц - разрабатывать презентации для повышения наглядности при демонстрации ключевых показателей деятельности; - проводить получение данных об аппаратном обеспечении персонального компьютера - оценивать быстродействие с учетом имеющегося оборудования - определять совместимость периферийного оборудования с основной вычислительной платформой; - оценивать текущую производительность ПК, сопоставлять ее с номинальной

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 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-8.1: Составляет рефераты по результатам обзора научно-технической	численный метод; - разработать алгоритм решения поставленной задачи; - применять полученные знания к численному решению задач практики; - оценивать адекватность полученного численного решения, его сходимость и необходимый ресурс времени; - использовать дискретную математику при проектировании сетей, разработке программного обеспечения; - решать стандартные задачи по дискретной математике; - использовать знания по дискретной математике в решении стандартных задач профессиональной деятельности; - проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; - анализировать альтернативные варианты для достижения намеченных результатов;	прикладные средства для контроля состояния системы; - применять инструментарий математического анализа при решении задач; -анализировать способы решения поставленных задач; - пользоваться учебной и научной литературой; - обоснованно выбрать численный метод; - разработать алгоритм решения поставленной задачи; - применять полученные знания к численному решению задач практики; - оценивать адекватность полученного численного решения, его сходимость и необходимый ресурс времени; - использовать дискретную математику при проектировании сетей, разработке программного обеспечения; - решать стандартные задачи по дискретной математике;	контроля состояния системы; - применять инструментарий математического анализа при решении задач; -анализировать способы решения поставленных задач; - пользоваться учебной и научной литературой; - обоснованно выбрать численный метод; - разработать алгоритм решения поставленной задачи; - применять полученные знания к численному решению задач практики; - оценивать адекватность полученного численного решения, его сходимость и необходимый ресурс времени; - использовать дискретную математику при проектировании сетей, разработке программного обеспечения; - решать стандартные задачи по дискретной математике; - использовать знания по	- выявлять нештатные ситуации программных или аппаратных элементов вычислительной системы - использовать прикладные средства для контроля состояния системы; - применять инструментарий математического анализа при решении задач; -анализировать способы решения поставленных задач; - пользоваться учебной и научной литературой; - обоснованно выбрать численный метод; - разработать алгоритм решения поставленной задачи; - применять полученные знания к численному решению задач практики; - оценивать адекватность полученного численного решения, его сходимость и

литературы, нормативных и методических документов ОПК-8.2: Систематизирует научную информацию в области информационной безопасности ОПК-8.3: Использует информационно-справочные системы при поиске информации в области профессиональной деятельности 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	- использовать нормативно-правовую документацию в сфере профессиональной деятельности; - самостоятельно проводить анализ поставленной задачи; - формулировать задачу с использованием соответствующих физических законов; - осуществлять поиск возможных методов ее решения, выбирать и обосновывать наиболее рациональный метод; - выбирать и рассчитывать режимы работы элементов электронных устройств в схемах; - рассчитывать электрическую схему; - применять современные средства автоматизированного проектирования ЭС; - строить и анализировать временные диаграммы, передаточные и частотные характеристики в САПР; - использовать функциональные	- использовать знания по дискретной математике в решении стандартных задач профессиональной деятельности; - проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; - анализировать альтернативные варианты для достижения намеченных результатов; - использовать нормативно-правовую документацию в сфере профессиональной деятельности; - самостоятельно проводить анализ поставленной задачи; - формулировать задачу с использованием соответствующих физических законов; - осуществлять поиск возможных методов ее решения, выбирать и обосновывать наиболее рациональный метод;	дискретной математике в решении стандартных задач профессиональной деятельности; - проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; - анализировать альтернативные варианты для достижения намеченных результатов; - использовать нормативно-правовую документацию в сфере профессиональной деятельности; - самостоятельно проводить анализ поставленной задачи; - формулировать задачу с использованием соответствующих физических законов; - осуществлять поиск возможных методов ее решения, выбирать и обосновывать наиболее рациональный метод;	необходимый ресурс времени; - использовать дискретную математику при проектировании сетей, разработке программного обеспечения; - решать стандартные задачи по дискретной математике; - использовать знания по дискретной математике в решении стандартных задач профессиональной деятельности; - проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; - анализировать альтернативные варианты для достижения намеченных результатов; - использовать нормативно-правовую документацию в сфере

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	возможности САПР при исследовании и анализе параметров и характеристик ЭС; - 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 и охране результатов интеллектуальной деятельности в организации;	- выбирать и рассчитывать режимы работы элементов электронных устройств в схемах; - рассчитывать электрическую схему; - применять современные средства автоматизированного проектирования ЭС; - строить и анализировать временные диаграммы, передаточные и частотные характеристики в САПР; - использовать функциональные возможности САПР при исследовании и анализе параметров и характеристик ЭС; - применять действующую законодательную базу в области обеспечения информационной безопасности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;	- выбирать и рассчитывать режимы работы элементов электронных устройств в схемах; - рассчитывать электрическую схему; - применять современные средства автоматизированного проектирования ЭС; - строить и анализировать временные диаграммы, передаточные и частотные характеристики в САПР; - использовать функциональные возможности САПР при исследовании и анализе параметров и характеристик ЭС; - применять действующую законодательную базу в области обеспечения информационной безопасности; - классифицировать защищаемую информацию по видам тайны и степеням	профессиональной деятельности; - самостоятельно проводить анализ поставленной задачи; - формулировать задачу с использованием соответствующих физических законов; - осуществлять поиск возможных методов ее решения, выбирать и обосновывать наиболее рациональный метод; - выбирать и рассчитывать режимы работы элементов электронных устройств в схемах; - рассчитывать электрическую схему; - применять современные средства автоматизированного проектирования ЭС; - строить и анализировать временные диаграммы, передаточные и частотные характеристики в САПР; - использовать

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 автоматизированной системе ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации	- 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 проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - разрабатывать модели	- 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	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	функциональные возможности САПР при исследовании и анализе параметров и характеристик ЭС; - 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

ОПК-4.1.4: Организует работу персонала автоматизированной системы с учетом требований по защите информации	угроз объекта информатизации; - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа; - использовать средства физической защиты объекта информатизации; - использовать требования руководящих документов регламентирующих защиту информации ограниченного доступа; - работать с научно-технической литературой - находить нормативные и методические документы, регламентирующие порядок действий; - составлять рефераты по результатам обзора; - систематизировать данные в профессиональной предметной области; - выделять актуальные источники, регламентирующие порядок	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; - разрабатывать модели угроз объекта информатизации; - составлять перечень	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; - разрабатывать модели угроз объекта информатизации;	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; - применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям
ОПК-4.2.1: Настраивает операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации				
ОПК-4.2.2: Применяет программные средства обеспечения безопасности данных				
ОПК-4.2.3: Управляет полномочиями пользователей автоматизированной системы				
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 ОПК-4.4.1: Применяет инструментальные средства контроля защищенности информации в автоматизированных системах ОПК-4.4.2: Документирует действия по устранению неисправностей в работе системы защиты информации автоматизированной системы ОПК-4.4.3: Регистрирует события, связанные с защитой информации в автоматизированных системах	обеспечения информационной безопасности; - работать с информационно-справочными системами, содержащими документы профессиональной области; - составлять параметрические поисковые запросы при поиске информации в справочной системе; - выполнять шифрование криптографическими методами; - определять целесообразность применения тех или иных методов защиты; - анализировать статистику распределения данных после шифрования; - решать задачи криптографической защиты информации с использованием блочных и поточных систем; - решать задачи с использованием криптографических систем с открытым ключом; - решать задачи с использованием	лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа; - использовать средства физической защиты объекта информатизации; - использовать требования руководящих документов регламентирующих защиту информации ограниченного доступа; - работать с научно-технической литературой - находить нормативные и методические документы, регламентирующие порядок действий; - составлять рефераты по результатам обзора; - систематизировать данные в профессиональной предметной области; - выделять актуальные источники,	- составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа; - использовать средства физической защиты объекта информатизации; - использовать требования руководящих документов регламентирующих защиту информации ограниченного доступа; - работать с научно-технической литературой - находить нормативные и методические документы, регламентирующие порядок действий; - составлять рефераты по результатам обзора; - систематизировать данные в профессиональной предметной области;	безопасности информации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - разрабатывать модели угроз объекта информатизации; - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа; - использовать средства физической защиты объекта информатизации; - использовать

	криптографических хеш-функций и протоколов; - 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; - оценивать угрозы информационной безопасности объекта информатизации; - 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 нарушения безопасности	регламентирующие порядок обеспечения информационной безопасности; - работать с информационно-справочными системами, содержащими документы профессиональной области; - составлять параметрические поисковые запросы при поиске информации в справочной системе; - выполнять шифрование криптографическими методами; - определять целесообразность применения тех или иных методов защиты; - анализировать статистику распределения данных после шифрования; - решать задачи криптографической защиты информации с использованием блочных и поточных систем; - решать задачи с использованием криптографических	- выделять актуальные источники, регламентирующие порядок обеспечения информационной безопасности; - работать с информационно-справочными системами, содержащими документы профессиональной области; - составлять параметрические поисковые запросы при поиске информации в справочной системе; - выполнять шифрование криптографическими методами; - определять целесообразность применения тех или иных методов защиты; - анализировать статистику распределения данных после шифрования; - решать задачи криптографической защиты информации с использованием блочных и поточных систем; - решать задачи с	требования руководящих документов регламентирующих защиту информации ограниченного доступа; - работать с научно-технической литературой - находить нормативные и методические документы, регламентирующие порядок действий; - составлять рефераты по результатам обзора; - систематизировать данные в профессиональной предметной области; - выделять актуальные источники, регламентирующие порядок обеспечения информационной безопасности; - работать с информационно-справочными системами, содержащими документы профессиональной

	телекоммуникационных систем; - применять политики безопасности на объектах информатизации; - организовывать выполнение мер по обеспечению информационной безопасности; - 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-аппаратных средств защиты информации в компьютерных сетях;	систем с открытым ключом; - решать задачи с использованием криптографических хеш-функций и протоколов; - 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; - оценивать угрозы информационной безопасности объекта информатизации; - использовать средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - применять известные	использованием криптографических систем с открытым ключом; - решать задачи с использованием криптографических хеш-функций и протоколов; - 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; - оценивать угрозы информационной безопасности объекта информатизации; - использовать средства защиты информации от утечки по техническим каналам и контроля	области; - составлять параметрические поисковые запросы при поиске информации в справочной системе; - выполнять шифрование криптографическими методами; - определять целесообразность применения тех или иных методов защиты; - анализировать статистику распределения данных после шифрования; - 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;

	- оценивать оптимальность выбора программно-аппаратных средств; - 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; - определять информационную инфраструктуру и	методики оценки угроз; - принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности телекоммуникационных систем; - применять политики безопасности на объектах информатизации; - организовывать выполнение мер по обеспечению информационной безопасности; - 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	эффективности защиты информации; - применять известные методики оценки угроз; - принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности телекоммуникационных систем; - применять политики безопасности на объектах информатизации; - организовывать выполнение мер по обеспечению информационной безопасности; - 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	- 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; - оценивать угрозы информационной безопасности объекта информатизации; - 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

	информационные ресурсы организации, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - оценивать информационные риски в автоматизированных системах; - проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня 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	администрировать средства программно-аппаратной защиты информации. - производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях; - оценивать оптимальность выбора программно-аппаратных средств; - 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	подсистему политики безопасности организации; - применять и администрировать средства программно-аппаратной защиты информации. - производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях; - оценивать оптимальность выбора программно-аппаратных средств; - 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	защищенности и снижения рисков нарушения безопасности телекоммуникационных систем; - применять политики безопасности на объектах информатизации; - организовывать выполнение мер по обеспечению информационной безопасности; - 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

	аппаратных и программных систем защиты информации; - разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений; - 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; - устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности; - документировать действия	программно-аппаратных средств защиты информации в компьютерных сетях, операционных системах; - конфигурировать средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - оценивать информационные риски в автоматизированных системах; - проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты	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; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - оценивать информационные риски в автоматизированных системах; - проводить технико-экономическое	средства программно-аппаратной защиты информации. - производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях; - оценивать оптимальность выбора программно-аппаратных средств; - 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

	в журналах безопасности автоматизированных систем; - вести журналы технического обслуживания автоматизированных систем; - вести журнал регистрации инцидентов информационной безопасности в автоматизированных системах с указанием степени важности инцидента; - устанавливать программные и технические средства в соответствии с технической документацией; -производить настройку параметров работы технических и программных средств; - осуществлять автономную наладку технических и программных средств системы защиты информации автоматизированной системы; - применять программные средства обеспечения безопасности данных;	информации в автоматизированной системе с целью обеспечения требуемого уровня 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; - определять подлежащие защите информационные ресурсы автоматизированных систем; - составлять комплексы правил, процедур, практических приемов,	обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня 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; - определять подлежащие защите информационные ресурсы автоматизированных	программно-аппаратных средств защиты информации в компьютерных сетях, операционных системах; - конфигурировать средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - оценивать информационные риски в автоматизированных системах; - проводить технико-экономическое обоснование проектных решений программно-

	- применять типовые программные средства резервирования и восстановления информации в автоматизированных системах; - настраивать систему резервного копирования; - проверять корректность резервной копии; - применять политики безопасности в автоматизированной системе; - применять инструментальные средства контроля защищенности информации в автоматизированных системах; - документировать действия в журналах безопасности автоматизированных систем, вести журналы технического обслуживания автоматизированных систем; - вести журнал регистрации инцидентов информационной безопасности в автоматизированных системах с указанием	принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - разрабатывать организационно-распорядительные документы по защите информации; - устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности; - документировать действия в журналах безопасности автоматизированных систем; - вести журналы технического обслуживания автоматизированных систем; - вести журнал регистрации инцидентов информационной безопасности в автоматизированных системах с указанием степени важности	систем; - составлять комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - разрабатывать организационно-распорядительные документы по защите информации; - устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности; - документировать действия в журналах безопасности автоматизированных систем; - вести журналы технического обслуживания автоматизированных систем; - вести журнал регистрации инцидентов информационной	аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня 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; - определять

	степени важности инцидента.	инцидента; - устанавливать программные и технические средства в соответствии с технической документацией; -производить настройку параметров работы технических и программных средств; - осуществлять автономную наладку технических и программных средств системы защиты информации автоматизированной системы; - 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;	безопасности в автоматизированных системах с указанием степени важности инцидента; - устанавливать программные и технические средства в соответствии с технической документацией; -производить настройку параметров работы технических и программных средств; - осуществлять автономную наладку технических и программных средств системы защиты информации автоматизированной системы; - применять программные средства обеспечения безопасности данных; - применять типовые программные средства резервирования и восстановления информации в автоматизированных системах;	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; - устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности; - документировать действия в журналах безопасности автоматизированных систем; - вести журналы технического обслуживания автоматизированных

		- применять политики безопасности в автоматизированной системе; - применять инструментальные средства контроля защищенности информации в автоматизированных системах; - документировать действия в журналах безопасности автоматизированных систем, вести журналы технического обслуживания автоматизированных систем; - вести журнал регистрации инцидентов информационной безопасности в автоматизированных системах с указанием степени важности инцидента.	- настраивать систему резервного копирования; - проверять корректность резервной копии; - применять политики безопасности в автоматизированной системе; - применять инструментальные средства контроля защищенности информации в автоматизированных системах; - документировать действия в журналах безопасности автоматизированных систем, вести журналы технического обслуживания автоматизированных систем; - вести журнал регистрации инцидентов информационной безопасности в автоматизированных системах с указанием степени важности инцидента.	систем; - вести журнал регистрации инцидентов информационной безопасности в автоматизированных системах с указанием степени важности инцидента; - устанавливать программные и технические средства в соответствии с технической документацией; -производить настройку параметров работы технических и программных средств; - осуществлять автономную наладку технических и программных средств системы защиты информации автоматизированной системы; - 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; - применять политики безопасности в автоматизированной системе; - применять инструментальные средства контроля защищенности информации в автоматизированных системах; - документировать действия в журналах безопасности автоматизированных систем, вести журналы технического обслуживания автоматизированных систем; - вести журнал регистрации инцидентов

				информационной безопасности в автоматизированных системах с указанием степени важности инцидента.
Практико-ориентированные показатели (навыки)				
УК-1.1: Анализирует задачу, выделяя ее базовые составляющие УК-1.2: Определяет и ранжирует информацию, требуемую для решения поставленной задачи УК-1.3: Осуществляет поиск информации для решения поставленной задачи по различным типам запросов ОПК-2.1: Ищет информацию в глобальной информационной сети Интернет ОПК-2.2: Подготавливает документы в среде типовых офисных пакетов ОПК-2.3: Определяет состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных	Обучающийся **не владеет:** - базовыми элементами технологии разработки; - программными приемами декларативного описания предметной области; - навыками структуризации знаний и его программирования; - правилами ранжирования информации; - процедурами упорядочения элементов; - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур; - технологией формирования поискового запроса на основе ключевых слов - навыками анализа результатов работы	Обучающийся **частично владеет:** - базовыми элементами технологии разработки; - программными приемами декларативного описания предметной области; - навыками структуризации знаний и его программирования; - правилами ранжирования информации; - процедурами упорядочения элементов; - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур;	Обучающийся **владеет на среднем уровне:** - базовыми элементами технологии разработки; - программными приемами декларативного описания предметной области; - навыками структуризации знаний и его программирования; - правилами ранжирования информации; - процедурами упорядочения элементов; - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур; - технологией формирования	Обучающийся **владеет на высоком уровне:** - базовыми элементами технологии разработки; - программными приемами декларативного описания предметной области; - навыками структуризации знаний и его программирования; - правилами ранжирования информации; - процедурами упорядочения элементов; - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования

устройств ОПК-2.4: Применяет технические и программные средств тестирования с целью определения исправности компьютера и оценки его производительности ОПК-3.1: Использует методы аналитической геометрии и векторной алгебры при решении прикладных задач ОПК-3.2: Использует типовые модели и методы математического анализа при решении стандартных прикладных задач ОПК-3.3: Выполняет типовые расчеты с использованием основных формул дифференциального и интегрального исчисления ОПК-3.4: Использует расчетные формулы и таблицы при решении стандартных вероятностно-статистических задач ОПК-3.5: Решает задачи профессиональной области с применением дискретных моделей ОПК-4.1: Решает базовые	поисковых систем (топ выдачи) - навыками поиска и сопоставления результатов на русском и английском языке, в том числе с разнородным контентом№ - навыками работы с текстом с расширенным форматированием - навыками составления электронных таблиц с организацией вычислений - навыками создания презентаций для демонстрации результатов работы и повышения их наглядности; - навыками получения данных в режиме программного опроса оборудования - навыками определения состава вычислительной системы на основе интегрированного и периферийного оборудования на уровне визуального анализа - навыками оценки номинального быстродействия ПК; - навыками оценки производительности	- технологией формирования поискового запроса на основе ключевых слов - навыками анализа результатов работы поисковых систем (топ выдачи) - навыками поиска и сопоставления результатов на русском и английском языке, в том числе с разнородным контентом№ - навыками работы с текстом с расширенным форматированием - навыками составления электронных таблиц с организацией вычислений - навыками создания презентаций для демонстрации результатов работы и повышения их наглядности; - навыками получения данных в режиме программного опроса оборудования - навыками определения состава вычислительной	поискового запроса на основе ключевых слов - навыками анализа результатов работы поисковых систем (топ выдачи) - навыками поиска и сопоставления результатов на русском и английском языке, в том числе с разнородным контентом№ - навыками работы с текстом с расширенным форматированием - навыками составления электронных таблиц с организацией вычислений - навыками создания презентаций для демонстрации результатов работы и повышения их наглядности; - навыками получения данных в режиме программного опроса оборудования - навыками определения состава вычислительной системы на основе интегрированного и периферийного оборудования на уровне	поисковых процедур; - технологией формирования поискового запроса на основе ключевых слов - навыками анализа результатов работы поисковых систем (топ выдачи) - навыками поиска и сопоставления результатов на русском и английском языке, в том числе с разнородным контентом№ - навыками работы с текстом с расширенным форматированием - навыками составления электронных таблиц с организацией вычислений - навыками создания презентаций для демонстрации результатов работы и повышения их наглядности; - навыками получения данных в режиме программного опроса оборудования - навыками

прикладные физические задачи ОПК-4.2: Анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях ОПК-4.3: Анализирует процессы, протекающие в линейных и нелинейных электрических цепях 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	компьютеры - навыками локализации неисправностей на различных уровнях - навыками применения актуальных технических и программных средств тестирования с целью локализации исправности системы; - навыками решения основных математических задач; - инструментами сбора и обработки необходимых данных для математической постановки и решения задач; - навыками анализа и интерпретации результатов решения задач; - методами применения стандартных методов; - навыками применения моделей вычислительной математики для решения прикладных задач; - основными методами численного решения задач оптимизации; - методами оценки адекватности полученного численного решения, его сходимости и необходимого	системы на основе интегрированного и периферийного оборудования на уровне визуального анализа - навыками оценки номинального быстродействия ПК; - навыками оценки производительности компьютеры - навыками локализации неисправностей на различных уровнях - навыками применения актуальных технических и программных средств тестирования с целью локализации исправности системы; - навыками решения основных математических задач; - инструментами сбора и обработки необходимых данных для математической постановки и решения задач; - навыками анализа и интерпретации результатов решения задач; - методами применения	визуального анализа - навыками оценки номинального быстродействия ПК; - навыками оценки производительности компьютеры - навыками локализации неисправностей на различных уровнях - навыками применения актуальных технических и программных средств тестирования с целью локализации исправности системы; - навыками решения основных математических задач; - инструментами сбора и обработки необходимых данных для математической постановки и решения задач; - навыками анализа и интерпретации результатов решения задач; - методами применения стандартных методов; - навыками применения моделей вычислительной математики для решения	определения состава вычислительной системы на основе интегрированного и периферийного оборудования на уровне визуального анализа - навыками оценки номинального быстродействия ПК; - навыками оценки производительности компьютеры - навыками локализации неисправностей на различных уровнях - навыками применения актуальных технических и программных средств тестирования с целью локализации исправности системы; - навыками решения основных математических задач; - инструментами сбора и обработки необходимых данных для математической постановки и решения задач;

в области защиты информации, сертификации и аттестации по требованиям безопасности информации ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации 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-8.1: Составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов ОПК-8.2: Систематизирует научную информацию в области информационной	ресурса времени; - навыками и приемами исследования и моделирования прикладных задач методами дискретной математики; - навыками работы с математическими методами и моделями компьютерной математики в рамках своей профессиональной деятельности; - методиками разработки цели и задач проекта, - методами оценки потребности в ресурсах, продолжительности и стоимости проекта; - навыками работы с нормативно-правовой документацией; - навыками решения базовых прикладных задач; - методами экспериментального исследования параметров и характеристик электронных приборов; - методами расчета электрических цепей; - методами моделирования электронных средств в САПР; - средствами САПР для	стандартных методов; - навыками применения моделей вычислительной математики для решения прикладных задач; - основными методами численного решения задач оптимизации; - методами оценки адекватности полученного численного решения, его сходимости и необходимого ресурса времени; - навыками и приемами исследования и моделирования прикладных задач методами дискретной математики; - навыками работы с математическими методами и моделями компьютерной математики в рамках своей профессиональной деятельности; - методиками разработки цели и задач проекта, - методами оценки потребности в ресурсах, продолжительности и	прикладных задач; - основными методами численного решения задач оптимизации; - методами оценки адекватности полученного численного решения, его сходимости и необходимого ресурса времени; - навыками и приемами исследования и моделирования прикладных задач методами дискретной математики; - навыками работы с математическими методами и моделями компьютерной математики в рамках своей профессиональной деятельности; - методиками разработки цели и задач проекта, - методами оценки потребности в ресурсах, продолжительности и стоимости проекта; - навыками работы с нормативно-правовой документацией; - навыками решения базовых прикладных	- навыками анализа и интерпретации результатов решения задач; - методами применения стандартных методов; - навыками применения моделей вычислительной математики для решения прикладных задач; - основными методами численного решения задач оптимизации; - методами оценки адекватности полученного численного решения, его сходимости и необходимого ресурса времени; - навыками и приемами исследования и моделирования прикладных задач методами дискретной математики; - навыками работы с математическими методами и моделями компьютерной математики в рамках своей

безопасности ОПК-8.3: Использует информационно-справочные системы при поиске информации в области профессиональной деятельности 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	моделирования и построения передаточных характеристик и временных диаграмм электронных устройств, расчета электрических цепей; - 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,	стоимости проекта; - навыками работы с нормативно-правовой документацией; - навыками решения базовых прикладных задач; - методами экспериментального исследования параметров и характеристик электронных приборов; - методами расчета электрических цепей; - методами моделирования электронных средств в САПР; - средствами САПР для моделирования и построения передаточных характеристик и временных диаграмм электронных устройств, расчета электрических цепей; - навыками работы с нормативными правовыми актами;	задач; - методами экспериментального исследования параметров и характеристик электронных приборов; - методами расчета электрических цепей; - методами моделирования электронных средств в САПР; - средствами САПР для моделирования и построения передаточных характеристик и временных диаграмм электронных устройств, расчета электрических цепей; - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих	профессиональной деятельности; - методиками разработки цели и задач проекта, - методами оценки потребности в ресурсах, продолжительности и стоимости проекта; - навыками работы с нормативно-правовой документацией; - навыками решения базовых прикладных задач; - методами экспериментального исследования параметров и характеристик электронных приборов; - методами расчета электрических цепей; - методами моделирования электронных средств в САПР; - средствами САПР для моделирования и построения передаточных

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	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 формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа; - навыками создания локальных нормативных	- 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	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; - навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками работы с технической документацией на компоненты	характеристик и временных диаграмм электронных устройств, расчета электрических цепей; - 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

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 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	актов; - навыками организации и контроля пропускного режима; - навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа; - технологией работы с актуальной нормативно-правовой базой - навыками реферирования научно- технической литературы; - навыками систематизации данных в профессиональной предметной области; - навыками ранжирования научных данных с учетом современных требований нормативно-правовой базы; - навыками работы с основными информационно-справочными системами, содержащими документы профессиональной области; - навыками выделения необходимой информации 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 формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа; - навыками создания локальных нормативных актов; - навыками организации и контроля пропускного режима; - навыками разработки	автоматизированных систем на русском и иностранном языках; - навыками разработки модели угроз и модели нарушителя объекта информатизации; - навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа; - навыками создания локальных нормативных актов; - навыками организации и контроля пропускного режима; - навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа; - технологией работы с актуальной нормативно-правовой базой - навыками реферирования научно-	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 формулирования основных требований, предъявляемых к организации защиты информации

ОПК-4.2.1: Настраивает операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации ОПК-4.2.2: Применяет программные средства обеспечения безопасности данных ОПК-4.2.3: Управляет полномочиями пользователей автоматизированной системы 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 ОПК-4.4.1: Применяет инструментальные средства контроля защищенности информации в	учетом параметрических поисковых запросов; - навыками шифрования в режиме ручного расчета; - навыками оценки сходимости методов преобразования; - навыками автоматизации этапов криптографического преобразования; - способами защиты информации от утечки по техническим каналам на объектах информатизации; - навыками применения технических средств защиты информации; - навыками определения каналов утечки; - навыками планирования, контроля; - способами предотвращения угрозам информационной безопасности объекта информатизации; - навыками использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - методами проведения анализа угроз	проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа; - технологией работы с актуальной нормативно-правовой базой - навыками реферирования научно-технической литературы; - навыками систематизации данных в профессиональной предметной области; - навыками ранжирования научных данных с учетом современных требований нормативно-правовой базы; - навыками работы с основными информационно-справочными системами, содержащими документы профессиональной области; - навыками выделения необходимой	технической литературы; - навыками систематизации данных в профессиональной предметной области; - навыками ранжирования научных данных с учетом современных требований нормативно-правовой базы; - навыками работы с основными информационно-справочными системами, содержащими документы профессиональной области; - навыками выделения необходимой информации с учетом параметрических поисковых запросов; - навыками шифрования в режиме ручного расчета; - навыками оценки сходимости методов преобразования; - навыками автоматизации этапов криптографического преобразования; - способами защиты информации от утечки по техническим каналам на объектах	ограниченного доступа; - навыками создания локальных нормативных актов; - навыками организации и контроля пропускного режима; - навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа; - технологией работы с актуальной нормативно-правовой базой - навыками реферирования научно-технической литературы; - навыками систематизации данных в профессиональной предметной области; - навыками ранжирования научных данных с учетом современных требований нормативно-правовой базы; - навыками работы с

автоматизированных системах ОПК-4.4.2: Документирует действия по устранению неисправностей в работе системы защиты информации автоматизированной системы ОПК-4.4.3: Регистрирует события, связанные с защитой информации в автоматизированных системах	информационной безопасности; - навыками применения политик безопасности на объектах информатизации; - навыками управления; - навыками создания локально-нормативных документов; - 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 современных ОС, ВС и СУБД; - навыками использования	информации с учетом параметрических поисковых запросов; - навыками шифрования в режиме ручного расчета; - навыками оценки сходимости методов преобразования; - навыками автоматизации этапов криптографического преобразования; - способами защиты информации от утечки по техническим каналам на объектах информатизации; - навыками применения технических средств защиты информации; - навыками определения каналов утечки; - навыками планирования, контроля; - способами предотвращения угрозам информационной безопасности объекта информатизации; - навыками использования средств защиты информации от утечки по техническим	информатизации; - навыками применения технических средств защиты информации; - навыками определения каналов утечки; - навыками планирования, контроля; - способами предотвращения угрозам информационной безопасности объекта информатизации; - навыками использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - методами проведения анализа угроз информационной безопасности; - навыками применения политик безопасности на объектах информатизации; - навыками управления; - навыками создания локально-нормативных документов; - навыками установки и настройки программно-аппаратных средств	основными информационно-справочными системами, содержащими документы профессиональной области; - навыками выделения необходимой информации с учетом параметрических поисковых запросов; - навыками шифрования в режиме ручного расчета; - навыками оценки сходимости методов преобразования; - навыками автоматизации этапов криптографического преобразования; - способами защиты информации от утечки по техническим каналам на объектах информатизации; - навыками применения технических средств защиты информации; - навыками определения каналов утечки;

	межсетевых экранов и систем обнаружения вторжений; - 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; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих	каналам и контроля эффективности защиты информации; - методами проведения анализа угроз информационной безопасности; - навыками применения политик безопасности на объектах информатизации; - навыками управления; - навыками создания локально-нормативных документов; - 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	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 современных ОС, ВС и СУБД; - навыками использования межсетевых экранов и систем обнаружения вторжений; - навыками определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях; - навыками разработки порядка применения	- навыками планирования, контроля; - способами предотвращения угрозам информационной безопасности объекта информатизации; - навыками использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - методами проведения анализа угроз информационной безопасности; - навыками применения политик безопасности на объектах информатизации; - навыками управления; - навыками создания локально-нормативных документов; - навыками установки и настройки программно-аппаратных средств защиты информации в соответствии с заданными политиками

	защите; - навыками оценки систем и отдельных методов и средств защиты информации; - навыками оценки информационных рисков в автоматизированных системах; - навыками управления информационной безопасности; - навыками подготовки исходных данных для проектирования подсистем; - навыками оценки эффективности проектных решений; - навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений; - навыками определения подлежащих защите информационных ресурсов автоматизированных систем; - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств	нейтрализацией; - навыками анализа и администрирования подсистем защиты современных ОС, ВС и СУБД; - навыками использования межсетевых экранов и систем обнаружения вторжений; - 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	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; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - навыками оценки систем и отдельных методов и средств защиты информации; - навыками оценки информационных рисков в автоматизированных системах;	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 современных ОС, ВС и СУБД; - навыками использования межсетевых экранов и систем обнаружения вторжений; - навыками определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях; - навыками разработки порядка применения программно-

	обеспечения защиты информации в автоматизированной системе; - навыками разработки организационно-распорядительных документов по обеспечения защиты информации в автоматизированной системе; - навыками оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности; - навыками анализа документации, журналов аудита и безопасности автоматизированных систем локальных и распределенных; - навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания; - навыками анализа событий, связанных с защитой информации в	типовых операционных системах, системах управления базами данных, компьютерных сетях; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - навыками оценки систем и отдельных методов и средств защиты информации; - навыками оценки информационных рисков в автоматизированных системах; - навыками управления информационной безопасности; - навыками подготовки исходных данных для проектирования подсистем; - навыками оценки эффективности проектных решений; - навыками разработки основных показателей технико-экономического обоснования соответствующих	- навыками управления информационной безопасности; - навыками подготовки исходных данных для проектирования подсистем; - навыками оценки эффективности проектных решений; - навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений; - навыками определения подлежащих защите информационных ресурсов автоматизированных систем; - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; - навыками разработки организационно-распорядительных	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; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - навыками оценки систем и отдельных методов и средств защиты информации; - навыками оценки информационных рисков в автоматизированных

	автоматизированных системах - навыками составления отчетов по журналам регистрации инцидентов информационной безопасности; - навыками установки антивирусной защиты; - навыками настройки встроенных средств защиты информации программного обеспечения; - навыками проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем; - навыками применения программных средства обеспечения безопасности данных; - навыками фильтрации информации, подлежащей резервному копированию; - навыками применения методик резервного копирования и восстановления;	проектных решений; - навыками определения подлежащих защите информационных ресурсов автоматизированных систем; - 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 оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности; - навыками анализа документации, журналов аудита и безопасности	документов по обеспечения защиты информации в автоматизированной системе; - навыками оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности; - навыками анализа документации, журналов аудита и безопасности автоматизированных систем локальных и распределенных; - навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания; - навыками анализа событий, связанных с защитой информации в автоматизированных системах - навыками составления отчетов по журналам регистрации инцидентов информационной	системах; - навыками управления информационной безопасности; - навыками подготовки исходных данных для проектирования подсистем; - навыками оценки эффективности проектных решений; - навыками разработки основных показателей технико-экономического обоснования соответствующих проектных решений; - навыками определения подлежащих защите информационных ресурсов автоматизированных систем; - навыками разработки комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе;

	- навыками управления полномочиями пользователей автоматизированной системы; - навыками использования инструментальных средств контроля защищенности информации в автоматизированных системах; - навыками анализа документации, журналов аудита и безопасности автоматизированных систем локальных и распределенных; навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания; - навыками анализа событий, связанных с защитой информации в автоматизированных системах, составлять отчеты по журналам регистрации инцидентов информационной безопасности.	автоматизированных систем локальных и распределенных; - навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания; - навыками анализа событий, связанных с защитой информации в автоматизированных системах - навыками составления отчетов по журналам регистрации инцидентов информационной безопасности; - навыками установки антивирусной защиты; - навыками настройки встроенных средств защиты информации программного обеспечения; - навыками проверки работоспособности отдельных программных, программно-аппаратных	безопасности; - навыками установки антивирусной защиты; - навыками настройки встроенных средств защиты информации программного обеспечения; - навыками проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем; - навыками применения программных средства обеспечения безопасности данных; - навыками фильтрации информации, подлежащей резервному копированию; - навыками применения методик резервного копирования и восстановления; - навыками управления полномочиями пользователей автоматизированной системы;	- навыками разработки организационно-распорядительных документов по обеспечения защиты информации в автоматизированной системе; - навыками оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности; - навыками анализа документации, журналов аудита и безопасности автоматизированных систем локальных и распределенных; - навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания; - навыками анализа событий, связанных с защитой информации в

		(в том числе криптографических) и технических средств защиты информации автоматизированных систем; - навыками применения программных средства обеспечения безопасности данных; - навыками фильтрации информации, подлежащей резервному копированию; - навыками применения методик резервного копирования и восстановления; - навыками управления полномочиями пользователей автоматизированной системы; - навыками использования инструментальных средств контроля защищенности информации в автоматизированных системах; - навыками анализа документации, журналов аудита и безопасности	- навыками использования инструментальных средств контроля защищенности информации в автоматизированных системах; - навыками анализа документации, журналов аудита и безопасности автоматизированных систем локальных и распределенных; навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания; - навыками анализа событий, связанных с защитой информации в автоматизированных системах, составлять отчеты по журналам регистрации инцидентов информационной безопасности.	автоматизированных системах - навыками составления отчетов по журналам регистрации инцидентов информационной безопасности; - навыками установки антивирусной защиты; - навыками настройки встроенных средств защиты информации программного обеспечения; - навыками проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем; - навыками применения программных средства обеспечения безопасности данных; - навыками фильтрации информации, подлежащей

		автоматизированных систем локальных и распределенных; навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического обслуживания; - навыками анализа событий, связанных с защитой информации в автоматизированных системах, составлять отчеты по журналам регистрации инцидентов информационной безопасности.		резервному копированию; - навыками применения методик резервного копирования и восстановления; - навыками управления полномочиями пользователей автоматизированной системы; - навыками использования инструментальных средств контроля защищенности информации в автоматизированных системах; - навыками анализа документации, журналов аудита и безопасности автоматизированных систем локальных и распределенных; навыками выявления потенциальных угроз в автоматизированных системах на основе анализа соответствующих журналов безопасности и технического

				обслуживания; - навыками анализа событий, связанных с защитой информации в автоматизированных системах, составлять отчеты по журналам регистрации инцидентов информационной безопасности.

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 (преддипломной) 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	УК-1 ОПК-2
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-2 ОПК-5
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 проведения мониторинга безопасности ТКС. Создание плана работы коллектива из 3 – 4 человек, реализующего политику безопасности в ТКС.	УК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-8 ОПК-9

		Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. Мониторинг состояния информационной безопасности. Самостоятельное проведение анализа результатов проведенного мониторинга информационной безопасности. Представление результатов руководителю практики от организации. Организация работы 2-3 человек и руководство их работой в процессе работ по обеспечению информационной безопасности. 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 повышению уровня информационной безопасности предприятия. Самостоятельное составление краткосрочного плана работ по обеспечению безопасности организации, эксплуатирующей ТКС. Организация работы 2-3 человек и руководство их работой в процессе составления краткосрочного и долгосрочного прогнозов. Представление своего прогноза с обоснованием руководителю практики от организации. Представление результатов руководителю практики от организации.	ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-4.4 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10
Отчетный этап	Выработка по итогам прохождения практики	Формулирование основных выводов Написание текста отчета	УК-1 ОПК-2

	выводов и предложений, оформление отчета по практике и его защита	Оформление отчета по практике и представление на проверку руководителю Подготовка к защите отчета по практике	

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 (преддипломной)

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 (ПРЕДДИПЛОМНАЯ)

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.				
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 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	350049, Краснодарский край, г. Краснодар, Центральный административный округ, ул. им. Котовского, д 76/2, к.11, 30 кв.м, №22	практическая подготовка	Общество с ограниченной ответственностью «Поставщик коммерческой информации»	Договор о практической подготовке 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 (преддипломной) 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 (преддипломную) 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 (ПРЕДДИПЛОМНУЮ) 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:	УК-1 ОПК-2	
Содержательный этап:	УК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-8 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-4.4 ПК-1 ПК-2	

	ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10	
Выполнение индивидуального задания:	УК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-8 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-4.4 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10	
Отчетный этап: Составление отчета по учебной практике Заполнение дневника практики	УК-1 ОПК-2	

**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	УК-1 ОПК-2		

	средой разработки			
2	Содержательный этап,	УК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-8 ОПК-9 ОПК-10 ОПК-12 ОПК-4.1 ОПК-4.2 ОПК-4.3 ОПК-4.4 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10		
4	Отчетный этап Составление отчета по практике	УК-1 ОПК-2		

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 (ПРЕДДИПЛОМНОЙ)

_____

(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 производственной 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.

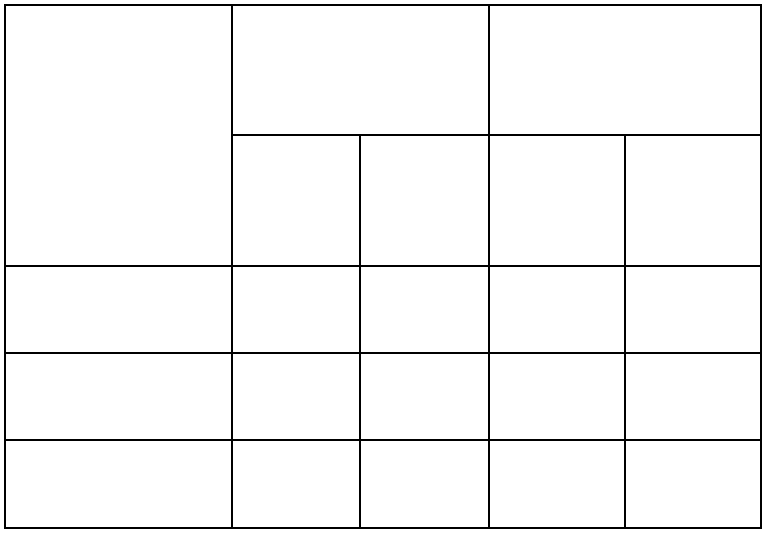
Таблицу с большим количеством строк допускается переносить на другую страницу. При переносе части таблицы на другую страницу слово "Таблица", ее номер и наименование указывают один раз слева над первой частью таблицы, а над другими частями также слева пишут слова "Продолжение таблицы" и указывают номер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