ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНО
приказом ректора
от «08» мая 2020 г. № 266-1

Б2.В.04 (Пд) ПРАКТИКА
производственная – преддипломная

рабочая программа практики

Направление подготовки – 10.03.01 Информационная безопасность
Профиль – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника – бакалавр
Форма обучения – очная
Нормативный срок обучения – 4 года
Способ проведения практики – стационарная
Форма проведения практики – дискретная
Кафедра разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 9
Продолжительность в неделях – 4
Часов по учебному плану – 324

Форма промежуточной аттестации в семестре:
зачет с оценкой 8

ИРКУТСК

Рабочая программа практики разработана в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденным Приказом Министерства образования и науки Российской Федерации от 01.12.2016 г. № 1515, и на основании учебного плана по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)», утвержденного Учёным советом ИрГУПС от 30.12.2016 г. протокол № 6.

Программу составил: к.т.н., доцент Е.А. Головкова

Рабочая программа практики обсуждена и рекомендована к применению в образовательном процессе для обучения обучающихся по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры «Информационные системы и защита информации».
Протокол от «29» апреля 2020 г. № 11

Зав. кафедрой, д.т.н., доцент Л.В. Аршинский

1 ЦЕЛИ И ЗАДАЧИ ПРОВЕДЕНИЯ ПРАКТИКИ	
1.1 Цели проведения практики	
1	закрепление полученных в вузе теоретических и практических знаний; подбор материалов, проведение испытания и тестирования систем и технологий информационной безопасности, разработанных в соответствии с заданием на выпускную квалификационную работу; закрепление профессиональных умений и навыков управления информационной безопасностью предприятия.
2	решение реальной задачи по информационной безопасности.
1.2 Задачи проведения практики	
1	закрепление и углубление теоретической и практической подготовки обучающегося в области информационной безопасности.
2	сбор материалов в соответствии с заданием на выпускную квалификационную работу.
3	оформление, полученных результатов в виде отчета.
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологии профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	
Научно-образовательное воспитание обучающихся	
Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества. Цель достигается по мере решения в единстве следующих задач: – формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности; – создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками; – популяризация научных знаний среди обучающихся; – содействие повышению привлекательности науки, поддержка научно-технического творчества; – создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества; – совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности	

2 МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Для успешного прохождения преддипломной практики необходимы знания, умения и навыки, приобретенные в результате освоения дисциплин базовой и вариативной частей учебного плана по направлению подготовки 10.03.01 Информационная безопасность, а также предшествующих практик.
2.2 Дисциплины и практики, для которых прохождение данной практики необходимо как предшествующее	
1	Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы

безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
Минимальный уровень освоения компетенции	
Знать	понятие, основные виды и классификацию информационных ресурсов (активов) организации;
Уметь	выделять из общих информационных ресурсов предприятия, информацию подлежащую защите;
Владеть	навыками отнесения информации к категории защищаемой.
Базовый уровень освоения компетенции	
Знать	модели угроз информационной безопасности и модели нарушителей;
Уметь	строить частные модели угроз информационной безопасности предприятия;
Владеть	методиками построения частной модели угроз информационной безопасности предприятия.
Высокий уровень освоения компетенции	
Знать	методики оценки рисков реализации угроз при функционировании объекта защиты;
Уметь	применять на практике методики оценки рисков реализации угроз при функционировании объекта защиты;
Владеть	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
Минимальный уровень освоения компетенции	
Знать	принципы обеспечения информационной безопасности с помощью штатных и встроенных программно-аппаратных и технических средств защиты информации;
Уметь	устанавливать добавочные программно-аппаратные средства защиты информации (ПАСЗИ);
Владеть	навыками установки ПАСЗИ.
Базовый уровень освоения компетенции	
Знать	защитные механизмы ПАСЗИ;
Уметь	настраивать добавочные ПАСЗИ;
Владеть	навыками установки и настройки программно-аппаратных и технических средств защиты информации.
Высокий уровень освоения компетенции	
Знать	средства администрирования добавочных ПАСЗИ;
Уметь	отлаживать и тестировать программно-аппаратных и технических средства защиты информации;
Владеть	навыками установки, настройки и методами, инструментами тестирования программно-аппаратных и технических средств защиты информации.

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Минимальный уровень освоения компетенции	
Знать	программные средства системного, прикладного и специального назначения в области информационной безопасности;
Уметь	применять программные средства системного, прикладного и специального назначения для обеспечения информационной безопасности (ИБ) объекта защиты;
Владеть	навыками решения профессиональных задач с помощью программных средств.
Базовый уровень освоения компетенции	
Знать	инструментальные средства для обеспечения информационной безопасности объекта защиты;
Уметь	применять инструментальные средства для обеспечения ИБ;
Владеть	навыками решения профессиональных задач с помощью инструментальных средств.
Высокий уровень освоения компетенции	
Знать	языки и системы программирования для решения профессиональных задач в области информационной безопасности;
Уметь	разрабатывать программные средства обеспечения ИБ объекта защиты;
Владеть	хотя бы одним языком программирования.

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты	
Минимальный уровень освоения компетенции	
Знать	разновидности и основные функциональные особенности подсистем ИБ;
Уметь	осуществлять конфигурирование средств защиты информации; управлять учетными записями

	пользователей; осуществлять резервное копирование;
Владеть	навыками установки и настройки подсистем ИБ.
Базовый уровень освоения компетенции	
Знать	основные задачи администрирования подсистемы ИБ объекта защита; инструменты администрирования;
Уметь	администрировать подсистемы информационной безопасности объекта защиты;
Владеть	методами и инструментами администрирования подсистем ИБ.
Высокий уровень освоения компетенции	
Знать	виды многослойной защиты информации;
Уметь	организовывать многослойную защиту информации;
Владеть	моделями, методами и инструментами многослойной защиты информации.

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Минимальный уровень освоения компетенции	
Знать	терминологию, основные руководящие и регламентирующие документы в области информационной безопасности;
Уметь	проводить анализ угроз безопасности информационных систем;
Владеть	профессиональной терминологией в области ИБ.
Базовый уровень освоения компетенции	
Знать	основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ;
Уметь	реализовывать политику ИБ, применять нормативно-правовые акты и нормативно-правовые документы в области ИБ;
Владеть	навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации.
Высокий уровень освоения компетенции	
Знать	организацию работы и нормативно-правовые акты и стандарты в области технической защиты конфиденциальной информации по аттестации объектов информатизации;
Уметь	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;
Владеть	навыками работы с нормативно-правовыми актами.

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
Минимальный уровень освоения компетенции	
Знать	положение по аттестации объектов информатизации по требованиям безопасности информации;
Уметь	осуществлять предварительное ознакомление с аттестуемым объектом;
Владеть	основными понятиями в области аттестации объектов информатизации и знанием требований безопасности информации.
Базовый уровень освоения компетенции	
Знать	порядок проведения аттестации и контроля объекта информатизации по требованиямбезопасности информации;
Уметь	проводить аттестационные испытания объектов информатизации;
Владеть	навыками проведения аттестационных испытаний объектов информатизации по требованиям безопасности.
Высокий уровень освоения компетенции	
Знать	требования к нормативным и методическим документам по аттестации объектов информатизации;
Уметь	разрабатывать методику проведения аттестации объекта информатизации, учитывая требования нормативных и методических документов по аттестации объектов информатизации;
Владеть	навыками анализа результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждения заключения по результатам аттестации.

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
Минимальный уровень освоения компетенции	
Знать	основные программные, программно-аппаратные и технические средства защиты информации; основные метрологические показатели средств защиты информации;
Уметь	организовывать и проводить контрольные проверки работоспособности средств защиты информации (СЗИ);

Владеть	методами и инструментами проверки работоспособности СЗИ.
Базовый уровень освоения компетенции	
Знать	основные качественные показатели СЗИ; методы и инструменты проверки эффективности СЗИ;
Уметь	организовывать и проводить проверку эффективности СЗИ;
Владеть	методами и инструментами оценки эффективности СЗИ.
Высокий уровень освоения компетенции	
Знать	основы стандартизации, сертификации и технического документирования в области информационных технологии и информационной безопасности;
Уметь	разрабатывать план и комплекс мероприятий для организации и проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
Владеть	знаниями в области нормативно-правового и методологического обеспечения ИБ; стандартизации и сертификации.

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
Минимальный уровень освоения компетенции	
Знать	источники, методы и инструменты поиска, обработки информации;
Уметь	осуществлятьпоиск и обработку информации по предложенной теме исследования или разработке;
Владеть	методами и технологиями поиска,анализа и обработки информации.
Базовый уровень освоения компетенции	
Знать	ресурсы, содержащие достоверную научно-техническую литературу, действующие нормативные и методических материалы;
Уметь	составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
Владеть	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов.
Высокий уровень освоения компетенции	
Знать	существующие стандарты и методики оформления, согласования и подписи документов;
Уметь	планировать мероприятия по обеспечению информационной безопасности;
Владеть	навыками выделения и формулировки основных целей и задач, которые необходимо включить в план мероприятий по обеспечению информационной безопасности.

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	
Минимальный уровень освоения компетенции	
Знать	законодательную базу, нормативно-методические документы и российские стандарты в области ИБ;
Уметь	анализировать направления развития информационных технологий в области ИБ;
Владеть	навыками анализа нормативно-методических документов и российских стандартов в области ИБ;
Базовый уровень освоения компетенции	
Знать	средства и системы обеспечения ИБ объектов информатизации в соответствии с российскими стандартами;
Уметь	анализировать эффективность функционирования систем в области ИБ;
Владеть	навыками применения расчетов эффективности функционирования систем в области ИБ.
Высокий уровень освоения компетенции	
Знать	методы анализа информационной безопасности объектов и систем обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;
Уметь	анализировать и оценивать риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ;
Владеть	навыками анализа и оценки риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ.

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
Минимальный уровень освоения компетенции	
Знать	методику формирования комплекса мер по обеспечению информационной безопасности;

Уметь	применять методику формирования комплекса мер по обеспечению информационной безопасности;
Владеть	навыками формирования комплекса мер по обеспечению информационной безопасности.
Базовый уровень освоения компетенции	
Знать	методику формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности;
Уметь	пользоваться методикой формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности;
Владеть	навыками формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности.
Высокий уровень освоения компетенции	
Знать	методику управления процессом выполнения комплекса мер по обеспечению информационной безопасности;
Уметь	внедрять методику управления процессом выполнения комплекса мер по обеспечению информационной безопасности на предприятии;
Владеть	навыками управления процессом выполнения комплекса мер по обеспечению информационной безопасности на предприятии.

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
Минимальный уровень освоения компетенции	
Знать	основные средства и способы обеспечения информационной безопасности;
Уметь	определять комплекс мер и мероприятий для обеспечения информационной безопасности автоматизированных систем (АС);
Владеть	профессиональной терминологией в области управления ИБ.
Базовый уровень освоения компетенции	
Знать	основные методы управления информационной безопасностью;
Уметь	разрабатывать предложения по совершенствованию системы управления ИБ АС;
Владеть	методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации.
Высокий уровень освоения компетенции	
Знать	основные положения стандартов единой системы конструкторской и программной документации (ФСТЭК России, ФСБ России);
Уметь	методы аттестации уровней защищенности АС;
Владеть	методиками модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.

ПСК4-1: способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	
Минимальный уровень освоения компетенции	
Знать	классы защищенности автоматизированной системы управления;
Уметь	разрабатывать и внедрять систему защиты автоматизированной системы;
Владеть	навыками и методами защиты информации при разработке и внедрении автоматизированной системы.
Базовый уровень освоения компетенции	
Знать	состав мер защиты информации и их базовые наборы для соответствующего класса защищенности автоматизированной системы;
Уметь	обеспечивать защиту информации в ходе эксплуатации автоматизированной системы управления;
Владеть	навыками и методами защиты информации в ходе эксплуатации автоматизированной системы управления.
Высокий уровень освоения компетенции	
Знать	особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации;
Уметь	обеспечивать защиту информации при выводе из эксплуатации автоматизированной системы управления;
Владеть	навыками и методами защиты информации при выводе из эксплуатации автоматизированной

	системы управления.

ПСК4-2: способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	
Минимальный уровень освоения компетенции	
Знать	комплекс задач администрирования подсистем информационной безопасности систем управления базами данных (СУБД);
Уметь	устанавливать и конфигурировать новое аппаратное и программное обеспечения;
Владеть	навыками администрирования подсистем информационной безопасности СУБД.
Базовый уровень освоения компетенции	
Знать	комплекс задач администрирования подсистем информационной безопасности операционной системы (ОС);
Уметь	устанавливать и конфигурировать необходимые обновления для ОС и используемых программ, в том числе СУБД;
Владеть	навыками администрирования подсистем информационной безопасности ОС.
Высокий уровень освоения компетенции	
Знать	комплекс задач администрирования компьютерных сетей;
Уметь	выполнять комплекс задач администрирования компьютерных сетей;
Владеть	навыками администрирования компьютерных сетей.

ПСК4-3: способностью планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	
Минимальный уровень освоения компетенции	
Знать	основные составляющие информационных систем, режимы их работы;
Уметь	рассчитывать показатели надежности и безотказности информационных систем в различных условиях их эксплуатации;
Владеть	методами анализа надежности и безотказности информационных систем.
Базовый уровень освоения компетенции	
Знать	показатели надежности и безотказности аппаратных и программных составляющих информационных систем, методики их расчета;
Уметь	организовывать и проводить мероприятия по зашита информации в автоматизированных системах с соблюдением требований нормативных и методических федеральных документов;
Владеть	методами, организации и управлении мероприятиями по обеспечению информационной безопасности, корректной оценки внешних воздействий и вероятных угроз.
Высокий уровень освоения компетенции	
Знать	основные мероприятия по обеспечению информационной безопасности и защиты информационных систем от последствий воздействия на них внешних сильнодействующих агрессивных факторов;
Уметь	восстанавливать утерянную или искаженную информацию, планировать и организовывать мероприятия по защите информации, связанных с обеспечением надежности функционирования автоматизированных систем;
Владеть	методами восстановления аппаратной и программной части информационных систем и потерянной, в связи с этим – восстановлением информации.

ПСК4-4: способностью участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	
Минимальный уровень освоения компетенции	
Знать	классы объектов защиты; основные составляющие системы защиты;
Уметь	определять особенности информационной системы как объекта защиты;
Владеть	навыками работы с нормативно-правовыми актами и нормативно-методическими документами в сфере защиты информации.
Базовый уровень освоения компетенции	
Знать	системы, комплексы и средства обеспечения информационной безопасности (ИБ);
Уметь	разрабатывать современные программные и аппаратно-технические комплексы и модернизировать известные средства защиты информации (проектировать комплексную систему защиты информации и информационных систем);
Владеть	методами и средствами проектирования систем обеспечения информационной безопасности и защиты информационных систем (ИС).
Высокий уровень освоения компетенции	

Знать	современные технологии и методы проектирования систем обеспечения информационной безопасности;
Уметь	учитывать весь комплекс особенностей объектов защиты, составлять техническое задание, внедрять и применять систему защиты информации;
Владеть	приемами сочетания средств защиты, комплексами управления информационной безопасностью.

В результате прохождения практики обучающийся должен

Знать	
1	тему выпускной квалификационной работы в окончательном виде по профилю направления «Безопасность информационных систем и технологий»;
2	действующее российское и международное законодательство по вопросам обеспечения информационной безопасности и защите персональных данных;
3	требования государственных регулирующих органов по технической защите персональных данных, в том числе о лицензировании деятельности по технической защите конфиденциальной информации, сертификации средств защиты информации и аттестации объектов информатизации;
4	основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
5	правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
6	организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
7	структуру комплексной системы защиты персональных данных;
8	методы и средства защиты персональных данных, обрабатываемых в информационных системах;
9	меры ответственности за нарушение установленных требований по защите персональных данных;
10	основные методы управления информационной безопасностью;
11	методы аттестации уровня защищенности информационных систем.
Уметь	
1	обосновать целесообразность разработки темы;
2	подобрать необходимые источники по теме (литературу, отчеты, техническую документацию и др.) и провести их анализ;
3	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
4	анализировать состав защищаемых персональных данных;
5	проводить классификацию информационных систем обработки персональных данных;
6	использовать методы оценки уязвимости защищаемых персональных данных, построения модели угроз;
7	применять методы и способы защиты информации в информационных системах персональных данных;
8	оформлять нормативную документацию с учетом применения технологии защищенного документооборота при обработке персональных данных с использованием средств автоматизации и без использования таковых;
9	определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем;
10	разрабатывать частные политики информационной безопасности информационных систем;
11	контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;
12	разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем;
13	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
14	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.
Владеть	
1	методами обработки имеющихся данных и анализа достоверности полученных результатов для

	подготовки собранного материала к оформлению выпускной квалификационной работы;
2	основами комплексной защиты персональных данных;
3	специальной профессиональной терминологией;
4	навыками анализа информационной инфраструктуры информационной системы и ее безопасности;
5	методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем;
6	методами управления информационной безопасностью информационных систем;
7	методами оценки информационных рисков;
8	навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем;
9	навыками участия в экспертизе состояния защищенности информации на объекте защиты;
10	навыками работы с нормативными правовыми актами;
11	навыками организации и обеспечения режима секретности;
12	методами организации и управления деятельностью служб защиты информации на предприятии;
13	методами формирования требований по защите информации.

4 СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

4.1 РАБОЧИЙ ГРАФИК (ПЛАН) ПРОХОЖДЕНИЯ ПРАКТИКИ

№	Период	Выполняемое мероприятие	Место выполнения мероприятия
1	За месяц до начала практики	Получение индивидуального задания, выполняемого в период практики	ФГБОУ ВО ИрГУПС, кафедра «Информационные системы и защита информации»
2	За неделю до начала практики	Прохождение инструктажа по охране труда и технике безопасности	ФГБОУ ВО ИрГУПС, кафедра «Информационные системы и защита информации»
3	Первый день практики	Ознакомление с приказом о приеме на практику и назначение руководителя практики от профильной организации	Профильная организация – место прохождения практики
		Согласование с руководителем практики от профильной организации рабочего графика (плана) прохождения практики, индивидуального задания, выполняемого в период практики, содержание практики и планируемых результатов практики	
		Прохождение медицинского осмотра и оформление на работу	
		Прохождение инструктажа по охране труда, технике безопасности, пожарной безопасности на рабочем месте и ознакомление с правилами трудового внутреннего распорядка профильной организации	
4	Период практики	Выполнение индивидуального задания	Профильная организация – место прохождения практики
5	За три дня до окончания практики	Написание отчета по практике	Профильная организация – место прохождения практики
6	Последний день практики	Получение отзыва от руководителя практики от профильной организации	Профильная организация – место прохождения практики
		Отправление через ЭИОС университета отчетных документов и получение оценки результатов прохождения практики и выполнения индивидуального	ФГБОУ ВО ИрГУПС, кафедра «Информационные

		задания от руководителя практики университета	системы и защита информации»

4.2 ТИПОВОЕ ЗАДАНИЕ, ВЫПОЛНЯЕМОЕ ОБУЧАЮЩИМСЯ В ПЕРИОД ПРОХОЖДЕНИЯ ПРАКТИКИ					
Код компетенции	Содержание компетенции	Выполняемая работа	Объем в час.	Учебная литература, ресурсы сети «Интернет»	Форма отчетности
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Анализ предметной области, изучение объекта информатизации, описание информационных активов и бизнес-процессов объекта. Построение модели угроз и нарушителей. Описание уязвимостей рассматриваемого объекта или ресурса.	18	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Изучение существующих средств обеспечения ИБ. Установка и настройка выбранных средств обеспечения ИБ.	18	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Применение программных средств системного, прикладного и специального назначения, а также инструментальных средств для решения задач, сформулированных в индивидуальном задании практики.	36	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	Администрирование выбранной в ходе практики системы обеспечения ИБ.	8	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Изучение базовых политик информационной безопасности. Выбор, разработка или доработка и конкретизация политик безопасности рассматриваемого объекта защиты.	22	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет

ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Участие в процессе аттестации объекта информатизации, если это определено заданием практики.	8	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Участие в контрольных проверках работоспособности и эффективности применяемых средств защиты информации.	8	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-9	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Подбор, изучение и анализ литературных источников, технической и нормативно-правовой документации.	18	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Анализ ИБ исследуемого объекта на соответствие требованиями государственных и международных стандартов в области ИБ.	18	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Подбор и реализация организационных, программных и технических мер по обеспечению ИБ для конкретного объекта или ресурса.	54	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Осуществление, обеспечение защиты конфиденциальной информации или информации ограниченного доступа.	36	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет

ПСК4-1	способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	Анализ и аудит информационных технологий организации.	18	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Э.1 – Э.8, 6.4.1	Отчет
ПСК4-2	способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Администрирование подсистем информационной безопасности.	8	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет
ПСК4-3	способностью планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	Оценка эффективности, надежности и отказоустойчивости средств обработки информации, а также обеспечение надежности функционирования и отказоустойчивости средств обработки информации.	18	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Э.1 – Э.8, 6.4.1	Отчет
ПСК4-4	способностью участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Разработка программных средств обеспечения ИБ объекта с учетом существующих угроз и уязвимостей.	36	Л1.1 – 1.5, Л2.1 – Л2.5, Л3.1, Л4.1, Л4.2, Э.1 – Э.8, 6.4.1	Отчет

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

Фонд оценочных средств разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

Фонд оценочных средств оформляется в виде приложения № 1 к рабочей программе практики и размещаются в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет.

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л1.1	Лапина М.А., Ревин А.Г., Лапин В.И.;.Килясхан	Информационное право : учебное пособие [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=118624	М. :Юнити-Дана, 2015	100 % онлайн

	ова И.Ш.			
Л1.2	Загинайлов Ю.Н.	Теория информационной безопасности и методология защиты информации : учебное пособие [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=276557	М. ; Берлин : Директ-Медиа, 2015	100 % онлайн
Л1.3	Кузнецов И.Н.	Бизнес-безопасность [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=453908	М. : Издательско-торговая корпорация «Дашков и К», 2016	100 % онлайн
Л1.4	Краковский Ю.М.	Информационная безопасность и защита информации: учебное пособие	М: ИрГУПС, 2016	93
Л1.5	Прохорова О.В.	Информационная безопасность и защита информации : учебник. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=438331	Самара : СГАСУ, 2014.	100 % онлайн
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Минин И.В., Минин О.В.	Защита конфиденциальной информации при электронном документообороте : учебное пособие [Электронный ресурс] biblioclub.ru/index.php?page=book&id=228779	Новосибирск : НГТУ, 2011	100 % онлайн
Л2.2	Нестеров С.А.	Основы информационной безопасности: Учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=363040	СПб. : Политехнический университет, 2014	100 % онлайн
Л2.3	Афанасьев А.А., Веденьев Л.Т., Воронцов А.А., Газизова Э.Р.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие [Электронный ресурс] http://e.lanbook.com/book/5114	М. : Горячая линия-Телеком, 2012	100 % онлайн
Л2.4	Малюк А.А., Горбатов В.С., Королев В.И.	Введение в информационную безопасность : учебное пособие. [Электронный ресурс] http://e.lanbook.com/books/element.php? pl1_id=5171	Горячая линия-Телеком, 2012.	100 % онлайн
Л2.5	Мэйволд Э.	Безопасность сетей : учебное пособие. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=429035	М : ИНТУИТ, 2016.	100 % онлайн
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия: учебное пособие.	- Иркутск: ИрГУПС, 2013	67
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный	Кол-во экз. в библиотеке/ 100% онлайн

			кабинет обучающегося	
Л4.1	Глухов Н.И., Середкин С.П.	Транспортная безопасность: учебно-методическое пособие для самостоятельной работы студентов	Иркутск: ИрГУПС, 2014	88
Л4.2	Темникова Е.А.	Методические рекомендации по выполнению задания по преддипломной практике.	Личный кабинет обучающегося	100% онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»	
Э.1	Линия защиты «Сюртель» www.suritel.ru
Э.2	Федеральная служба по техническому и экспортному контролю, www.fstec.ru
Э.3	Код безопасности. Средства защиты информации http://www.securitycode.ru
Э.4	Методики и технологии управления информационными рисками http://citforum.ru/security/articles/risk/
Э.5	Искусство управления информационной безопасностью http://www.iso27000.ru
Э.6	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru
Э.7	Рекомендации по организации и проведению производственной практики обучающихся по программам высшего и среднего профессионального образования в образовательных организациях Федерального агентства железнодорожного транспорта (Приложение к приказу Росжелдора от 10.06.2015 № 243). http://web-edu.iriit/sites/files/20150902104946.pdf
Э.8	Положение об организации в ОАО «РЖД» практики студентов образовательных организаций, реализующих программы среднего профессионального и высшего образования (Утверждено распоряжением ОАО «РЖД» от 31.03.2015 г. № 813р). http://web-edu.iriit/sites/files/20150428143150.pdf
Э.9	Памятка для студентов по охране труда при прохождении практики https://www.irgups.ru/web-edu/sites/files/20150401155322.rtf
6.3 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем	
6.3.1 Перечень базового программного обеспечения	
6.3.1.1	ОС Microsoft Windows XP Professional, количество – 227, лицензия № 44718499; ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083; Libre Office v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org
6.3.2 Перечень специализированного программного обеспечения	
6.3.2.1	Firefox (браузер), (лицензия: бесплатно, количество: не ограничено).
6.3.2.2	MaxPatrol (демонстрационная версия), (лицензия: бесплатно, количество: не ограничено).
6.3.2.3	Packet Tracer (лицензия: бесплатно, количество: не ограничено).
6.3.2.4	PEM (лицензия: бесплатно, количество: не ограничено).
6.3.2.5	Wireshark(лицензия: бесплатно, количество: не ограничено).
6.3.3 Перечень информационных справочных систем	
6.3.3.1	Информационно-справочная система Консультант Плюс http://www.consultant.ru
6.4 Правовые и нормативные документы	
6.4.1	Положение об организации и проведении практики обучающихся по программам высшего образования (бакалавриат, магистратура и специалитет) № П.311200.05.7.075-2017
6.4.2	Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2017.

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	Учебная лаборатория «Сетевые технологии», Д-508, Оснащение: локальная вычислительная сеть, Веб-сервер, DHCP-сервер, FTP-сервер.
3	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и организован доступ в электронную информационно-образовательную среду ИрГУПС.
4	Учебная лаборатория «Средства и методы защиты информации», Д-525.
5	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС.

	Помещения для самостоятельной работы обучающихся: читальные залы; учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.
6	Помещение для хранения и профилактического обслуживания учебного оборудования – А-521.
7	Профильные организации, оснащенные сертифицированными средствами защиты информации в соответствии с: государственным реестром сертифицированных средств защиты информации; выпиской из перечня средств защиты информации, сертифицированных ФСБ России.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Порядок прохождения практики обучающимися в профильной организации:

В первый день прохождения практики обучающийся обязан явиться в отдел управления персоналом профильной организации к началу рабочего дня.

Обучающиеся по договорам о целевом обучении получают направление на медкомиссию от предприятия, с которым заключен договор. Обучающиеся за счёт средств субсидий на выполнение государственного задания или за счёт средств физического или юридического лица представляют справку о состоянии здоровья, полученную по месту прикрепления медицинского полиса обязательного медицинского страхования.

При поступлении на практику обучающийся проходит инструктажи по охране труда, технике безопасности, пожарной безопасности, а также знакомится с правилами внутреннего трудового распорядка.

В студенческой аттестационной книжке производственного обучения руководителем практикиот профильной организации ставится отметка о согласовании индивидуального задания и рабочего графика (плана) прохождения практики.

Обучающиеся выполняют индивидуальные задания, предусмотренные программами практики и пишут отчёт о практике.

В последний день практики обучающийся сдаёт руководителю практики от кафедры оригиналы или отправляет посредством ЭИОС (через личный кабинет студента) электронные копии следующих документов: заполненной путёвки, индивидуального задания, согласованного с руководителем практики от профильной организации, аттестационного листа и отзыва руководителя практики от профильной организации о прохождении практики обучающегося, отчёта обучающегося о прохождении практики.

После прохождения практики все оригиналы вышеперечисленных документов обучающиеся должны сдать руководителю практики от кафедры.

На основании представленных документов о прохождении практики обучающимся производится промежуточная аттестация обучающегося и выставляется дифференцированный зачет.

Инструкция по оформлению отчета по практике дана в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2017.

Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой практики, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Приложение 1 к рабочей программе по дисциплине Б2.В.04(Пд) «Производственная - преддипломная»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по практике

Б2.В.04(Пд) «Производственная - преддипломная»

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры «Информационные системы и защита информации» с участием основных работодателей 29.04.2020 г., протокол № 11.

СОДЕРЖАНИЕ

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Практика производственная - преддипломная участвует в формировании компетенции:
ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;
ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты;
ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;
ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ПСК4-1: способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации;
ПСК4-2: способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей;
ПСК.4-3: способностью планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации;
ПСК.4-4: способностью участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности.

1.1 Таблица траекторий формирования у обучающихся компетенций ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-9; ПК-10; ПК-13; ПК-15; ПСК.4-1; ПСК.4-2; ПСК.4-3; ПСК.4-4 при освоении образовательной программы

Код	Наименование	Индекс и наименование дисциплин,	Семестр	Этапы

компе-тенции	компетенции	практик, участвующих в формировании компетенции	изучения дисциплины	формирования компетенции
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Б1.Б.11 Основы информационной безопасности	2	1
		Б1.В.02 Теоретические основы компьютерной безопасности	3	2
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	3
		Б1.В.ДВ.07.02 Методология определения ценности информации	6	4
		Б1.В.ДВ.08.01 Методология анализа информационных рисков	6	4
		Б1.В.ДВ.08.02 Инстументарий анализа информационных рисков	6	4
		Б2.В.03(П) Производственная практика - эксплуатационная	6	4
		Б2.В.04(Пд) Производственная практика - преддипломная	8	5
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	5
ПК–1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Б1.Б.12 Аппаратные средства вычислительной техники	1	1
		Б1.Б.13 Программно-аппаратные средства защиты информации	7	5
		Б1.Б.14 Криптографические методы защиты информации	6	4
		Б1.Б.16 Техническая защита информации	5	3
		Б1.Б.17 Сети и системы передачи информации	4	2
		Б1.Б.23 Электроника и схемотехника	4	2
		Б1.В.04 Безопасность операционных систем	5	3
		Б2.В.03(П) Производственная практика - эксплуатационная	6	4
		Б2.В.04 (Пд) Производственная практика - преддипломная	8	6
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	6
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения	Б1.Б.19 Языки программирования	2	1
		Б2.В.01(У) Учебная практика - ознакомительная	2	1
		Б1.В.ДВ.03.01 Основы программирования	3	2
		Б1.В.ДВ.05.01 Системы управления базами данных	3	2
		Б1.В.ДВ.10.01 Теория языков программирования	3	2
		Б1.В.ДВ.10.02 Теория компиляции	3	2
		Б1.Б.20 Технологии и методы программирования	5	3
		Б1.В.ДВ.05.02 Средства сетевых систем	5	3

	профессиональных задач	управления базами данных		
		Б1.В.ДВ.09.01 Языковые средства доступа к информации в системах баз данных	5	3
		Б1.В.ДВ.09.02 Администрирование систем баз данных	5	3
		Б1.Б.35 Основы системного анализа	6	4
		Б2.В.03(П) Производственная практика - эксплуатационная	6	4
		Б1.В.ДВ.02.01 Защита и обработка конфиденциальных документов	7	5
		Б1.В.ДВ.02.02 Защита электронного документооборота	7	5
		Б1.В.06 Безопасность систем баз данных	8	6
		Б2.В.04(Пд) Производственная практика - преддипломная	8	6
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	6
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	Б1.В.03 Безопасность вычислительных сетей	7	1
		Б1.В.06 Безопасность систем баз данных	8	2
		Б1.В.ДВ.06.02 Сетевое администрирование	8	2
		Б2.В.03(П) Производственная - эксплуатационная	6	3
		Б2.В.04(Пд) Производственная - преддипломная	8	2
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	2
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Б1.Б.15 Организационное и правовое обеспечение информационной безопасности	4	1
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	1
		Б2.В.03(П) Производственная практика - эксплуатационная	6	2
		Б1.В.08 Методология построения защищенных автоматизированных систем	8	3
		Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем	8	3
		Б1.В.05 Комплексная защита в информационных системах персональных данных	8	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	3

		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3
ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Б1.Б.33 Метрология, стандартизация и сертификация	4	1
		Б2.В.03(П) Производственная - эксплуатационная	6	2
		Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта	7	3
		Б1.В.08 Методология построения защищенных автоматизированных систем	8	4
		Б2.В.04(Пд) Производственная - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	4
ПК–6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Б1.Б.12 Аппаратные средства вычислительной техники	1	1
		Б1.Б.13 Программно-аппаратные средства защиты информации	7	4
		Б1.Б.16 Техническая защита информации	5	2
		Б2.В.03(П) Производственная практика - эксплуатационная	6	3
		Б2.В.04 (Пд) Производственная практика - преддипломная	8	5
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	5
ПК-9	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Б2.В.02(У) Учебная - по получению первичных профессиональных умений и навыков	4	1
		Б2.В.04 (Пд) Производственная практика - преддипломная	8	2
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	2
ПК-10	способность проводить анализ информационной безопасности объектов и систем на	Б1.В.02 Теоретические основы компьютерной безопасности	3	1
		Б1.В.07 Аудит информационной безопасности	6	2
		Б1.В.01 Комплексное обеспечение	8	3

	соответствие требованиям стандартов в области информационной безопасности	информационной безопасности автоматизированных систем		
		Б2.В.04(Пд) Производственная практика - преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Б1.В.ДВ.07.02 Методология определения ценности информации	6	1
		Б1.Б.21 Основы управления информационной безопасностью	78	2
		Б1.В.08 Методология построения защищенных автоматизированных систем	8	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Б1.Б.15 Организационное и правовое обеспечение информационной безопасности	4	1
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	1
		Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта	7	2
		Б1.В.ДВ.02.01 Защита и обработка конфиденциальных документов	7	2
		Б1.В.ДВ.02.02 Защита электронного документооборота	7	2
		Б1.Б.21 Основы управления информационной безопасностью	78	2
		Б1.В.05 Комплексная защита в информационных системах персональных данных	8	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3
ПСК4-1	способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в	Б1.Б.25 Информационные технологии	2	1
		Б1.В.ДВ.03.02 Корпоративные информационные системы	3	2
		Б2.В.03(П) Производственная практика - эксплуатационная	6	3
		Б1.В.ДВ.06.01 Информационная безопасность открытых систем	8	4
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая	8	4

	них информации	подготовку к процедуре защиты и процедуру защиты		
ПСК4-2	способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Б1.Б.17 Сети и системы передачи информации	4	1
		Б1.В.04 Безопасность операционных систем	5	2
		Б1.В.ДВ.05.01 Системы управления базами данных	5	2
		Б1.В.ДВ.05.02 Средства сетевых систем управления базами данных	5	2
		Б1.В.ДВ.09.02 Администрирование систем баз данных	5	2
		Б1.В.03 Безопасность вычислительных сетей	7	3
		Б1.В.06 Безопасность систем баз данных	8	4
		Б1.В.ДВ.06.01 Информационная безопасность открытых систем	8	4
		Б1.В.ДВ.06.02 Сетевое администрирование	8	4
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	4
ПСК4-3	способностью планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	Б1.В.ДВ.04.01 Катастрофоустойчивость и надежность информационных систем	6	1
		Б2.В.04(Пд) Производственная – преддипломная	8	2
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	2
ПСК4-4	способностью участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Б1.Б.19 Языки программирования	2	1
		Б1.В.ДВ.10.01 Теория языков программирования	3	2
		Б1.В.ДВ.10.02 Теория компиляции	3	2
		Б1.Б.20 Технологии и методы программирования	5	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и	8	4

		процедуру защиты		

1.2 Таблица соответствия уровней освоения компетенций ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-9; ПК-10; ПК-13; ПК-15; ПСК.4-1; ПСК.4-2; ПСК.4-3; ПСК.4-4 планируемым результатам обучения

Код компетенции	Наименование компетенции	Выполняемая работа	Уровни освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Анализ предметной области, изучение объекта информатизации, описание информационных активов и бизнес-процессов объекта. Построение модели угроз и нарушителей. Описание уязвимостей рассматриваемого объекта или ресурса.	Минимальный уровень	**Знать:** понятие, основные виды и классификацию информационных ресурсов (активов) организации; **Уметь:** выделять из общих информационных ресурсов предприятия, информацию подлежащую защите; **Владеть:** навыками отнесения информации к категории защищаемой;
			Базовый уровень	**Знать:** модели угроз информационной безопасности и модели нарушителей; **Уметь:** строить частные модели угроз информационной безопасности предприятия; **Владеть:** методиками построения частной модели угроз информационной безопасности предприятия;
			Высокий уровень	**Знать:** методики оценки рисков реализации угроз при функционировании объекта защиты; **Уметь:** применять на практике методики оценки рисков реализации угроз при функционировании объекта защиты; **Владеть:** способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

ПК–1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Изучение существующих средств обеспечения ИБ. Установка и настройка выбранных средств обеспечения ИБ.	Минимальный уровень	**Знать:** принципы обеспечения информационной безопасности с помощью штатных и встроенных программно-аппаратных и технических средств защиты информации; **Уметь:** устанавливать добавочные программно-аппаратные средства защиты информации (ПАСЗИ); **Владеть:** навыками установки ПАСЗИ.
			Базовый уровень	**Знать:** защитные механизмы ПАСЗИ; **Уметь:** настраивать добавочные ПАСЗИ; **Владеть:** навыками установки и настройки программно-аппаратных и технических средств защиты информации.
			Высокий уровень	**Знать:** средства администрирования добавочных ПАСЗИ; **Уметь:** отлаживать и тестировать программно-аппаратных и технических средства защиты информации; **Владеть:** навыками установки, настройки и методами, инструментами тестирования программно-аппаратных и технических средств защиты информации.
ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Применение программных средств системного, прикладного и специального назначения, а также инструментальных средств для решения задач, сформулированных в индивидуальном задании практики.	Минимальный уровень	**Знать:** программные средства системного, прикладного и специального назначения в области информационной безопасности; **Уметь:** применять программные средства системного, прикладного и специального назначения для обеспечения ИБ объекта защиты; **Владеть:** навыками решения профессиональных задач с помощью программных средств.
			Базовый уровень	**Знать:** инструментальные средства для обеспечения информационной безопасности объекта защиты; **Уметь:** применять инструментальные средства для обеспечения ИБ; **Владеть:** навыками решения профессиональных задач с

				помощью инструментальных средств.
			Высокий уровень	**Знать:** языки и системы программирования для решения профессиональных задач в области информационной безопасности; **Уметь:** разрабатывать программные средства обеспечения ИБ объекта защиты; **Владеть:** хотя бы одним языком программирования.
ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	Администрирование выбранной в ходе практики системы обеспечения ИБ.	Минимальный уровень	**Знать:** разновидности и основные функциональные особенности подсистем ИБ; **Уметь:** осуществлять конфигурирование средств защиты информации; управлять учетными записями пользователей; осуществлять резервное копирование; **Владеть:** навыками установки и настройки подсистем ИБ.
			Базовый уровень	**Знать:** основные задачи администрирования подсистемы ИБ объекта защита; инструменты администрирования; **Уметь:** администрировать подсистемы информационной безопасности объекта защиты; **Владеть:** методами и инструментами администрирования подсистем ИБ.
			Высокий уровень	**Знать:** виды многослойной защиты информации; **Уметь:** организовывать многослойную защиту информации; **Владеть:** моделями, методами и инструментами многослойной защиты информации.
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный	Изучение базовых политик информационной безопасности. Выбор, разработка или доработка и конкретизация политик	Минимальный уровень	**Знать:** терминологию, основные руководящие и регламентирующие документы в области информационной безопасности; **Уметь:** проводить анализ угроз безопасности информационных систем; **Владеть:** профессиональной

	подход к обеспечению информационной безопасности объекта защиты	безопасности рассматриваемого объекта защиты.		терминологией в области ИБ.
			Базовый уровень	**Знать:** основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ; **Уметь:** реализовывать политику ИБ, применять нормативно-правовые акты и нормативно-правовые документы в области ИБ; **Владеть:** навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации.
			Высокий уровень	**Знать:** организацию работы и нормативно-правовые акты и стандарты в области технической защиты конфиденциальной информации по аттестации объектов информатизации; **Уметь:** разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; **Владеть:** навыками работы с нормативно-правовыми актами.
ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Участие в процессе аттестации объекта информатизации, если это определено заданием практики.	Минимальный уровень	**Знать:** положение по аттестации объектов информатизации по требованиям безопасности информации; **Уметь:** осуществлять предварительное ознакомление с аттестуемым объектом; **Владеть:** основными понятиями в области аттестации объектов информатизации и знанием требований безопасности информации.
			Базовый уровень	**Знать:** порядок проведения аттестации и контроля объекта информатизации по требованиям безопасности информации; **Уметь:** проводить аттестационные испытания объектов информатизации; **Владеть:** навыками проведения

				аттестационных испытаний объектов информатизации по требованиям безопасности.
			Высокий уровень	**Знать:** требования к нормативным и методическим документам по аттестации объектов информатизации; **Уметь:** разрабатывать методику проведения аттестации объекта информатизации, учитывая требования нормативных и методических документов по аттестации объектов информатизации; **Владеть:** навыками анализа результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждения заключения по результатам аттестации.
ПК–6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Участие в контрольных проверках работоспособности и эффективности применяемых средств защиты информации.	Минимальный уровень	**Знать:** основные программные, программно-аппаратные и технические средства защиты информации; основные метрологические показатели средств защиты информации; **Уметь:** организовывать и проводить контрольные проверки работоспособности средств защиты информации (СЗИ); **Владеть:** методами и инструментами проверки работоспособности СЗИ.
			Базовый уровень	**Знать:** основные качественные показатели СЗИ; методы и инструменты проверки эффективности СЗИ; **Уметь:** организовывать и проводить проверку эффективности СЗИ; **Владеть:** методами и инструментами оценки эффективности СЗИ.
			Высокий уровень	**Знать:** основы стандартизации, сертификации и технического документирования в области информационных технологии и информационной безопасности; **Уметь:** разрабатывать план и комплекс мероприятий для организации и проведения контрольных проверок работоспособности и эффективности применяемых

				программных, программно-аппаратных и технических средств защиты информации; **Владеть:** знаниями в области нормативно-правового и методологического обеспечения ИБ; стандартизации и сертификации.
ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Подбор, изучение и анализ литературных источников, технической и нормативно-правовой документации.	Минимальный уровень	**Знать:** источники, методы и инструменты поиска, обработки информации; **Уметь:** осуществлять поиск и обработку информации по предложенной теме исследования или разработке; **Владеть:** методами и технологиями поиска, анализа и обработки информации.
			Базовый уровень	**Знать:** ресурсы, содержащие достоверную научно-техническую литературу, действующие нормативные и методических материалы; **Уметь:** составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; **Владеть:** способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов.
			Высокий уровень	**Знать:** существующие стандарты и методики оформления, согласования и подписи документов; **Уметь:** планировать мероприятия по обеспечению информационной безопасности; **Владеть:** навыками выделения и формулировки основных целей и задач, которые необходимо включить в план мероприятий по обеспечению информационной безопасности.
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям	Анализ ИБ исследуемого объекта на соответствие требованиями государственных и международных стандартов в области ИБ.	Минимальный уровень	**Знать:** законодательную базу, нормативно-методические документы и российские стандарты в области ИБ; **Уметь:** анализировать направления развития информационных технологий в области ИБ; **Владеть:** навыками анализа

	стандартов в области информационной безопасности	Анализ ИБ исследуемого объекта на соответствие требованиями государственных и международных стандартов в области ИБ.		нормативно-методических документов и российских стандартов в области ИБ;
			Базовый уровень	**Знать:** средства и системы обеспечения ИБ объектов информатизации в соответствии с российскими стандартами; **Уметь:** анализировать эффективность функционирования ИТ в области ИБ; **Владеть:** навыками применения расчетов эффективности функционирования ИТ в области ИБ.
			Высокий уровень	**Знать:** методы анализа информационной безопасности объектов и систем обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; **Уметь:** анализировать и оценивать риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ; **Владеть:** навыками анализа и оценки риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ.
ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Подбор и реализация организационных, программных и технических мер по обеспечению ИБ для конкретного объекта или ресурса.	Минимальный уровень	**Знать:** методику формирования комплекса мер по обеспечению информационной безопасности; **Уметь:** применять методику формирования комплекса мер по обеспечению информационной безопасности; **Владеть:** навыками формирования комплекса мер по обеспечению информационной безопасности.
			Базовый уровень	**Знать:** методику формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности; **Уметь:** пользоваться методикой формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности;

				Владеть: навыками формирования и организации поддержки выполнения комплекса мер по обеспечению информационной безопасности.
			Высокий уровень	**Знать:** методику управления процессом выполнения комплекса мер по обеспечению информационной безопасности; **Уметь:** внедрять методику управления процессом выполнения комплекса мер по обеспечению информационной безопасности на предприятии; **Владеть:** навыками управления процессом выполнения комплекса мер по обеспечению информационной безопасности на предприятии.
ПК-15	Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Осуществление, обеспечение защиты конфиденциальной информации или информации ограниченного доступа.	Минимальный уровень	**Знать:** основные средства и способы обеспечения информационной безопасности; **Уметь:** определять комплекс мер и мероприятий для обеспечения информационной безопасности автоматизированных систем (АС); **Владеть:** профессиональной терминологией в области управления ИБ.
			Базовый уровень	**Знать:** основные методы управления информационной безопасностью; **Уметь:** разрабатывать предложения по совершенствованию системы управления ИБ АС; **Владеть:** методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации.
			Высокий уровень	**Знать:** основные положения стандартов единой системы конструкторской и программной документации (ФСТЭК России, ФСБ России); **Уметь:** организовывать технологический процесс защиты информации; **Владеть:** методиками модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными

				методическими документами ФСБ России, ФСТЭК России.
ПСК4-1	Способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	Анализ и аудит информационных технологий организации.	Минимальный уровень	**Знать:** классы защищенности автоматизированной системы управления; **Уметь:** разрабатывать и внедрять систему защиты автоматизированной системы; **Владеть:** навыками и методами защиты информации при разработке и внедрении автоматизированной системы.
			Базовый уровень	**Знать:** состав мер защиты информации и их базовые наборы для соответствующего класса защищенности автоматизированной системы; **Уметь:** обеспечивать защиту информации в ходе эксплуатации автоматизированной системы управления; **Владеть:** навыками и методами защиты информации в ходе эксплуатации автоматизированной системы управления.
			Высокий уровень	**Знать:** особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации; **Уметь:** обеспечивать защиту информации при выводе из эксплуатации автоматизированной системы управления; **Владеть:** навыками и методами защиты информации при выводе из эксплуатации автоматизированной системы управления.
ПСК4-2	Способностью выполнять комплекс задач администрирования подсистем информационной	Администрирование подсистем информационной безопасности.	Минимальный уровень	**Знать:** комплекс задач администрирования подсистем информационной безопасности СУБД; **Уметь:** устанавливать и конфигурировать новое

	безопасности операционных систем, систем управления базами данных, компьютерных сетей			аппаратное и программное обеспечения; **Владеть:** навыками администрирования подсистем информационной безопасности СУБД.
			Базовый уровень	**Знать:** комплекс задач администрирования подсистем информационной безопасности ОС; **Уметь:** устанавливать и конфигурировать необходимые обновления для операционной системы (ОС) и используемых программ, в том числе СУБД; **Владеть:** навыками администрирования подсистем информационной безопасности ОС.
			Высокий уровень	**Знать:** комплекс задач администрирования компьютерных сетей; **Уметь:** выполнять комплекс задач администрирования компьютерных сетей; **Владеть:** навыками администрирования компьютерных сетей.
ПСК4-3	Способностью планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	Оценка эффективности, надежности и отказоустойчивости средств обработки информации, а также обеспечение надежности функционирования и отказоустойчивости средств обработки информации.	Минимальный уровень	**Знать:** основные составляющие информационных систем, режимы их работы; **Уметь:** рассчитывать показатели надежности и безотказности информационных систем в различных условиях их эксплуатации; **Владеть:** методами анализа надежности и безотказности информационных систем.
			Базовый уровень	**Знать:** показатели надежности и безотказности аппаратных и программных составляющих информационных систем, методики их расчета; **Уметь:** организовывать и проводить мероприятия по зашита информации в автоматизированных системах с соблюдением требований нормативных и методических федеральных документов; **Владеть:** методами , организации и управлении мероприятиями по обеспечению информационной безопасности, корректной оценки внешних

				воздействий и вероятных угроз.
			Высокий уровень	**Знать:** основные мероприятия по обеспечению информационной безопасности и защиты информационных систем от последствий воздействия на них внешних сильнодействующих агрессивных факторов; **Уметь:** восстанавливать утерянную или искаженную информацию, планировать и организовывать мероприятия по защите информации, связанных с обеспечением надежности функционирования автоматизированных систем; **Владеть:** методами восстановления аппаратной и программной части информационных систем и потерянной, в связи с этим – восстановлением информации.
ПСК4-4	Способностью участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Разработка программных средств обеспечения ИБ объекта с учетом существующих угроз и уязвимостей.	Минимальный уровень	**Знать:** классы объектов защиты; основные составляющие системы защиты; **Уметь:** определять особенности информационной системы как объекта защиты; **Владеть:** навыками работы с нормативно-правовыми актами и нормативно-методическими документами в сфере защиты информации.
			Базовый уровень	**Знать:** системы, комплексы и средства обеспечения информационной безопасности (ИБ); **Уметь:** разрабатывать современные программные и аппаратно-технические комплексы и модернизировать известные средства защиты информации (проектировать комплексную систему защиты информации и информационных систем); **Владеть:** методами и средствами проектирования систем обеспечения информационной безопасности

				и защиты информационных систем (ИС).
			Высокий уровень	**Знать:** современные технологии и методы проектирования систем обеспечения информационной безопасности; **Уметь:** учитывать весь комплекс особенностей объектов защиты, составлять техническое задание, внедрять и применять систему защиты информации; **Владеть:** приемами сочетания средств защиты, комплексами управления информационной безопасностью.

1.3 Программа контрольно-оценочных мероприятий за период изучения дисциплины

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

№	Неделя	Наименование оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
1	2	3	4	5	6
1		Текущий контроль	Противопожарный инструктаж и инструктаж по технике безопасности	ПК-9	Собеседование (устно)
2	1-2	Текущий контроль	Ознакомление с организационно-управленческой структурой предприятия. Изучение бизнес-процессов и информационной системы предприятия. Ознакомление с применяемыми на предприятии подходами, методиками и средствами защиты информации. Изучение локальных нормативных актов по организации защиты информации на предприятии.	ОПК-7, ПК-5, ПК-6, ПК-9, ПСК4-1, ПСК4-3	Отчет по практике (письменно)
3	3	Текущий контроль	Анализ существующих угроз информационной безопасности и уязвимостей информационной системы предприятия. Построение модели угроз, модели уязвимостей, а также модели нарушителей информационной безопасности предприятия. Изучение политик	ОПК-7, ПК-4, ПК-5, ПК-10, ПСК4-1, ПСК4-3	Отчет по практике (письменно)

			безопасности, если таковые есть, их усовершенствование, а если таковые отсутствуют, то и разработка.		
4	4	Текущий контроль	Оценка рисков информационной безопасности предприятия. Разработка или усовершенствование механизмов защиты информационных активов предприятия. Оценка возврата инвестиций на информационную безопасность.	ПК-1, ПК-2, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-3	Отчет по практике (письменно)
	5-6	Текущий контроль	Организация технологического процесса защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Выполнение работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	ПК-1, ПК-2, ПК-3, ПК-13, ПК-15, ПСК4-1, ПСК4-2, ПСК4-3, ПСК4-4	Отчет по практике (письменно)
5	6	Промежуточная аттестация – зачет с оценкой	Защита отчета по производственной – преддипломной практике.	ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2, ПСК4-3, ПСК4-4	Доклад (устно), собеседование (устно)

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

Контроль качества прохождения практики включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице.

№	Наименование	Краткая характеристика оценочного средства	Представление

	оценочного средства		оценочного средства в ФОС
1	Собеседование	Средство контроля прохождения практики, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с выполнением задания на практику, и рассчитанное на выяснение объема знаний обучающегося по определенной теме. Может быть использовано для оценки знаний обучающихся.	Комплект теоретических вопросов
2	Отчет по практике	Средство, позволяющее оценить способность обучающегося решать задачи, приближенные к профессиональной деятельности. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Отчет по практике
3	Дифференцированный зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов к зачету

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета с оценкой, а также шкала для оценивания уровня освоения компетенций

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенций
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный

«неудовлетворительно»	«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

Оценка по зачету (ЗО) с оценкой рассчитывается по формуле

$$ЗО = \frac{O_1 + O_2 + O_3}{3},$$

где O_1, O_2 - оценки соответственно за вопросы, O_3 - оценка за защиту отчета по производственной практике.

При получении не целого числа учитывается оценка по практике руководителя практики от профильного предприятия. Если *ЗО* не является целым, то применяются правила округления до целого. Например, если $O_1 = 4$, $O_2 = 5$, $O_3 = 5$, тогда $ЗО = 4{,}67$. Учитывая, что оценка по практике руководителя практики от предприятия равна 5, получаем $ЗО = 5$.

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседования с обучающимся

Оценка	Критерий оценки
«зачтено»	Обучающийся полностью и правильно ответил на предложенные вопросы. Показал отличные знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Даны верные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого вопроса
	Обучающийся полностью и правильно ответил на предложенные вопросы с небольшими неточностями. Показал хорошие знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. В рамках рассматриваемой темы ни на все дополнительные вопросы даны верные ответы.
«незачтено»	При ответах обучающийся продемонстрировал недостаточный уровень знаний, умений и владения ими при решении задач в рамках усвоенного учебного материала

После оценивания обучающиеся расписываются о проведенных инструктажах в «Журнале регистрации первичного, повторного, внепланового противопожарного инструктажа (для студентов)» и «Журнале инструктажа на рабочем месте по охране труда (для студентов)».

Руководитель в индивидуальном порядке проводит устное собеседование с обучающимся, объясняет порядок прохождения производственной практики, правила заполнения журнала «Студенческая аттестационная книжка производственного обучения», формирование разделов индивидуального задания в отчет и сроки представления отчета о выполнении индивидуального задания при прохождении производственной практики.

Отчет по практике

Шкала оценивания	Критерии оценивания
«отлично»	Обучающийся: – своевременно, качественно выполнил весь объем работы, требуемый программой практики; – показал глубокую теоретическую, методическую, профессионально-прикладную подготовку; – умело применил полученные знания во время прохождения практики; – ответственно и с интересом относился к своей работе.

	Отчет: – выполнен в полном объеме и в соответствии с предъявляемыми требованиями; – результативность практики представлена в количественной и качественной обработке, продуктах деятельности; – материал изложен грамотно, доказательно; – свободно используются понятия, термины, формулировки; – выполненные задания соотносятся с формированием компетенций.
«хорошо»	Обучающийся: – демонстрирует достаточно полные знания всех профессионально-прикладных и методических вопросов в объеме программы практики; – полностью выполнил программу, с незначительными отклонениями от качественных параметров; – проявил себя как ответственный исполнитель, заинтересованный в будущей профессиональной деятельности. Отчет: – представлен почти в полном объеме и в соответствии с предъявляемыми требованиями; – грамотно используется профессиональная терминология – четко и полно излагается материал, но не всегда последовательно; – описывается анализ выполненных заданий, но не всегда четко соотносится выполнение профессиональной деятельности с формированием определенной компетенции.
«удовлетворительно»	Обучающийся: – выполнил программу практики, однако часть заданий вызвала затруднения; – не проявил глубоких знаний теории и умения применять ее на практике, допускал ошибки в планировании и решении задач; – в процессе работы не проявил достаточной самостоятельности, инициативы и заинтересованности. Отчет: – низкий уровень владения профессиональным стилем речи в изложении материала; – низкий уровень оформления документации по практике; – носит описательный характер, без элементов анализа; – низкое качество выполнения заданий, направленных на формирование компетенций.
«неудовлетворительно»	Обучающийся: – владеет фрагментарными знаниями и не умеет применить их на практике, не способен самостоятельно продемонстрировать наличие знаний при решении поставленной задачи; – не выполнил программу практики в полном объеме. Отчет: – документы по практике не оформлены в соответствии с требованиями; – описание и анализ видов профессиональной деятельности, выполненных заданий отсутствует или носит фрагментарный характер.

3 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

3.1 Перечень теоретических вопросов к собеседованию

Противопожарный инструктаж и инструктаж по технике безопасности

1. Основные понятия по технике безопасности на рабочих местах.
2. Требования по технике безопасности и охране труда на предприятии.
3. Требования по технике безопасности и охране труда при работе на рабочем

месте.

4. Требования по технике безопасности и охране труда при работе на вычислительной технике.
5. Требования по технике безопасности и охране труда при работе с приборами и системами.
6. Требования по технике безопасности при работе с легковоспламеняющимися жидкостями.
7. Требования безопасности в аварийных ситуациях.
8. Требования безопасности по окончании работы.
9. Основные правила выполнения противопожарной безопасности на рабочих местах.
10. Схемы эвакуации.
11. Инструкции по противопожарной безопасности.
12. Необходимые таблички и указатели.
13. Перечень документации по противопожарной безопасности.
14. Оборудование с повышенной огнеопасностью.
15. Обеспечение безопасности людей при пожаре.
16. Основная документация по пожарной безопасности.
17. Основные требования пожарной безопасности при работе с легковоспламеняющимися и горючими жидкостями.
18. Основные требования пожарной безопасности при работе с химическими веществами.
19. Основные требования пожарной безопасности при работе с горючими газами.
20. Запрещенные действия при работе с приборами и системами.

3.2 Перечень письменных вопросов в отчете по практике по разделам

1. Информационные активы предприятия. Основные угрозы и уязвимости активов предприятия.
2. Основные нормативно-правовые документы в области информационной безопасности, которыми должны руководствоваться специалисты по ИБ на предприятии.
3. Современные подходы и механизмы обеспечения информационной безопасности предприятия.
4. Планирование мероприятий по защите информации на предприятии. Установка, настройка, управление средствами обеспечения ИБ.
5. Оценка рисков информационной безопасности. Управление рисками.
6. Анализ возврата инвестиций от внедрения контрмер.

3.3 Перечень теоретических вопросов к зачету с оценкой

1. Цели и задачи обеспечения информационной безопасности России.
2. Определение понятий «безопасность информации» и «защита информации».
3. Право человека на доступ к информации.
4. Принципы отнесения сведений к гос. тайне и их засекречивание.
5. Правовой институт рассекречивания сведений, отнесенных к гос. тайне.
6. Институт служебной тайны – основа защиты конфиденциальных сведений в органах государственной власти и органах местного самоуправления.
7. Санкции за неправомерное распространение сведений, составляющих служебную тайну.
8. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации (Закон «Об информации информационных технологиях и защите информации»)

9. Информация как объект правовых отношений,(Закон «Об информации информационных технологиях и защите информации»)
10. Право на доступ к информации (Закон «Об информации информационных технологиях и защите информации»).
11. Ограничение доступа к информации (Закон «Об информации информационных технологиях и защите информации»).
12. Защита информации (Закон «Об информации информационных технологиях и защите информации»).
13. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
14. Краткая характеристика основных этапов развития системы защиты коммерческой тайны в России и за рубежом.
15. Уровень нормативного регулирования отношений в области коммерческой тайны в России в период возрождения рыночной экономики.
16. Действительная и потенциальная коммерческая ценность.
17. Необходимые условия в коммерческой организации для сохранности сведений, составляющих коммерческую тайну.
18. Законодательство Российской Федерации о коммерческой тайне, (Закон «О коммерческой тайне»)
19. Что такое режим коммерческой тайны, (Закон «О коммерческой тайне»)
20. Права обладателя информации, составляющей коммерческую тайну
21. Охрана конфиденциальности информации в рамках трудовых отношений
22. Конфиденциальность персональных данных.
23. Условия обработки персональных данных.
24. Ответственность за неправомерное распространение персональных данных.
25. Применение гражданско-правового института к обязательствам работников, связанным с неправомерным распространением сведений.
26. Организационные источники и каналы утечки.
27. Силы, средства и условия организационной защиты информации.
28. Особенности системы организационной защиты информации.
29. Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий.
30. Подбор персонала на должности, связанные с работой с конфиденциальной информацией.
31. Допуск к секретной информации.
32. Организация доступа к конфиденциальной информации.
33. Текущая работа с персоналом, обладающим конфиденциальной информацией.
34. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
35. Основные функции службы безопасности предприятия.
36. Состав и типовая структура службы безопасности.
37. Организация охраны территории, зданий, помещений и персонала.
38. Организация пропускного и внутриобъектового режимов.
39. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.
40. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.
41. Аналитическая работа как основа управления системой организационной защиты информации.
42. Методики аналитической работы, обеспечивающие управляемость

системы организационной защиты информации.

43. Планирование процессов организационной защиты информации.

44. Оценка и анализ состояния системы ОЗИ как основа планирования

45. Контроль функционирования системы организационной защиты информации.

46. Сущность контроля как функции управления.

47. Основы обеспечения безопасности человека. Общие положения безопасности человека

48. Контроль функционирования системы организационной защиты информации.

49. Факторы, влияющие на безопасность предпринимательской деятельности в России, и состояние ее защиты

50. Безопасность внутриофисной работы — противодействие мошенничеству, хищениям и утечке информации

51. Кражи, совершаемые персоналом

52. Анализ рисков нарушений политики информационной безопасности

53. Мероприятия по обеспечению политики информационной безопасности

54. Изучение конкурентов по рынку аналогичных товаров и услуг

55. Концепция информационной безопасности предприятия

56. Угрозы информационной безопасности (основные определения и критерии классификации угроз). Средства защиты.

57. Сценарии реализации угроз информационной безопасности (разглашение конфиденциальной информации и обход средств защиты от разглашения конфиденциальной информации; кража конфиденциальной информации; нарушение авторских прав на информацию; нецелевое использование ресурсов).

58. Вредоносная программа. Классификация вредоносных программ (вирусы; черви; троянские программы; спам; другие вредоносные программы). Способы распространения вредоносных программ.

59. Основы борьбы с вредоносными программами. Диагностика заражения вредоносными программами. Антивирусное программное обеспечение. Комплексные средства антивирусной защиты.

60. Уязвимости ОИС. Причины уязвимости ИС. Классификация уязвимостей.

61. Уязвимости архитектуры клиент-сервер (конфигурация системы, уязвимость операционных систем, уязвимость серверов, уязвимость рабочих станций, уязвимость каналов связи).

62. Уязвимость системных утилит, команд и сетевых сервисов. Уязвимость современных технологий программирования. Ошибки в программном обеспечении.

63. Модель угроз ИБ. Модель нарушителей ИБ. Инсайдеры и аутсайдеры.

64. Атаки на открытые системы. Удаленные атаки на открытые системы. Классификация удаленных атак.

65. Анализ сетевого трафика. Подмена доверенного объекта или субъекта системы. Внедрение ложного объекта в систему.

66. Типичные сценарии и уровни атак. Удаленный контроль над станцией в сети.

67. Классические методы взлома (взлом парольной защиты). Современные методы взлома: перехват данных при их перемещении по каналам связи и перехват ввода с клавиатуры; мониторинг в графических интерфейсах; подмена системных утилит; нападения с использованием сетевых протоколов.

68. Обеспечение информационной безопасности в открытых системах. Комплексный и фрагментарный подходы к защите ИС. Четырехуровневая модель открытой системы.

69. Эшелонированная защита ОИС в целом и отдельных ее элементов.

топология сети: физическая изоляция; изоляция протокола; выделенные каналы.

70. Организационно-правовые методы защиты открытых систем.

71. Политика информационной безопасности. Разновидности политик ИБ. Основные положения политики ИБ.

72. Информационная безопасность в глобальных сетях. Удаленные атаки и механизмы их реализации в глобальных сетях.

73. Криптографическая защита информации. Понятия о симметричных криптосистемах (шифры перестановки; шифры сложной замены; одноразовая система шифрования; шифрование методом гаммирования; DES).

74. Криптографическая защита информации. Понятия об асимметричных криптосистемах (однонаправленные функции; криптосистема шифрования данных RSA; электронная цифровая подпись).

75. Криптографическая защита информации. Аппаратно-программные криптографические средства защиты информации.

76. Межсетевые экраны (firewall): прикладного уровня; с пакетной фильтрацией; гибридные межсетевые экраны.

77. Организация и эксплуатация виртуальных частных сетей (VPN).

78. Иерархическая модель доверия. Сетевая модель доверия.

79. Управление ключами и сертификация ключей.

80. Протокол конфиденциального обмена данными SSL. Протокол WEP. Протокол 802.1X - контроль доступа в сеть по портам.

81. Стандарты и спецификации в области информационной безопасности.

82. Какой подход к оценке рисков используется в вашей организации?

83. Какие категории информационных рисков охватывает используемый вами подход?

84. Какие сотрудники вашей организации участвуют в процессах управления рисками и как распределяются между ними роли?

85. Кто и на основании какой информации принимает решения по обработке рисков?

86. К какой категории специалистов, с точки зрения отношения к оценке

87. рисков, вы сами относитесь?

88. Какие информационные риски представляют наибольшую опасность для вашей организации?

89. Какие процессы включает в себя система управления рисками и как эти процессы связаны с другими процессами системы управления (СУИР) ИБ?

90. Какие виды активов важнее для бизнеса вашей организации и почему?

91. Какие информационные риски вы рассматриваете в качестве основных?

92. В каких случаях область действия СУИР может охватывать не всю организацию?

93. Каковы отличительные признаки системного подхода к управлению рисками?

94. Какие виды нормативных и рабочих документов требуются для управления рисками в организации?

95. Каким образом могут распределяться обязанности и ответственность за управление рисками в организации?

96. Какие факторы влияют на решение о принятии риска?

97. На основании каких данных определяется вероятность угрозы?

98. Назовите основные источники уязвимостей.

99. Перечислите основные и вспомогательные бизнес-процессы ФГБОУ ВО ИрГУПС.

100. Какие этапы включает в себя оценка риска?

101. Какие параметры могут использоваться для описания бизнес-процессов

организации?

102. Какие категории требований безопасности необходимо учитывать при оценке рисков?

103. Как можно определить ценность тех или иных активов?

104. Как связаны между собой оценка рисков и планирование непрерывности бизнеса?

105. Раскройте сущность комплексной системы защиты информационных активов предприятий.

106. Опишите особенности система защиты информационных активов хозяйствующего субъекта.

107. Исследуйте особенности организационного направления в деятельности по защите информационных активов предприятия.

108. Охарактеризуйте сущность направления в организационной защите – работе с персоналом, определении его надежности.

109. Как осуществить оценку надежности персонала, как основного источника угроз информационным активам предприятия?

110. Суть методики оценки возможного ущерба при реализации угроз безопасности?

111. Охарактеризуйте сущность направления в организационной защите - информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.

112. Обоснуйте позицию защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.

113. Проведите сравнительный анализ нескольких наиболее известных методик оценки информационных рисков.

114. Изложите суть экспертных методов по определению ценности защищаемых информационных активов.

115. Изложите суть методики оценки затрат на обеспечение информационной защищенности хозяйствующего субъекта.

116. Изложите суть эффективности оценки информационных рисков.

117. Современные программно-аппаратные средства обеспечения ИБ.

118. Современные технические средства обеспечения ИБ.

119. Организационные меры по защите информации.

3.4 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2, ПСК4-3, ПСК4-4	Получение индивидуального задания, выполняемого в период прохождения практики	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-7, ПК-1, ПК-2, ПК-3,	Прохождение инструктажа по охране труда и технике безопасности	Знание	3 – ОТЗ 3 – ЗТЗ

ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2	Ознакомление с приказом о назначении руководителя практики от профильной организации	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2	Согласование с руководителем практики от профильной организации рабочего графика (плана) прохождения практики, индивидуального задания, выполняемого в период практики, содержание практики и планируемых результатов практики	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-7, ПК-1, ПК-2, ПК-3,	Прохождение медицинского осмотра и оформление на работу (по необходимости)	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-7, ПК-1, ПК-2, ПК-3,	Прохождение инструктажа по охране труда, технике безопасности, пожарной безопасности на рабочем месте и ознакомление с правилами трудового внутреннего распорядка профильной организации	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2, ПСК4-3, ПСК4-4	Выполнение индивидуального задания	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2, ПСК4-3, ПСК4-4	Получение отзыва от руководителя практики от профильной организации	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2, ПСК4-3, ПСК4-4	Написание отчета по практике	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	2 – ОТЗ 2 – ЗТЗ
ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2,	Отправка отчетных документов по практике через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося)	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	0– ОТЗ 0 – ЗТЗ
		Действие	2– ОТЗ

ПСК4-3, ПСК4-4			2 – ЗТЗ
ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-13, ПК-15, ПСК4-1, ПСК4-2, ПСК4-3, ПСК4-4	Оценивание руководителем практики от ИрГУПС выполнения индивидуального задания и результатов прохождения практики	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
		Итого	60 – ОТЗ 60 – ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

Образец типового варианта итогового теста,
предусмотренного рабочей программой практики

1. В чем заключается основная цель производственной - организационно-управленческой практики?

a) Повышение прибыльности компании.
b) Отдых от учебы.
c) Получение опыта работы в организации.
d) Отсутствие цели и задач.

Правильный ответ: c) Получение опыта работы в организации.

2. Какой из перечисленных процессов относится к организационной части управления?

a) Проектирование продукции.
b) Управление человеческими ресурсами.
c) Складское хозяйство.
d) Обслуживание оборудования.

Правильный ответ: b) Управление человеческими ресурсами.

3. Какие основные этапы включает в себя процесс производственного планирования?

a) Определение целей, сбор данных, анализ, разработка плана, контроль и коррекция.
b) Работа с технической документацией.
c) Управление производственным процессом.
d) Разработка рекламной кампании.

Правильный ответ: a) Определение целей, сбор данных, анализ, разработка плана, контроль и коррекция.

4. Какие факторы могут влиять на производственную эффективность организации?

a) Погода и климатические условия.
b) Политическая стабильность в стране.
c) Состояние оборудования и квалификация персонала.
d) Фазы луны.

Правильный ответ: c) Состояние оборудования и квалификация персонала.

5. Какой из следующих методов управления качеством наиболее акцентирует внимание на предупреждении дефектов?

a) Контроль качества на этапе производства.
b) Система менеджмента качества ISO 9001.
c) Контроль качества готовой продукции.
d) Утилизация бракованных изделий.

Правильный ответ: a) Контроль качества на этапе производства.

6. Какие из перечисленных функций относятся к управлению производственным процессом?

a) Маркетинг и реклама.
b) Планирование производства и контроль выполнения плана.
c) Развитие стратегии компании.
d) Бухгалтерский учет.

Правильный ответ: b) Планирование производства и контроль выполнения плана.

7. Что означает термин "линейная структура управления" в организации?

a) Управление осуществляется в одной вертикальной цепи командования.
b) Управление осуществляется через комитеты и коллегиальные органы.
c) Отсутствие структуры управления в организации.
d) Управление осуществляется горизонтально.

Правильный ответ: a) Управление осуществляется в одной вертикальной цепи командования.

8. Какие ключевые элементы включает в себя система управления качеством ISO 9001?

a) Стандарты для продукции и услуг.
b) Документация, обучение персонала, контроль процессов и управление изменениями.
c) Маркетинговая стратегия и анализ конкурентов.
d) Внутренние аудиты и обслуживание оборудования.

Правильный ответ: b) Документация, обучение персонала, контроль процессов и управление изменениями.

9. Какие из следующих факторов могут влиять на производственную безопасность в организации?

a) Географическое положение офисов.
b) Техническое состояние оборудования и наличие обученного персонала.
c) Цвет стен в офисе.
d) Наличие кафе в здании.

Правильный ответ: b) Техническое состояние оборудования и наличие обученного персонала.

10. Для обеспечения безопасности информации на предприятии необходимо разработать _____, который будет определять политику и процедуры в области информационной безопасности.

Ответ: стандарт

11. Информационная безопасность предприятия включает в себя защиту информации от угроз, в том числе от внутренних источников. Для этого используются системы контроля доступа и механизмы _____.

Ответ: аутентификации и авторизации

12. При оценке рисков информационной безопасности, необходимо провести анализ возможных угроз и определить их _____ на бизнес-процессы.

Ответ: влияние

13. Политика информационной безопасности должна быть _____ всем сотрудникам предприятия, чтобы они знали, как действовать в случае инцидента.

Ответ: доступна

14. Для защиты конфиденциальной информации, часто используют шифрование данных, чтобы сделать их _____ для несанкционированного доступа.

Ответ: неразборчивыми

15. При управлении информационной безопасностью, важно регулярно обновлять и «патчить» программное обеспечение и операционные системы, чтобы закрыть известные _____.

Ответ: уязвимости

16. Сотрудники предприятия могут быть слабым звеном в системе информационной безопасности. Необходимо проводить обучение и _____ сотрудников в области безопасности.

Ответ: осведомление

17. План восстановления после инцидента включает в себя шаги по восстановлению работы информационных систем и _____ данных.

Ответ: восстановлению

18. Система мониторинга и реагирования на инциденты информационной безопасности позволяет быстро обнаруживать и реагировать на аномалии и потенциальные _____.

Ответ: угрозы

4 Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Руководитель практики от кафедры не менее, чем за два месяца до срока инструктивного занятия должен сообщить каждому о подготовке к практике производственной – преддипломной (далее производственная практика. Перед практикой проводится организационное собрание. Руководитель практики от кафедры проводит с обучающимися противопожарный инструктаж и инструктаж по технике безопасности. Проводится устное собеседование. После получения допуска обучающиеся расписываются о проведенных инструктажах в «Журнале регистрации первичного, повторного, внепланового противопожарного инструктажа (для студентов)» и «Журнале инструктажа на рабочем месте по охране труда (для студентов)».
Отчет по практике	По окончании производственной – преддипломной практики обучающийся составляет письменный отчет, содержание которого определено индивидуальным заданием на производственную практику, согласно Положению «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2017. В день окончания производственной – преддипломной практики обучающийся сдает «Студенческую аттестационную книжку производственного обучения» руководителю производственной практики для проверки полноты заполнения основных пунктов – наличие сроков прибытия и убытия обучающегося, подкрепленные печатями, заполнение таблиц проведения инструктажа, освоения компетенций и других таблиц журнала. В этот же день вместе со «Студенческой аттестационной книжкой производственного обучения» обучающийся сдает оформленный отчет по производственной – преддипломной практике руководителю практики и защищает его. Защита отчета осуществляется в течение 5-7 минут в форме доклада о проделанной работе, достигнутых результатах, а также полученных умениях и навыках работы со средствами контроля. Доклад можно представлять устно, либо в сопровождении с презентацией. По завершению доклада обучающемуся задаются вопросы по теме его работы. По результатам защиты отчетов по производственной – преддипломной практике руководитель выставляет учащимся оценки по 4-х бальной шкале, учитывая критерии, указанные в фонде оценочных средств. Результаты сформированности компетенций при прохождении производственной – преддипломной практики учащимися, руководитель практики заносит в «Студенческую аттестационную книжку производственного обучения». Также в ней он может отметить результаты выполнения обучающимся программы практики, его отношение к работе и трудовой дисциплине.

Для организации и проведения промежуточной аттестации в форме зачета с оценкой составляются 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:

– перечень теоретических вопросов к зачету;

– индивидуальные задания по прохождению производственной практики.

Описание процедуры проведения промежуточной аттестации по практике в форме зачета с оценкой и оценивания результатов обучения

Руководитель практики от профильной организации в последний день практики:

– пишет отзыв руководителя о прохождении обучающимся практики;

– заполняет аттестационный лист по практике, оценивая уровни сформированности компетенций (качество выполнения обучающимся работ индивидуального задания на практику) у обучающегося по результатам прохождения практики; результаты оценивания заносит в следующую таблицу (уровень сформированности компетенции отмечается в таблице, например, знаком «+»; если за компетенцией закреплено несколько видов работы, то при оценивании уровня сформированности компетенции при прохождении практики учитываются все виды работы):

Код компетенции	Содержание компетенции	Уровни сформированности компетенций			
		Высокий	Базовый	Минимальный	Компетенция не освоена

– выставляет оценку за выполнение программы практики.

Руководитель практики от профильной организации при оценивании уровня сформированности компетенции у обучающегося по результатам прохождения практики должен руководствоваться:

– четкостью владения обучающимся нормативной документацией;

– качеством и своевременностью выполнения обучающимся работ;

– качеством ведения отчетной документации;

– исполнительской дисциплиной обучающегося;

– наличием элементов рационализаторских предложений поступивших от обучающегося.

Обучающийся в последний день практики:

– сканирует или фотографирует отчетные документы по практике: отчет по практике, путевку на практику, листы для занесения поощрений и замечаний, отзыв руководителя от профильной организации и аттестационный лист по практике;

– отправляет отчетные документы по практике через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося) руководителю производственной практики.

Руководитель производственной практики в последний день практики оценивает выполнение обучающимся индивидуального задания и прохождение обучающимся практики, учитывая:

– оценку, выставленную руководителем практики от профильной организации, за выполнение обучающимся программы практики;

– отзыв руководителя практики от профильной организации о прохождении обучающимся практики;

– отчет обучающегося по практике;

– отсутствие и(или) наличие поощрений и(или) замечаний.