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.03 (П) ПРАКТИКА
производственная – эксплуатационная

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. – 3
Продолжительность в неделях – 2
Часов по учебному плану – 108

Форма промежуточной аттестации в семестре:
зачет с оценкой 6

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.ф.-м.н., доцент А. А. Бутин

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 и углубление теоретических и практических знаний, полученных при изучении дисциплин базовой и вариативных частей учебного плана в ходе лекционных и практических занятий, лабораторного практикума и выполнения курсовых работ.
2	приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника.

1.2 Задачи проведения практики

1	знакомство с вопросами техники безопасности и охраны окружающей среды на предприятии.
2	знакомство с практической работой предприятия; изучение деловой документации.
3	изучение и анализ опыта использования технологий построения защищенных автоматизированных систем (АС) на предприятии.
4	овладение практической методикой проектирования/ внедрения/эксплуатации компонент комплексной системы защиты информации АС (выполнение практического задания по будущей специальности: настройка защищенных режимов работы операционных систем, систем баз данных, сайтов, сетевого взаимодействия, добавочных систем защиты информации и т.д.).
5	подготовка и систематизация необходимых материалов для отчета и выполнения последующих курсовых работ и выпускной квалификационной работы.

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

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП

2.1 Требования к предварительной подготовке обучающегося

1	Б1.Б.14 Криптографические методы защиты информации
2	Б1.Б.16 Техническая защита информации
3	Б1.Б.18 Безопасность жизнедеятельности
4	Б1.Б.20 Технологии и методы программирования
5	Б1.Б.27 Правоведение
6	Б1.В.04 Безопасность операционных систем
7	Б1.В.07 Аудит информационной безопасности
8	Б1.В.ДВ.05.01 Системы управления базами данных

2.2 Дисциплины и практики, для которых прохождение данной практики необходимо как предшествующее

1	Б1.Б.13 Программно-аппаратные средства защиты информации
2	Б1.Б.21 Основы управления информационной безопасностью
3	Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем
4	Б1.В.03 Безопасность вычислительных сетей
5	Б1.В.05 Комплексная защита в информационных системах персональных данных
6	Б1.В.06 Безопасность систем баз данных
7	Б1.В.ДВ.06.01 Информационная безопасность открытых систем
8	Б2.В.04(Пд) Производственная практика - преддипломная

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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	
Минимальный уровень освоения компетенции	
Знать	порядок выделения информации, подверженной угрозам информационной безопасности (ИБ);
Уметь	выделять виды и формы информации, подверженной угрозам ИБ;
Владеть	навыками выделения видов и форм информации, подверженной угрозам ИБ;
Базовый уровень освоения компетенции	
Знать	порядок проведения аудита ИБ в организации;
Уметь	проводить аудит ИБ АС;
Владеть	навыками проведения аудита ИБ АС;
Высокий уровень освоения компетенции	
Знать	методы и способы реализации атак на информационные ресурсы АС;
Уметь	анализировать методы и способы реализации атак на информационные ресурсы АС.
Владеть	навыками применения методов и способов реализации атак на информационные ресурсы АС.
ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
Минимальный уровень освоения компетенции	
Знать	основные классы штатных и добавочных программно-аппаратных средств обеспечения ИБ;
Уметь	устанавливать добавочные программно-аппаратные средства обеспечения ИБ;
Владеть	основными навыками администрирования встроенных программно-аппаратные средств обеспечения ИБ;
Базовый уровень освоения компетенции	
Знать	основные методы администрирования добавочных программно-аппаратные средств обеспечения информационной безопасности;
Уметь	администрировать штатную подсистему программно-аппаратной защиты информации;
Владеть	базовыми навыками администрирования добавочных программно-аппаратные средств обеспечения информационной безопасности;
Высокий уровень освоения компетенции	
Знать	методы администрирования штатных и добавочных программно-аппаратные средств обеспечения информационной безопасности;
Уметь	администрировать комплексную подсистему программно-аппаратной защиты информации.
Владеть	глубокими навыками администрирования встроенных и добавочных программно-аппаратные средств обеспечения ИБ.

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Минимальный уровень освоения компетенции	
Знать	способы распространения современного программного обеспечения;
Уметь	применять программные средства системного назначения;
Владеть	владеть инструментальные средствами программирования;
Базовый уровень освоения компетенции	
Знать	основные категории требований к программно-аппаратной реализации средств обеспечения ИБ;
Уметь	применять программные средства прикладного назначения;
Владеть	владеть языками программирования;
Высокий уровень освоения компетенции	
Знать	методики применения программных средств специального назначения;
Уметь	применять программные средства специального назначения;
Владеть	владеть системами программирования.

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты	
Минимальный уровень освоения компетенции	
Знать	основные классы штатных и добавочных программно-аппаратных средств обеспечения ИБ;
Уметь	устанавливать добавочные программно-аппаратные средства обеспечения ИБ;
Владеть	основными навыками администрирования встроенных программно-аппаратные средств обеспечения информационной безопасности;
Базовый уровень освоения компетенции	
Знать	основные методы администрирования добавочных программно-аппаратные средств обеспечения информационной безопасности;
Уметь	администрировать штатную подсистему программно-аппаратной защиты информации;
Владеть	базовыми навыками администрирования добавочных программно-аппаратные средств обеспечения

	информационной безопасности;
Высокий уровень освоения компетенции	
Знать	методы администрирования штатных и добавочных программно-аппаратные средств обеспечения информационной безопасности;
Уметь	администрировать комплексную подсистему программно-аппаратной защиты информации;
Владеть	глубокими навыками администрирования встроенных и добавочных программно-аппаратные средств обеспечения ИБ.

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Минимальный уровень освоения компетенции	
Знать	состав минимального набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Уметь	формировать минимальный набор необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Владеть	навыками выбора минимального набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Базовый уровень освоения компетенции	
Знать	состав базового набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Уметь	формировать базовый набор необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Владеть	навыками выбора базового набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Высокий уровень освоения компетенции	
Знать	состав полного набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Уметь	формировать полный набор необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Владеть	навыками выбора полного набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС.

ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
Минимальный уровень освоения компетенции	
Знать	нормативно-правовую базу проведения аттестации объекта информатизации (ОИ) по требованиям ФСТЭК РФ;
Уметь	организовать работы по специальной проверке и исследованию ОИ;
Владеть	навыками анализа требований ФСТЭК РФ и ФСБ РФ по аттестации ОИ;
Базовый уровень освоения компетенции	
Знать	нормативно-правовую базу проведения аттестации объекта информатизации (ОИ) по требованиям ФСТЭК РФ и ФСБ РФ;
Уметь	проводить специальные проверки ОИ;
Владеть	навыками проведения специальных проверок ОИ по требованиям безопасности информации;
Высокий уровень освоения компетенции	
Знать	нормативно-правовую базу проведения аттестации объекта информатизации (ОИ) по требованиям ФСЭК РФ, ФСБ РФ и международным стандартам;
Уметь	проводить специальную проверку и исследования ОИ;
Владеть	навыками проведения специальных проверок и исследований ОИ по требованиям безопасности информации.

ПК-6: способность 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	методики проведения проверки эффективности работы программных, программно-аппаратных и технических средств защиты информации;
Уметь	организовать проверки эффективности работы программных, программно-аппаратных и технических средств защиты информации;
Владеть	навыками тестирования работоспособности программных, программно-аппаратных и технических средств защиты информации;

Базовый уровень освоения компетенции	
Знать	способы устранения нештатных ситуаций в процессе функционирования программных, программно-аппаратных и технических средств защиты информации;
Уметь	проводить проверки эффективности работы программных, программно-аппаратных и технических средств защиты информации;
Владеть	навыками анализа результатов тестирования работоспособности программных, программно-аппаратных и технических средств защиты информации;
Высокий уровень освоения компетенции	
Знать	методики проведения проверки эффективности работы и способы устранения нештатных ситуаций;
Уметь	проводить проверки эффективности работы программно-аппаратных средств защиты информации и способы устранения нештатных ситуаций;
Владеть	навыками тестирования работоспособности программных, программно-аппаратных и технических средств защиты информации и анализа его результатов.

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	
Минимальный уровень освоения компетенции	
Знать	состав минимального набора необходимых мер по обеспечению ИБ в зависимости от специфики функционирования АС;
Уметь	формировать проект минимального набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС;
Владеть	навыками проектирования минимального набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования АС;
Базовый уровень освоения компетенции	
Знать	методики проведения аудита АС ОИ;
Уметь	провести аудит АС ОИ по необходимым требованиям ИБ;
Владеть	навыками проектирования базового набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования АС;
Высокий уровень освоения компетенции	
Знать	методики разработки политики информационной безопасности организации;
Уметь	провести аудит АС ОИ по требованиям ИБ с формированием соответствующих проектных решений;
Владеть	навыками проектирования полного набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования АС.

ПСК-4-1: способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	
Минимальный уровень освоения компетенции	
Знать	порядок идентификации и учета информационных технологий в составе АС;
Уметь	определять стандартный набор мер для защиты информационных ресурсов;
Владеть	навыками реализации базового набора мер защиты информации;
Базовый уровень освоения компетенции	
Знать	порядок проведения аудита ИБ организации;
Уметь	адаптировать технологии защиты информации с учетом специфики инфраструктуры ОИ;
Владеть	навыками применения базового адаптированного набора мер защиты информации;
Высокий уровень освоения компетенции	
Знать	методы и способы реализации атак на информационные технологии АС;
Уметь	противодействовать реализациям угроз на информационные технологии АС;
Владеть	навыками применения базового адаптированного уточненного набора мер защиты информации.

В результате прохождения практики обучающийся должен

Знать	
1	порядок проведения аудита ИБ в организации;
2	основные способы администрирования добавочных программно-аппаратные средств обеспечения ИБ;
3	нормативно-правовую базу проведения аттестации объекта информатизации по требованиям ФСТЭК РФ;
Уметь	
1	устанавливать добавочные программно-аппаратные средства обеспечения ИБ;
2	администрировать комплексную подсистему защиты информации.
3	проводить проверки эффективности работы программных, программно-аппаратных и технических средств защиты информации;
Владеть	

1	навыками выделения информационных ресурсов, подлежащих защите;
2	навыками тестирования работоспособности программных, программно-аппаратных и технических средств защиты информации и анализа его результатов;
3	навыками участия в организации и сопровождении аттестации объекта информатизации по требованиям безопасности 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 задания от руководителя практики университета	ФГБОУ ВО ИрГУПС, кафедра «Информационные 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	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и	Проведение аудита объекта информатизации	8	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2	Отчет

	возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты			Э.1-Э.6	
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Установка и эксплуатация средств защиты информации	12	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2 Э.1-Э.6	Отчет
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Установка и эксплуатация программного обеспечения различного назначения	10	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2 Э.1-Э.6	Отчет
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты	Администрирование подсистемы защиты информации	24	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2 Э.1-Э.6	Отчет
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Участие в реализации мероприятий по установке, настройке и эксплуатации средств защиты	10	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2 Э.1-Э.6	Отчет
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Участие в проведении специальных мероприятий при аттестации ОИ	18	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2 Э.1-Э.6	Отчет
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Тестирование и эксплуатация средств защиты	10	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2 Э.1-Э.6	Отчет
ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Аудит объекта. Проектирование системы защиты информации	8	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2 Э.1-Э.6	Отчет
ПСК-4-1	способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах,	Аудит информационных технологий организации	8	Л1.1 – Л1.6, Л2.1 – Л2.5, Л3.1, Л3.2, Л4.1, Л4.2 Э.1-Э.6	Отчет

	при организации защиты обрабатываемой в них информации				

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ 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	Корниенко А.А	Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте: учебник. [Электронный ресурс] https://e.lanbook.com/book/59240#book_name	М.: УМЦ по образованию на ж.-д. трансп., 2014.	100% онлайн
Л1.2	Корниенко А.А.	Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. [Электронный ресурс] https://e.lanbook.com/book/59241	М.: Учебно-методический центр по образованию на ж.д. транспорте, 2014	100% онлайн
Л1.3	Загинайлов Ю.Н.	Теория информационной безопасности и методология защиты информации: учебное пособие. [Электронный ресурс] http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1	М., Берлин: Директ-Медиа, 2015	100% онлайн
Л1.4	Афанасьев А.А., Веденьев Л.Т., Воронцов А.А.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. [Электронный ресурс] http://e.lanbook.com/books/element.php?pl1_id=5114	Горячая линия-Телеком, 2012	100% онлайн
Л1.5	Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью». Выпуск 1: учебное пособие. [Электронный ресурс] https://e.lanbook.com/book/5178#book_name	М.: «Горячая линия-Телеком», 2012.	100% онлайн
Л1.6	Проскурин В.Г.	Защита в операционных системах. [Электронный ресурс] http://e.lanbook.com/books/element.php?pl1_id=63241	Горячая линия-Телеком, 2014	100% онлайн
Л1.7	Малюк А.А., Горбатов В.С., Королев В.И.	Введение в информационную безопасность: учебное пособие. [Электронный ресурс] https://e.lanbook.com/book/5171#book_name	«Горячая линия-Телеком», 2012.	100% онлайн
Л1.8	Паршин К.А.	Оценка уровня информационной безопасности на объекте информатизации: учебное пособие. [Электронный ресурс] https://e.lanbook.com/book/80018#book_name	М.: УМЦ по образованию на ж.-д. трансп., 2015.	100% онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Серия «Вопросы управление информационной безопасностью». Выпуск 2. Управление рисками информационной безопасности: учебное пособие. [Электронный ресурс] https://e.lanbook.com/book/5179#book_name	М.: «Горячая линия-Телеком», 2012	100% онлайн
Л2.2	Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Серия «Вопросы управление информационной безопасностью». Выпуск 3. Управление инцидентами информационной безопасности и непрерывностью бизнеса: Учебное пособие. [Электронный ресурс] https://e.lanbook.com/book/5180#book_name	М.: «Горячая линия-Телеком», 2013	100% онлайн
Л2.3	Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Серия «Вопросы управление информационной безопасностью». Выпуск 4. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие. [Электронный ресурс] https://e.lanbook.com/book/5181#book_name	М.: «Горячая линия-Телеком», 2012	100% онлайн
Л2.4	Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Серия «Вопросы управление информационной безопасностью». Выпуск 5. Проверка и оценка деятельности по управлению информационной безопасностью: учебное пособие. [Электронный ресурс] https://e.lanbook.com/book/5182#book_name	М.: «Горячая линия-Телеком», 2012	100% онлайн
Л2.5	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: методические указания и рекомендации. [Электронный ресурс] https://e.lanbook.com/book/5150#book_name	М.: «Горячая линия-Телеком», 2012	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.	Коммерческая тайна предприятия и технология ее защиты: учебное пособие	Иркутск: ИрГУПС, 2005	16
Л3.2	Глухов Н.И.	Оценка информационных рисков предприятия: Учеб. 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 кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л4.1	Глухов Н.И., Середкин С.П.	Транспортная безопасность: учебно-методическое пособие для самостоятельной работы студентов	Иркутск: ИрГУПС, 2014	88
Л4.2	Бутин А.А.	Методические рекомендации по выполнению задания по производственной практике.	Личный кабинет обучающегося	100% онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Э.1	НОУ «ИНТУИТ» http://www.intuit.ru
Э.2	Официальный сайт Microsoft http://www.microsoft.com
Э.3	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru
Э.4	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.5	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.6	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	Mozilla FireFox (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	Профильные организации, оснащенные сертифицированными средствами защиты информации в соответствии с: государственным реестром сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00); выпиской из перечня средств защиты информации, сертифицированных ФСБ России (http://clsz.fsb.ru/certification.htm).
7	Помещение для хранения и профилактического обслуживания учебного оборудования – А-521.

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 практики от 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.03 (П) Практика «производственная – эксплуатационная»

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

Б2.В.03 (П) Практика «производственная - эксплуатационная»

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

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

Практика «Производственная – эксплуатационная» участвует в формировании компетенций:

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;

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПСК-4-1: способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации.

Таблица траекторий формирования у обучающихся компетенций ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПСК-4-1 при освоении образовательной программы

Код компе-тенции	Наименование компетенции	Индекс и наименование дисциплин, практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы 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	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 -	6	4

	функционирования объекта защиты	эксплуатационная		
		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 профессиональных задач	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 управления базами данных	5	3
		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	8	6

		практика - преддипломная		
		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	8	4

		квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		
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-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Б1.Б.32 Основы кибернетики	5	2
		Б1.В.07 Аудит информационной безопасности	6	3
		Б1.В.ДВ.04.02 Эффективность информационных систем	6	3
		Б1.В.ДВ.07.01 Экономика защиты информации	6	3
		Б1.В.ДВ.08.01 Методология анализа информационных рисков	6	3
		Б1.В.ДВ.08.02 Инструментарий анализа информационных рисков	6	3
		Б2.В.03(П) Производственная - эксплуатационная	6	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	4
ПСК4-1	способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	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 подготовку к процедуре защиты и процедуру защиты	8	4

Таблица соответствия уровней освоения компетенций ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-4-1 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	Администрирование выбранной в ходе практики	Минимальный уровень	**Знать:** разновидности и основные функциональные особенности подсистем ИБ;

	информационной безопасности объекта защиты	системы обеспечения 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 подход к обеспечению информационной безопасности объекта защиты	Изучение базовых политик информационной безопасности. Выбор, разработка или доработка и конкретизация политик безопасности рассматриваемого объекта защиты.	Минимальный уровень	**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	**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.
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.

Программа контрольно-оценочных мероприятий за период прохождения практики

№	Неделя	Наименование контрольно-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	Тема «Оформление на практику»	ОПК-7 ПК-1-ПК-7 ПСК-4-1	Отчет по практике (письменно)
	1	Текущий контроль	Тема «Инструктаж по технике безопасности»	ОПК-7 ПК-1-ПК-7 ПСК-4-1	Отчет по практике (письменно)
	1	Текущий контроль	Тема «Инструктаж по методике выполнения задания»	ОПК-7 ПК-1-ПК-7 ПСК-4-1	Отчет по практике (письменно)
	1	Текущий контроль	Тема «Ознакомление с рабочим местом практики»	ОПК-7 ПК-1-ПК-7 ПСК-4-1	Отчет по практике (письменно)
	1	Текущий контроль	Тема «Изучение проектно--технической документации»	ОПК-7 ПК-1-ПК-7 ПСК-4-1	Отчет по практике (письменно)
	2	Текущий контроль	Тема «Разработка технического задания. Выполнение задания на преддипломную практику»	ОПК-7 ПК-1-ПК-7	Отчет по практике (письменно)

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
1	2	3	4	5	6
				ПСК-4-1	
	2	Текущий контроль	Тема «Обработка и анализ полученных результатов»	ОПК-7 ПК-1-ПК-7 ПСК-4-1	Отчет по практике (письменно)
	2	Текущий контроль	Тема «Оформление документов и защита отчета научному руководителю»	ОПК-7 ПК-1-ПК-7 ПСК-4-1	Отчет по практике Собеседование (устно)

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

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.

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 сформированности компетенций представлен в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
Текущий контроль успеваемости			
1	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	Задания на практику
2	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы по темам/разделам дисциплины
Промежуточная аттестация			
3	Зачет (дифференцированный зачет)	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к зачету

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации, 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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседования

Шкала оценивания	Критерии оценивания
«отлично»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»	Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»	Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	Не было попытки выполнить задание

Отчет по практике, отчет по НИР

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: – выполнен 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; – низкий уровень владения методической терминологией; – 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 заданий; – 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 Типовые вопросы для собеседования

1. Тема практической работы?
2. Где проходила практика?
3. Кто руководил практикой на предприятии?
4. Какие задачи были поставлены в рамках практики?

5 . Какие программно-аппаратные средства обеспечения информационной безопасности использовались в ходе практики?
6. Какие технические средства и приборы использовались в ходе практики?
7. Какие литературные источники изучены в ходе практики?
8. Охарактеризуйте состояние исследований в Вашей предметной области.
9. Охарактеризуйте качество и достоверность предложенных решений.
10 . Какие основные результаты имеются в Вашей предметной области?
11. Какие задачи предметной области являются основными и какие второстепенными?
12. Назначение и особенности работы ИС предметной области.
13. Что нового предлагается в Вашей работе?
14. Перспективы внедрения работы на производстве.
15. Вопросы по содержанию отчета и теме исследования

3.2 Типовые вопросы для отчета

Типовые вопросы, которые нужно отразить в отчете:
1. Предметная область практики;
2. Задачи предметной области;
3. Известные методы решения поставленных задач;
4. Проблемы существующих научно-технических решений, известных в предметной области;
5. Описание основных результатов прохождения практики;
6. Возможные предложения по совершенствованию существующих алгоритмических, математических, программно-технических решений, известных в предметной области;
7. Полученные навыки/знания за период прохождения практики;
8 Список использованных источников.

3.3 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по практике

Индикатор достижения компетенции	Тема в соответствии с РПП	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-7	Прохождение инструктажа по охране труда и технике безопасности	Знание	5 – ОТЗ 5 – ЗТЗ
ПК-1 ПК-2 ПК-3	Ознакомление с приказом о приеме на практику и назначение руководителя практики от профильной организации	Знание	5 – ОТЗ 5 – ЗТЗ
ПК-4	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	5 – ОТЗ 5 – ЗТЗ
ПК-5	Прохождение медицинского осмотра и оформление на работу	Знание	5 – ОТЗ 5 – ЗТЗ
ПК-6	Прохождение инструктажа по охране труда, технике безопасности, пожарной безопасности на рабочем месте и	Знание	5 – ОТЗ 5 – ЗТЗ

	ознакомление с правилами трудового внутреннего распорядка профильной организации.	Умение	5 – ОТЗ 5 – ЗТЗ
ПК-1 ПК-2 ПК-3 ПК-7 ПСК-4-1	Выполнение индивидуального задания	Знание	5 – ОТЗ 5 – ЗТЗ
		Умение	5 – ОТЗ 5 – ЗТЗ
		Навык	5 – ОТЗ 5 – ЗТЗ
ПК-7	Получение отзыва от руководителя практики от профильной организации	Знание	5 – ОТЗ 5 – ЗТЗ
ПК-6	Написание отчета по практике	Знание	5 – ОТЗ 5 – ЗТЗ
ПК-3	Отправление через ЭИОС университета отчетных документов и получение оценки результатов прохождения практики и выполнения индивидуального задания от руководителя практики от университета	Знание	5 – ОТЗ 5 – 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 практики.

Образец типового варианта итогового теста,
предусмотренного рабочей программой практики

1. Выберите правильное определение термина «информация»:
   а) совокупность содержащихся в базах данных сведений;
   б) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;
   в) сведения (сообщения, данные) воспроизводимые различными системами;
   г) сведения (сообщения, данные) независимо от формы их представления.

2. Выберите правильное определение термина «обладатель информации»:
   а) лицо, самостоятельно создавшее информацию;
   б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;
   в) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
   г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

3. Предоставление информации – это

Ответ: действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

4. Защищаемые помещения – это

Ответ: помещения, специально предназначенные для проведения конфиденциальных мероприятий.

5. Выберите правильное определение термина «контролируемая зона»:

а) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;

в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;

г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

6. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):

а) методы и способы защиты информации от несанкционированного доступа;

б) методы и способы сокрытия информации от внутренних нарушителей;

в) методы и способы устранения конкурентов;

г) методы и способы защиты информации от утечки по техническим каналам.

7. Технические способы защиты информации в зависимости от используемых средств классифицируются как (выберите все верные варианты ответов):

а) полуактивные;

б) пассивные;

в) разноплановые;

г) удостоверяющие;

д) активные.

8. Технический канал утечки информации – это

Ответ: совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

9. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно ____

Ответ: 16.

10. Техническими каналами утечки информации являются (выберите все верные варианты ответов):

а) кражи технических средств информационной системы;

б) утечки акустической (речевой) информации;

в) утечки информации, реализуемые через общедоступные информационные сети;

г) утечки видовой информации;

д) утечки информации по каналам побочных электромагнитных излучений;

е) утечки информации, реализуемые через интернет.

11. Несанкционированный доступ к информации – это

Ответ: **доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств.**

12. Механизм контроля целостности СЗИ Secret Net предназначен для

а) формирония цифровых отпечатков данных;
б) контроля информационных потоков;
в) слежения за неизменностью содержимого ресурсов компьютера.

13. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для

а) ограничения использования программного обеспечения на компьютере;
б) установки ограниченного количества программ;
в) сбора сведений об используемых приложениях.

14. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями

а) «конфиденциально»;
б) «секретно»;
в) «строго конфиденциально»,
г) «неконфиденциально».

15. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного_____

Ответ: логарифма.

16. Хэш-функции предназначены, главным образом, для _____

Ответ: контроля целостности данных.

17. Длина хэш-кода алгоритма MD5 составляет _____

Ответ: 128 бит.

18. Каким образом в СЗИ Secret Net реализуется настройка дискреционного разграничения доступа к файлам и папкам?

Ответ: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы.

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 спланированных оценочных средств в соответствии с рабочей программой дисциплины

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Обучающийся представляет отчет по практике, отвечает на вопросы руководителя практики от кафедры/научного руководителя магистратуры. В ходе собеседования обучаемый должен продемонстрировать знание предметной области исследования по своей тематике, используемого программного и аппаратного обеспечения, изученной литературы, иметь представление о состоянии аналогичных исследований в стране и за рубежом.
Отчет по практике	Обучающийся должен представить отчет, в который должны войти: 1. Введение (задание на практику) 2. Краткое описание предприятия, где проходила практика, состав, решаемые задачи 3. Описание текущего состояния предметной области с изложением ее проблем и задач

	4. Описание существующих программно-технических решений в области исследования 5. Предложения по развитию/совершенствованию известных решений (при наличии) 6. Заключение (выводы по практике) 7. Список источников Оценка за практику выставляется с учетом мнения руководителя практики от производства, полноты представленного материала, качества и полноты ответов на вопросы по итогам практики

Описание процедур проведения промежуточной аттестации в форме зачета и оценивания результатов обучения

Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).