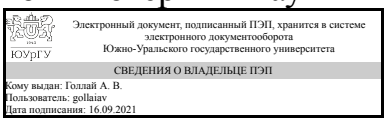
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Директор института
Высшая школа электроники и компьютерных наук



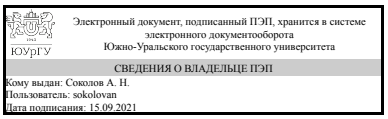
А. В. Голлай

РАБОЧАЯ ПРОГРАММА
практики
к ОП ВО от 01.07.2020 №084-2630

Практика Производственная практика, преддипломная практика
для специальности 10.05.03 Информационная безопасность автоматизированных систем
Уровень специалист **Тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

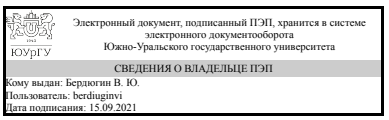
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
доцент



В. Ю. Бердюгин

Челябинск

1. Общая характеристика

Вид практики

Производственная

Способ проведения

Стационарная или выездная

Тип практики

преддипломная

Форма проведения

Дискретно по видам практик

Цель практики

Целями преддипломной практики являются:
- закрепление и конкретизация результатов теоретического обучения;
- приобретение студентами умений и навыков самостоятельной практической работы по специальности "Информационная безопасность автоматизированных систем";
- получение студентами практических навыков выполнения мероприятий по организационной, правовой и технической защите информации, овладение методами работы с техническими и программно-аппаратными средствами защиты информации;
- развитие у студентов навыков проведения анализа деятельности предприятий и организаций по усовершенствованию их работы;
- подготовка выпускной квалификационной работы.

Задачи практики

Задачами преддипломной практики являются:
- использование нормативных правовых документов по обеспечению защиты информации;
- изучение принципов формирования комплекса мер по обеспечению информационной безопасности с учетом их правовой обоснованности, административно-управленческой и технической реализуемости, а также экономической целесообразности;
- изучение видов и форм информации, подверженной угрозам, видов и возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;
- участие в эксплуатации и администрировании подсистем управления информационной безопасностью предприятия;
- участие в работах по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;
- проведение предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности с учетом

экономической эффективности разработок;
- оформление рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности;
- применение программных средств системного, прикладного и специального назначения;
- использование инструментальных средств и систем программирования для решения профессиональных задач;
- проведение анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.

Краткое содержание практики

Преддипломная практика студентов является составной частью основной образовательной программы высшего образования и представляет собой форму организации учебного процесса, непосредственно ориентированную на профессионально-практическую подготовку обучающихся.
Преддипломная практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм (далее организациях), основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по специальности "Информационная безопасность автоматизированных систем" или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.
Преддипломная практика является завершающим этапом учебного процесса, предназначенным для подготовки выпускной квалификационной работы.

2. Компетенции обучающегося, формируемые в результате прохождения практики

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения при прохождении практики (ЗУНы)
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Знать:принципы формирования политики информационной безопасности в информационных системах.
	Уметь:определять комплекс мер (правила, процедуры, практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем.
	Владеть:методами разработки частных политик информационной безопасности информационных систем.
ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Знать:принципы формирования и анализа проектных решений по обеспечению безопасности автоматизированных систем в соответствии с требованиями по защите информации.
	Уметь:оценивать информационные риски

	в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.
	Владеть:навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных систем.
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Знать:свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления; задачи органов защиты информации на предприятиях; действующие нормативные и методические документы по оформлению рабочей технической документации.
	Уметь:квалифицированно исследовать состав документации предприятия (организации); разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.
	Владеть:методами формирования требований по защите информации.
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Знать: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.
	Уметь:применять нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации.
	Владеть:навыками работы с нормативными правовыми актами в области обеспечения информационной безопасности и нормативными методическими документами ФСБ России и ФСТЭК России в области защиты информации.

	Знать:базовые методы и средства самоорганизации и самообразования при подготовке выпускной квалификационной работы.
ОК-8 способностью к самоорганизации и самообразованию	Уметь:планировать самостоятельную образовательную деятельность на основе формулирования ближайших и стратегических целей при подготовке выпускной квалификационной работы.
	Владеть:навыками планирования, определения средств и целей самостоятельной деятельности при подготовке выпускной квалификационной работы.

3. Место практики в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ	Перечень последующих дисциплин, видов работ
В.1.09 Обеспечение информационной безопасности на критически важных объектах Б.1.37 Комплексное обеспечение защиты информации объектов информатизации Б.1.23 Криптографические методы защиты информации Б.1.25 Техническая защита информации Б.1.30.01 Разработка защищенных автоматизированных систем Б.1.24.02 Правовое обеспечение информационной безопасности Б.1.24.01 Организационное обеспечение информационной безопасности Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности (8 семестр)	

Требования к «входным» знаниям, умениям, навыкам студента, необходимым для прохождения данной практики и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.24.01 Организационное обеспечение информационной безопасности	Знать: источники и классификацию угроз информационной безопасности; основы организационного обеспечения информационной безопасности. Уметь: разрабатывать технические задания на создание подсистем информационной

	безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов. Владеть: методами формирования требований по защите информации.
Б.1.24.02 Правовое обеспечение информационной безопасности	Знать: основы 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. Владеть: навыками работы с нормативными правовыми актами.
Б.1.25 Техническая защита информации	Знать: технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации. Уметь: анализировать и оценивать угрозы информационной безопасности объекта. Владеть: методами и средствами выявления угроз безопасности автоматизированным системам.
Б.1.23 Криптографические методы защиты информации	Знать: требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры; принципы построения криптографических алгоритмов. Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах. Владеть: криптографической терминологией.
Б.1.30.01 Разработка защищенных автоматизированных систем	Знать: методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Уметь: исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений. Владеть: методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем.
Б.1.37 Комплексное обеспечение защиты информации объектов информатизации	Знать: принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации). Уметь: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; выявлять уязвимости

	информационно-технологических ресурсов информационных систем. Владеть: навыками анализа информационной инфраструктуры информационной системы и ее безопасности; методами выявления угроз информационной безопасности информационных систем.
В.1.09 Обеспечение информационной безопасности на критически важных объектах	Знать: классы и характеристики критически важных объектов; понятия и определения, на которых базируются решения проблем информационной безопасности критически важных объектов; нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов. Уметь: реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам защиты информации ограниченного доступа. Владеть: терминологией и системным подходом при обеспечении информационной безопасности на критически важных объектах.
Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности (8 семестр)	Знать: место информационной безопасности автоматизированных систем в системе национальной безопасности РФ; риски информационной безопасности и проблемы построения комплексной системы защиты информации на предприятии; важность проведения анализа информационной безопасности объектов информатизации и автоматизированных систем. Уметь: выполнять поиск и проводить анализ изменения стандартов в области информационной безопасности. Владеть: навыками проведения анализа защищенности объектов информатизации и автоматизированных систем.

4. Время проведения практики

Время проведения практики (номер уч. недели в соответствии с графиком) с 23 по 26

5. Структура практики

Общая трудоемкость практики составляет зачетных единиц 6, часов 216, недель 4.

№ раздела (этапа)	Наименование разделов (этапов) практики	Кол-во часов	Форма текущего контроля

1	Организационный	8	Проверка дневника прохождения практики
2	Основной	144	Проверка дневника прохождения практики
3	Итоговый	64	Проверка отчета о прохождении практики

6. Содержание практики

№ раздела (этапа)	Наименование или краткое содержание вида работ на практике	Кол-во часов
1	Введение. Постановка задач практики. Производственный инструктаж, в том числе инструктаж по технике безопасности.	8
2.1	Знакомство с организацией и анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности: - автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите; - информационных технологий, формирующих информационную инфраструктуру предприятия (организации) в условиях существования угроз в информационной сфере и задействующих информационно-технологические ресурсы, подлежащие защите; - технологий обеспечения информационной безопасности автоматизированных систем; - систем управления информационной безопасностью автоматизированных систем. Выбор объекта проектирования. Сбор, обработка и систематизация фактического материала по выбранному объекту проектирования.	24
2.2	Знакомство с нормативными правовыми актами в области обеспечения информационной безопасности и нормативными методическими документами ФСБ России и ФСТЭК России в области защиты информации, необходимыми для обеспечения информационной безопасности выбранного объекта проектирования.	24
2.3	Разработка комплекса организационно-технических мероприятий, необходимых для обеспечения информационной безопасности выбранного объекта проектирования.	24
2.4	Выбор программно-аппаратных и технических средств защиты информации, необходимых для обеспечения информационной безопасности выбранного объекта проектирования.	24
2.5	Разработка документационного обеспечения защиты информации выбранного объекта проектирования.	24
2.6	Проведение технико-экономического обоснования разработанных проектных решений для обеспечения защиты информации	24

	выбранного объекта проектирования. Вопросы ТБ, ОТ и БЖД.	
3	Оформление отчета по преддипломной практике.	64

7. Формы отчетности по практике

По окончанию практики, студент предоставляет на кафедру пакет документов, который включает в себя:
- дневник прохождения практики, включая индивидуальное задание и характеристику работы практиканта организацией;
- отчет о прохождении практики.
Формы документов утверждены распоряжением заведующего кафедрой от 31.08.2016 №308-03-04.

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Форма итогового контроля – дифференцированный зачет.

8.1. Паспорт фонда оценочных средств

Наименование разделов практики	Код контролируемой компетенции (или ее части)	Вид контроля
Основной	ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Проверка основной главы и заключения ВКР
Все разделы	ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Дифференцированный зачет
Итоговый	ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Бонусное задание
Основной	ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Проверка основной главы и заключения ВКР
Все разделы	ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной	Дифференцированный зачет

	системы	
Основной	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Проверка введения и теоретической главы ВКР
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Дифференцированный зачет
Все разделы	ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Дифференцированный зачет

8.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Проверка основной главы и заключения ВКР	При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания: 1. Своевременность представления оцениваемых документов: 2 балла - документы представлены в назначенный срок; 1 балл - документы представлены с опозданием. 2. Вывод о достижении цели, сформулированной в задании на ВКР: 2 балла - цель полностью достигнута; 1 балл - цель достигнута частично; 0 - баллов цель не достигнута. 3. Качество разработанных студентом документов, регламентирующих обеспечение безопасности на объекте защиты: 2 балла - документы соответствую требованиям ГОСТ; 1 баллов - документы содержат отдельные нарушения; 0 баллов - документы отсутствуют или противоречат требования федеральных нормативно-правовых актов. 4. Практическое применение средств	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.

	и методов обеспечения информационной безопасности: 2 балла - при подготовке ВКР студент продемонстрировал навыки практического применения программно-технических средств обеспечения информационной безопасности; 1 балл - меры обеспечения информационной безопасности носили исключительно организационных характер. Максимальное количество баллов - 8. Весовой коэффициет - 2.	
Дифференцированный зачет	Зачет проводится в форме предварительной защиты ВКР перед комиссией, создаваемой распоряжением заведующего кафедры. В состав комиссии включаются: руководитель преддипломной практики и не менее двух преподавателей кафедры. Перед предварительной защитой студенту необходимо представить членам комиссии готовую дипломную работу и подписанный отзыв научного руководителя. В процессе предварительной защиты студент кратко излагает суть дипломной работы и отвечает на вопросы членов комиссии. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания: 1. Содержание и оформление ВКР: 3 балла - представленная ВКР полностью соответствует предъявляемым требованиям; 2 балл - представленная ВКР в целом соответствует предъявляемым требованиям однако имеются замечания, требующие частичной доработки;	Отлично: величина рейтинга обучающегося 85…100 % Хорошо: .величина рейтинга обучающегося 75…84 % Удовлетворительно: величина рейтинга обучающегося 60…74 % Неудовлетворительно: величина рейтинга обучающегося 0…59 %

	1 - балл, представленная ВКР в значительной мере не соответствует предъявляемым требованиям и серьезной доработки. 2. Содержание доклада: 3 балла -четко сформулированы цель и задачи ВКР, автор уверенно ориентируется в их тематике, может кратко изложить содержание; в презентации наглядно и в полном объеме отражены основные этапы ВКР; грамотное изложение материала; 2 балла - цель и задачи исследования сформулированы, но в отдельных случаях расплывчато, автор владеет профессиональной терминологией, грамотно и последовательно излагает материал, делает самостоятельные, обоснованные выводы, которые иногда не в полной мере связаны с содержанием работы; 1 - содержание работы не в полной мере соответствует заявленной теме, цель и задачи ВКР сформулированы неточно, путается в изложении материала; выводы носят формальный характер, зачастую не связаны с содержанием работы.. 3. Ответы на вопросы членов комиссии: 3 балла - студент грамотно и убедительно обосновывает актуальность темы ВКР, свободно ведет дискуссию по проблемам, отраженным в ВКР, отмечается уверенное владение профессиональной терминологией; 2 балла - студент в целом грамотно обосновывает актульность темы ВКР, владеет профессиональной терминологией, однако испытывает затруднения при ответе на некоторые вопросы членов комиссии; 1 балл - автор в недостаточной степени владеет профессиональной терминологией, испытывает затруднения при	

	ответах на большинство вопросов членов комиссии. Максимальное количество баллов - 9.	
Проверка введения и теоретической главы ВКР	При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания: 1. Своевременность представления оцениваемых документов: 2 балла - документы представлены в назначенный срок; 1 балл - документы представлены с опозданием. 2. Уровень знания нормативно-правовых документов: 2 балла - сссылки на нормативно-правовые документы абсолютно корректны; 1 балл - в ВКР имеются ссылки на утратившие силу нормативные документы. 3. Выводы по главе: 1 балл - вывод обобщает использованную информацию и содержит аргументированные субъективные суждения; 0 баллов - вывод отсутствует либо не содержит суждений и обобщений. Максимальное количество баллов - 5. Весовой коэффициет - 1.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.
Бонусное задание	Студент представляет копии документов, подтверждающие победу или участие в конференции. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Максимально возможная величина бонус-рейтинга +15 %.	Зачтено: 15 % за победу в конференции международного уровня +10 % за победу в конференции российского уровня +5 % за победу в конференции университетского уровня +1 % за участие в конференции. Не зачтено: не предусматривается.

8.3. Примерный перечень индивидуальных заданий

16. Разработка методов расчета экономической эффективности комплексной системы защиты информации предприятия (наименование предприятия).
20. «Программа внедрения цифровых водяных знаков в звуковые данные с использованием эхоэффекта».
42. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта).
26. Разработка комплексной системы защиты информации (КСЗИ) предприятия (название предприятия).
79. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).
63. Разработка методологии проектирования КСЗИ.
18 Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название предприятия).
15. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну (название предприятия).
80. «Исследование характеристик систем стеганографии звуковых данных с использованием дискретного вейвлет-преобразования».
34. Разработка моделей процессов защиты информации при проектировании КСЗИ.
47. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).
66. Комплексная система организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).
27. Автоматизация учета конфиденциальных документов на предприятии (название предприятия).
65. «Повышение информационной безопасности корпоративной вычисли-тельной сети (название предприятия)».
9. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).
41. Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам в (название предприятия).
33. Разработка моделей процессов защиты информации при проектировании КСЗИ.
53. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).
29. Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux.
75 Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).
25. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).
73. Организация защиты персональных данных на основе использования правовых мер (название предприятия).
49. «Разработка методики оценки эффективности средств зашиты информа-ции».
5. Разработка игровой (дискретной) модели программно-аппаратной защиты информации предприятия (наименование предприятия).

2. «Разработка комплексной системы защиты информации (название предприятия)».
1. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).
58. Построение алгоритма системы идентификации, защищенной от подделки продукции.
17. Разработка комплексной системы защиты информации в кабинете руководителя предприятия.
51. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия).
72 Автоматизация процесса проверок наличия конфиденциальных документов на предприятии (название предприятия).
61. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).
30. Организация порядка установления внутриобъектного спецрежима на объекте информатизации (название предприятия).
74. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну (название предприятия).
69. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).
23. «Система защиты данных в корпоративных сетях на основе криптографических методов».
46. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно (название предприятия).
4. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии .
45. Защита речевой информации в каналах связи коммерческих организаций.
56. Разработка проекта программно-аппаратной защиты информации предприятия (наименование предприятия).
43. Разработка комплексных систем видеонаблюдения и сигнализации для обеспечения защиты информации в (название предприятия).
22. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно (название предприятия).
52. Разработка систем видеонаблюдения и контроля доступа к объектам информатизации в (название предприятия).
77. Анализ методов оценки качества функционирования КСЗИ.
6. Организация порядка установления внутриобъектного спецрежима на объекте информатизации (название предприятия).
70. Анализ методов и форм работы с персоналом, допущенным к конфиденциальной информации, и разработка рекомендаций по их применению для торговых организаций.
11. Криптографические средства защиты информации на основе дискретных носителей.
78. Анализ нормативно-правовой базы по защите информации в сети Интернет.

Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия).
48. Организация защиты персональных данных на основе использования правовых мер (название предприятия).
32. «Система контроля движения на охраняемом объекте с помощью активных радиоволновых технических средств».33. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).
35. «Корреляционный анализ предупреждений системы обнаружения атак на основе нечеткой логики».
13. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).
59. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).
60. «Разработка методов и алгоритмов защиты исходного кода программ от несанкционированного доступа».
76. Разработка методологии проектирования КСЗИ.
71 Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия).
54. Комплексная автоматизированная система учета конфиденциальных документов на предприятии (название предприятия).
10. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).
44. Разработка организационного порядка установления внутриобъектного режима для торговой фирмы (название предприятия).
67. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).
38. Разработка изолированной программно-аппаратной среды в Windows NT (WINDOWS 2000, LINUX и т.д.) (наименование предприятия).
24. Разработка проекта комплексной системы программно-аппаратной защиты информации предприятия (наименование предприятия).
39. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия).
19. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта).
8. «Система обнаружения атак на основе искусственной нейронной сети».
7. Организация системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).
55. «Исследование принципов построения биометрических систем контроля доступа на основе анализа рукописного почерка».
28. Разработка методов расчета экономической эффективности программно-аппаратной защиты информации предприятия (наименование предприятия).
62. Организация автоматизированного пропускного режима на крупном предприятии (на примере).
40 Разработка комплексной системы защиты информации (КСЗИ) предпри-ятия

(название предприятия).
37. Организация комплексной системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).
50. Разработка мероприятий организационного характера по обеспечению комплексной защиты информации для (название предприятия).
57. Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия).
31. Разработка комплексной системы защиты информации в кабинете директора (название предприятия).
3. Анализ методов оценки качества функционирования КСЗИ.
64. Организация системы контроля доступа и защиты информации на предприятии (на примере ООО «Передвижная механизированная колонна-4»).
68. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).
12 Организация процессов мониторинга конфиденциального документооборота на предприятии (название предприятия).
14. Анализ нормативно-правовой базы по комплексной системы защиты информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия).
36. Разработка проекта корпоративной сети (название предприятия).
21 Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).

9. Учебно-методическое и информационное обеспечение практики

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

1. Безопасность жизнедеятельности [Текст] учеб. пособие для вузов А. Л. Бабаян и др.; под ред. А. И. Сидорова. - 3-е изд., перераб. и доп. - М.: КноРус, 2017

из них методические указания для самостоятельной работы студента:

1. Преддипломная практика по направлению подготовки "Информационная безопасность автоматизированных систем". Методические указания (учебно-методическая документация кафедры)

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в	Доступность (сеть Интернет /

			электронной форме	локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Болгова, Е. В. Производственная (научноисследовательская) и производственная (преддипломная) практика студентов: организация и проведение : учебно-методическое пособие / Е. В. Болгова, А. В. Калюжная, С. В. Ковальчук. — Санкт-Петербург : НИУ ИТМО, 2018. — 36 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/136535	Электронный каталог ЮУрГУ	Интернет / Авторизованный
2	Основная литература	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

10. Информационные технологии, используемые при проведении практики

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)
2. -Консультант Плюс(31.07.2017)
3. -Стандартинформ(бессрочно)

11. Материально-техническое обеспечение практики

Место прохождения практики	Адрес места прохождения	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, обеспечивающие прохождение практики
ФГУП "Приборостроительный завод", г.Трехгорный	456080, г. Трехгорный, ул. Заречная, 13	Стенды для отладки и испытаний микроэлектронного оборудования, серверы, ЛВС
ООО "Стратегия безопасности"	454052, г.Челябинск, ул. Пети Калмыкова, д.11-А	Программно-аппаратные комплексы по защите информации и оценке защищенности объектов информатизации.
АО "Челябинский радиозавод "Полет"	454080, Челябинск, ул. Тернопольская,	Стенды для отладки и испытаний микроэлектронного оборудования,

	6	серверы, ЛВС, средства доступа к глобальной сети