МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Удмуртский государственный университет»

ИНСТИТУТ ПРАВА, СОЦИАЛЬНОГО УПРАВЛЕНИЯ И БЕЗОПАСНОСТИ

ПРОГРАММА ПРАКТИКИ
учебная практика, ознакомительная

Специальность 10.05.05 «Безопасность информационных технологий в правоохранительной сфере

Специализация «*Организация и технология защиты информации*»

Квалификация выпускника специалист по защите информации

Курс 3, семестр 6, зачет -6 семестр

Формы обучения очная

ПРИЕМ 2021/2022

Разработчик(и) программы практики

ФИО	Ученая степень, звание, должность	Контактная информация (служебныеE-mail и телефон)
Бас А.С	Начальник лаборатории специальной техники	916-004

Экспертиза рабочей программы

Экспертиза рабочей программы

Первый уровень ***(оценка качества содержания программы, соответствие целям и задачам ООП ВО)***	
Руководитель ООП ВО	**Подпись руководителя ООО ВО**
Зам. директора по учебной работе	Лапшина Л.П.
Выписка из решения: Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.	

Второй уровень ***(оценка качества содержания программы и применяемых педагогических технологий)***		
Наименование кафедры	**№ протокола, дата**	**Зав. кафедрой**
Кафедра информационной безопасности в управлении	№ 6 от 02.02.2021 г.	Камалова Г.Г
Выписка из решения: Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.		

Третий уровень ***(соответствие целям подготовки и учебному плану образовательной программы)***		
Методическая комиссия	**№ протокола, дата**	**Председатель МК**
ИПСУБ	№ 3 от 10.02.2021 г.	Кайшев А.В.
Выписка из решения: Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.		

Программа практики составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки РФ от 26.11.2020 г. № 1461.

1. Указание вида практики, способа и формы (форм) ее проведения.

Вид практики: учебная

Тип практики: ознакомительная

Способ проведения практики: стационарная

Форма (формы) проведения: непрерывная

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.

Соотнесение планируемых результатов обучения при прохождении практики с планируемыми результатами освоения образовательной программы (компетенции из учебного плана) представлено в таблице 1.

Таблица 1

Планируемые результаты освоения ОП (компетенции)		**Планируемые результаты обучения при прохождении практики**		
Код	**Содержание компетенции**	**Знания**	**Умения**	**Навыки, опыт деятельности** *(по производственной практике)*
ОПК-9	Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности	ОПК-9.1.2 Знает логико-математические основы построения электронных цифровых устройств;	ОПК-9.3.3 владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов	

3. Указание места практики в структуре образовательной программы:

Дисциплины, на освоении знаний которых базируется практика:

Основы электро-,радиоизмерений;
Основы электротехники и радиоэлектроники

4. Указание объема практики в зачетных единицах и ее продолжительности в неделях (либо в астрономических часах).

Общий объем практики составляет 3 зачетных единиц, 108 академических часов, контактная работа – 2 час

Продолжительность практики 2 недели.

5. Содержание практики:

Цель практики: подготовка обучающегося к самостоятельному решению профессиональных задач в рамках научно-исследовательской деятельности в рамках требований ФГОС ВО, а также формирование у обучающихся первичных умений и навыков.

Задачи практики:

- вести биографическую работу с применением современных информационных технологий;
- формулировать и решать задачи, возникшие в ходе выполнения исследования;
- обрабатывать полученные результаты;
- оформлять результаты проделанной работы в соответствии с действующими требованиями нормативных документов с привлечением современных средств редактирования и печати.

База проведения практики:

Место прохождения практики - Кафедра информационной безопасности в управлении ФГБОУ ВО "Удмуртского государственного университета"

Общие задания по практике (виды работ, выполняемые в ходе практики): получение практических навыков и анализ полученных результатов по использованию конкретного устройства предназначенного для технической защиты конфиденциальной информации.

Этапы прохождения практики:

1.Подготовительный этап:

До начала прохождения практики руководителем практики со стороны университета обозначаются перед студентами конкретные задачи их практической деятельности, структура плана индивидуальной работы, форма и содержание отчетной документации.

2.Ознакомительный этап включает Инструктаж по технике безопасности при работе с электроустановками до 1000 Вольт. Прием зачетов по технике электробезопасности с подписью в журнале.

3.Основной этап прохождения практики состоит из выполнения заданий практики: общих и индивидуальных, определяемых руководителем практики

4. Заключительный этап включает подготовку студентами отчетных документов по практике (индивидуальная книжка обучающего по практике, отчет о проделанной работе) и защита отчета по практике.

6. Указание форм отчетности по практике:

Виды и формы текущего контроля прохождения практики обучающегося дифференцированный зачет

Виды и формы итоговой отчетности индивидуальная книжка по практике обучающегося и отчет о проделанной работе.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике:

Средства оценки сформированности компетенций: отчет о проделанной работе студента, отзыв руководителя практики.

Виды заданий для оценки уровня компетенций:

Виды работ для оценки уровня компетенций: отчет о практике должен содержать сведения о выполненных студентом работах в период практики (результаты исследований с последующими выводами).

Уровни сформированности компетенций

- **пороговый уровень** дает общее представление о практической деятельности, умеет использовать знания о выполнении практических действий, умеет выполнять

отдельные операции по виду деятельности, овладел некоторыми, методами и способами решения практических задач (соответствует оценке «удовлетворительно»);

- **базовый** позволяет решать типовые задачи, принимать профессиональные и управленческие решения, овладел основными навыками практической деятельности, приобрел опыт профессиональной деятельности, умеет принимать профессиональные и управленческие решения, умеет разрешать возникающие трудности в процессе выполнения деятельности (соответствует оценке «хорошо»);

- **повышенный уровень** предполагает готовность решать практические профессиональные задачи повышенной сложности, овладел всеми компонентами компетенции и приобрел высокий опыт деятельности, без затруднений решает возникающие трудности в процессе прохождения практики, овладел способностью принимать профессиональные и управленческие решения (соответствует оценке «отлично»).

8. Учебно-методическая литература и ресурсы сети Интернет, необходимых для проведения практики:

1. Методические пособия по работе с каждым комплексом и изделием изготовленные в стенах лаборатории «Специальная техника».

2. Стенды, комплексы и устройства предназначенные для поиска средств негласного съема информации и устройства предназначенные для защиты информации от утечки по техническим каналам.

9. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости): не используются

10. Описание материально-технической базы, необходимой для проведения практики:

Приёмник- коррелятор «Оракул; «Пиранья Анализатор спектра «АКС- 1292»; «Мангуст» и диктофоны: определение зоны подавления диктофонов; Индикаторы поля, галстучный микрофон и «Бриз mini»; Генераторы шума: «Бриз», «Бархан- 4» «Волна ВТ-2», «Ритон-3». Определение зоны подавления сотовых телефонов.

NF 431, АКС- 1292, SEL SP- 17D и радиоприёмник

Соната РК-1 и «Пиранья»; Изучение работы стенда ОПС, изучение теоретического материала по датчикам; Изучение стенда виброакустической защиты;Изучение метода разнесённых антенн с применением АКС- 1291, генератор шума «Бриз mini», NF 431 и галстучного микрофона; Изучение системы видеонаблюдения.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Удмуртский государственный университет»

ИНСТИТУТ ПРАВА, СОЦИАЛЬНОГО УПРАВЛЕНИЯ И БЕЗОПАСНОСТИ

«Утверждаю»
Директор института
_____ /Институт права, социального управления и безопасности/ В.Г. ВЕШИН
(подпись, ФИО)
«17» февраля 2021 г.

ПРОГРАММА ПРАКТИКИ
производственная практика, технологическая

Специальность 10.05.05 «безопасность информационных технологий в правоохранительной сфере»

Специализация «Организация и технология защиты информации»

Квалификация выпускника специалист по защите информации

Курс 4, семестр 8

Формы обучения очная

прием 2021/2022

Разработчик(и) программы практики

ФИО	Ученая степень, звание, должность	Контактная информация (служебныеE-mail и телефон)
Стерхова Т.Н	Доцент, ктн кафедры информационной безопасности в управлении	916-004

Экспертиза рабочей программы

Первый уровень
(оценка качества содержания программы, соответствие целям и задачам ООП ВО)

Руководитель ООП ВО	**Подпись руководителя ООО ВО**
Зам. директора по учебной работе	Лапшина Л.П.

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Второй уровень
(оценка качества содержания программы и применяемых педагогических технологий)

Наименование кафедры	**№ протокола, дата**	**Зав. кафедрой**
Кафедра информационной безопасности в управлении	№ 6 от 02.02.2021 г.	Камалова Г.Г

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Третий уровень
(соответствие целям подготовки и учебному плану образовательной программы)

Методическая комиссия	**№ протокола, дата**	**Председатель МК**
ИПСУБ	№ 3 от 10.02.2021 г.	Кайшев А.В.

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Программа практики составлена в соответствии с требованиями ФГОС ВО ФГОС ВО по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки РФ от 26.11.2020 г. № 1461

1. Указание вида практики, способа и формы (форм) ее проведения.

Вид практики: производственная

Тип практики: технологическая
Способ проведения практики: стационарная, выездная

Форма (формы) проведения: непрерывная

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.

Соотнесение планируемых результатов обучения при прохождении практики с планируемыми результатами освоения образовательной программы (компетенции из учебного плана) представлено в таблице 1.

Таблица 1

Планируемые результаты освоения ОП (компетенции)		**Планируемые результаты обучения при прохождении практики**		
Код	**Содержание компетенции**	**Знания**	**Умения**	**Навыки, опыт деятельности** *(по производственной практике)*
ОПК-4	Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	ОПК-4.1.3 знает основные этапы процесса проектирования и общие требования к содержанию проекта;	ОПК-4.2.1 умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	ОПК-4.2.3 умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;

3. Указание места практики в структуре образовательной программы:

Дисциплины, на освоении знаний которых базируется практика:

- Защита информационных процессов в компьютерных системах;
- Стандарты информационной безопасности;
- Аттестация объектов информатизации

4. Указание объема практики в зачетных единицах и ее продолжительности в неделях (либо в астрономических часах).

Общий объем практики составляет 3 зачетных единиц, 108 академических часов.

Продолжительность практики 2 недели.

5. Содержание практики:

Цель практики: приобретение практических навыков обеспечения защиты информации на предприятия различных форм собственности.

Задачи практики:

1. приобретение практических навыков аудита, обследования объекта защиты, построения системы защиты, ее эксплуатации в рамках программы практики;
2. ознакомление с применяемыми техническими средствами защиты конфиденциальной информации;
3. сбор материала для написания курсовой работы и выпускной квалификационной работы.

База проведения практики:

Местом прохождения производственной практики могут служить государственные, коммерческие и некоммерческие организации; информационные подразделения предприятий различных сфер деятельности, а также научно-производственные организации. Договоры на проведение практики заключены:

Министерство информатизации и связи Удмуртской Республики

Администрация г.Ижевска

Администрации МО

АУ УР «Ресурсный информационный центр Удм.Республики»

Министерство Внутренних Дел УР

Кафедра информационной безопасности в управлении ФГБОУ ВО "Удмуртского государственного университета"

Общие задания по практике (виды работ, выполняемые в ходе практики):

руководителями практики от института и предприятия выдается практиканту индивидуальное задание, связанное с выполняемой работой в отделе (службе) и с темой ВКР, направленное на углубленную разработку отдельных его частей.

Этапы прохождения практики:

1.Подготовительный этап:

До начала прохождения практики руководителем практики со стороны университета обозначаются перед студентами конкретные задачи их практической деятельности, структура плана индивидуальной работы, форма и содержание отчетной документации.

Со стороны руководителя практики организации проводится инструктаж по ОТ и пожарной безопасности

2.Ознакомительный этап включает знакомство с базой практики, с нормативной документацией, предметом деятельности.

3.Основной этап прохождения практики состоит из выполнения заданий практики: общих и индивидуальных, определяемых руководителями практик со стороны организации и университета.

4. Заключительный этап включает подготовку студентами отчетных документов по практике (индивидуальная книжка обучающего по практике, отчет о проделанной работе) и защита отчета по практике.

6. Указание форм отчетности по практике:

Виды и формы текущего контроля прохождения практики обучающегося дифференцированный зачет

Виды и формы итоговой отчетности индивидуальная книжка по практике обучающегося и отчет о проделанной работе.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике:

Средства оценки сформированности компетенций: отчет о проделанной работе студента, отзыв руководителя со стороны организации где студент проходил практику.

Виды заданий для оценки уровня компетенций: решение задач в соответствии с индивидуальным планом практики.

Виды работ для оценки уровня компетенций: отчет о практике должен содержать сведения о выполненных студентом работах в период практики (результаты исследований с последующими выводами).

Уровни сформированности компетенций

- **пороговый уровень** дает общее представление о практической деятельности, умеет использовать знания о выполнении практических действий, умеет выполнять отдельные операции по виду деятельности, овладел некоторыми, методами и способами решения практических задач (соответствует оценке «удовлетворительно»);

- **базовый** позволяет решать типовые задачи, принимать профессиональные и управленческие решения, овладел основными навыками практической деятельности, приобрел опыт профессиональной деятельности, умеет принимать профессиональные и управленческие решения, умеет разрешать возникающие трудности в процессе выполнения деятельности (соответствует оценке «хорошо»);

- **повышенный уровень** предполагает готовность решать практические профессиональные задачи повышенной сложности, овладел всеми компонентами компетенции и приобрел высокий опыт деятельности, без затруднений решает возникающие трудности в процессе прохождения практики, овладел способностью принимать профессиональные и управленческие решения (соответствует оценке «отлично»).

8. Учебно-методическая литература и ресурсы сети Интернет, необходимых для проведения практики:

Основная литература:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Указ Президента РФ от 05 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
Указ Президента РФ от 31 декабря 2015 № 683 «О Стратегии национальной безопасности Российской Федерации».
Постановление Правительства Российской Федерации от 3 ноября 1994 № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г.
Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992.
Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден Гостехкомиссией России, 1992. .
Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.
Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.
Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.
ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
ГОСТ Р 56546-2015 Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.
ГОСТ Р 56545-2015 Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.

ГОСТ Р 54583-2011/ISO/IEC/TR 15443-3:2007 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия.
ГОСТ Р 54582-2011/ISO/IEC/TR 15443-2:2005 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия.
ГОСТ Р 53647.6-2012 Национальный стандарт Российской Федерации. Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных.
ГОСТ Р 53114-2008 Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
ГОСТ Р 53113.1-2008 Национальный стандарт Российской Федерации. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.
ГОСТ Р 53113.2-2009 Национальный стандарт Российской Федерации. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.
ГОСТ Р 51275-2006 Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
ГОСТ Р ИСО/МЭК 15408-3-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
ГОСТ Р ИСО/МЭК 15408-2-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
ГОСТ Р ИСО/МЭК 18045-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
ГОСТ Р 50922-2006 Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.
ГОСТ Р 52069.0-2013 Национальный стандарт Российской Федерации. Защита информации. Система стандартов. Основные положения.
ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998.
ГОСТ Р 51241-98 Защита информации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Госстандарт России, 1998.
ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Ростехрегулирование, 2006.
ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Росстандарт, 2012.
ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по реализации системы менеджмента информационной безопасности. Росстандарт, 2012.
ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Госстандарт СССР, 1990.
ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Интернет-ресурсы:

www.fstec.ru; www.gost.ru; http://protect.gost.ru.

9. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости):

Информационные технологии используемые в организации для обеспечения функционирования процессов.
Программное обеспечение, используемое в организации в части обеспечения информационной безопасности.
Информационные справочные системы СПС «Консультант Плюс», «Гарант»

10. Описание материально-технической базы, необходимой для проведения практики:

Место проведения практики: структурные подразделения в организации (рабочее место)
Материально-техническое обеспечение практики: ресурсы организации, где студент проходит практику

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Удмуртский государственный университет»

ИНСТИТУТ ПРАВА, СОЦИАЛЬНОГО УПРАВЛЕНИЯ И БЕЗОПАСНОСТИ

«Утверждаю»
Директор института
_____ / В.Г. ВЕШИН
(подпись, ФИО)
«17» февраля 2021 г.

ПРОГРАММА ПРАКТИКИ
производственная практика,эксплуатационная

Специальность 10.05.05 «безопасность информационных технологий в правоохранительной сфере»

Специализация «Организация и технология защиты информации»

Квалификация выпускника специалист по защите информации

Курс 5, семестр 10

Формы обучения очная

Сроки проведения практики: 6 недель

прием 2021/2022

Разработчик(и) программы практики

ФИО	Ученая степень, звание, должность	Контактная информация (служебныеE-mail и телефон)
Стерхова Т.Н	Доцент, ктн кафедры информационной безопасности в управлении	916-004

Экспертиза рабочей программы

Первый уровень
(оценка качества содержания программы, соответствие целям и задачам ООП ВО)

Руководитель ООП ВО	**Подпись руководителя ООО ВО**
Зам. директора по учебной работе	Лапшина Л.П.

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Второй уровень
(оценка качества содержания программы и применяемых педагогических технологий)

Наименование кафедры	**№ протокола, дата**	**Зав. кафедрой**
Кафедра информационной безопасности в управлении	№ 6 от 02.02.2021 г.	Камалова Г.Г

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Третий уровень
(соответствие целям подготовки и учебному плану образовательной программы)

Методическая комиссия	**№ протокола, дата**	**Председатель МК**
ИПСУБ	№ 3 от 10.02.2021 г.	Кайшев А.В.

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Программа практики составлена в соответствии с требованиями ФГОС ВО ФГОС ВО по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки РФ от 26.11.2020 г. № 1461.

1. Указание вида практики, способа и формы (форм) ее проведения.

Вид практики: производственная

Тип практики: эксплуатационная
Способ проведения практики: стационарная, выездная

Форма (формы) проведения: непрерывная

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.

Соотнесение планируемых результатов обучения при прохождении практики с планируемыми результатами освоения образовательной программы (компетенции из учебного плана) представлено в таблице 1.

Таблица 1

Планируемые результаты освоения ОП (компетенции)		**Планируемые результаты обучения при прохождении практики**		
Код	**Содержание компетенции**	**Знания**	**Умения**	**Навыки, опыт деятельности** *(по производственной практике)*
ОПК-8	Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ОПК-8.1.1 знает технологии обеспечения информационной безопасности, способы их организации и оптимизации	ОПК-8.2.5 умеет пользоваться нормативными документами в области технической защиты информации	ОПК-8.3.1 владеет навыками выявления и устранения угроз информационной безопасности ОПК-8.3.4 владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ

3. Указание места практики в структуре образовательной программы:

Дисциплины, на освоении знаний которых базируется практика:

- Защита информационных процессов в компьютерных системах;
- Стандарты информационной безопасности;
- Корпоративная защита от внутренних и внешних угроз
- Аттестация объектов информатизации
- комплексная система защита информации
- администрирование отечественных операционных систем

4. Указание объема практики в зачетных единицах и ее продолжительности в неделях (либо в астрономических часах).

Общий объем практики составляет 6 зачетных единиц, 216 академических часов, контактная работа – 4 час

Продолжительность практики 4 недели.

5. Содержание практики:

Цель практики:

- ознакомить студентов с основными видами и задачами будущей профессиональной деятельности;

- применить полученные при обучении теоретические и практические знания на практике;

- способствовать ознакомлению студентов с использованием профильных дисциплин при проектировании систем защиты информации и комплексов обеспечения информационной безопасности;

- расширить практические представления студентов об объектах профессиональной деятельности.

Задачи практики:

4. овладение профессиональными навыками работы при решении практических задач;
5. выбор направления практической работы;
6. приобретение опыта работы в коллективе;
7. подготовка студентов к последующему осознанному изучению профессиональных, в том числе профильных дисциплин;

8. ознакомление с применяемыми техническими средствами защиты конфиденциальной информации;

9. сбор материала для написания выпускной квалификационной работы.

База проведения практики:

Местом прохождения производственной практики могут служить государственные, коммерческие и некоммерческие организации; информационные подразделения предприятий различных сфер деятельности, а также научно-производственные организации.

Общие задания по практике (виды работ, выполняемые в ходе практики):

руководителями практики от института и предприятия выдается практиканту индивидуальное задание, связанное с выполняемой работой в отделе (службе) и с темой ВКР, направленное на углубленную разработку отдельных его частей.

Этапы прохождения практики:

1.Подготовительный этап:

До начала прохождения практики руководителем практики со стороны университета обозначаются перед студентами конкретные задачи их практической деятельности, структура плана индивидуальной работы, форма и содержание отчетной документации.

Со стороны руководителя практики организации проводится инструктаж по ОТ и пожарной безопасности

2.Ознакомительный этап включает знакомство с базой практики, с нормативной документацией, предметом деятельности.

3.Основной этап прохождения практики состоит из выполнения заданий практики: общих и индивидуальных, определяемых руководителями практик со стороны организации и университета.

4. Заключительный этап включает подготовку студентами отчетных документов по практике (индивидуальная книжка обучающего по практике, отчет о проделанной работе) и защита отчета по практике.

6. Указание форм отчетности по практике:

Виды и формы текущего контроля прохождения практики обучающегося диффе-

ренцированный зачет

Виды и формы итоговой отчетности индивидуальная книжка по практике обучающегося и отчет о проделанной работе.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике:

Средства оценки сформированности компетенций: отчет о проделанной работе студента, отзыв руководителя со стороны организации где студент проходил практику.

Виды заданий для оценки уровня компетенций: решение задач в соответствии с индивидуальным планом практики.

Виды работ для оценки уровня компетенций: отчет о практике должен содержать сведения о выполненных студентом работах в период практики (результаты исследований с последующими выводами), техническое задание на выполнение выпускной квалификационной работы.

Форма технического задания на выполнение выпускной квалификационной работы

УТВЕРЖДАЮ
Зав. кафедрой информационной безопасности
в управлении
доцент, д.ю.н. Г.Г.Камалова
_____
«_____» _____ 20___ г.

Техническое задание
на выполнение выпускной квалификационной работы
студента ____ курса очной формы обучения специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»
«_____»
ФИО
«ТЕМА»

17 **Основание для выполнения:**

- федеральный государственный образовательный стандарт высшего образования по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

- п.___приказа ФГБОУ ВО УдГУ от _____ г. № ____ «О закреплении тем выпускных квалификационных работ»

18 **Цель работы**

19 **Задачи работы**

20 **Исходные данные для проведения работы:**

21 **План работы:**

Срок представления работы «_____» _____ 20____г.

Научный руководитель И. О.Ф

Студент И.О.Ф

Уровни сформированности компетенций

- **пороговый уровень** дает общее представление о практической деятельности, умеет использовать знания о выполнении практических действий, умеет выполнять отдельные операции по виду деятельности, овладел некоторыми, методами и способами решения практических задач (соответствует оценке «**удовлетворительно»**);

- **базовый** позволяет решать типовые задачи, принимать профессиональные и управленческие решения, овладел основными навыками практической деятельности, приобрел опыт профессиональной деятельности, умеет принимать профессиональные и управленческие решения, умеет разрешать возникающие трудности в процессе выполнения деятельности (соответствует оценке «**хорошо**»);

- **повышенный уровень** предполагает готовность решать практические профессиональные задачи повышенной сложности, овладел всеми компонентами компетенции и приобрел высокий опыт деятельности, без затруднений решает возникающие трудности в процессе прохождения практики, овладел способностью принимать профессиональные и управленческие решения (соответствует оценке «**отлично»**).

8. Учебно-методическая литература и ресурсы сети Интернет, необходимых для проведения практики:

Основная литература:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использо-

вании информационно-телекоммуникационных сетей международного информационного обмена».
Указ Президента РФ от 05 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
Указ Президента РФ от 31 декабря 2015 № 683 «О Стратегии национальной безопасности Российской Федерации».
Постановление Правительства Российской Федерации от 3 ноября 1994 № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г.
Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992.
Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден Гостехкомиссией России, 1992. .
Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.
Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.
Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.
ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
ГОСТ Р 56546-2015 Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

ГОСТ Р 56545-2015 Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.
ГОСТ Р 54583-2011/ISO/IEC/TR 15443-3:2007 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия.
ГОСТ Р 54582-2011/ISO/IEC/TR 15443-2:2005 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия.
ГОСТ Р 53647.6-2012 Национальный стандарт Российской Федерации. Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных.
ГОСТ Р 53114-2008 Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
ГОСТ Р 53113.1-2008 Национальный стандарт Российской Федерации. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.
ГОСТ Р 53113.2-2009 Национальный стандарт Российской Федерации. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.
ГОСТ Р 51275-2006 Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
ГОСТ Р ИСО/МЭК 15408-3-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
ГОСТ Р ИСО/МЭК 15408-2-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
ГОСТ Р ИСО/МЭК 18045-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
ГОСТ Р 50922-2006 Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.
ГОСТ Р 52069.0-2013 Национальный стандарт Российской Федерации. Защита информации. Система стандартов. Основные положения.

ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998.
ГОСТ Р 51241-98 Защита информации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Госстандарт России, 1998.
ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Ростехрегулирование, 2006.
ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Росстандарт, 2012.
ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по реализации системы менеджмента информационной безопасности. Росстандарт, 2012.
ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Госстандарт СССР, 1990.
ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Интернет-ресурсы:

www.fstec.ru; www.gost.ru; http://protect.gost.ru.

9. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости):

Информационные технологии используемые в организации для обеспечения функционирования процессов.
Программное обеспечение, используемое в организации в части обеспечения информационной безопасности.
Информационные справочные системы СПС «Консультант Плюс», «Гарант»

10. Описание материально-технической базы, необходимой для проведения практики:

Место проведения практики: структурные подразделения в организации (рабочее место)
Материально-техническое обеспечение практики: ресурсы организации, где студент проходит практику

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Удмуртский государственный университет»

ИНСТИТУТ ПРАВА, СОЦИАЛЬНОГО УПРАВЛЕНИЯ И БЕЗОПАСНОСТИ

«Утверждаю»
Директор института
_____ /_____/
подпись, ФИО
«17» февраля 2021 г.

ПРОГРАММА ПРАКТИКИ
производственная практика (преддипломная)

Специальность 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

Специализация «технологии защиты информации в правоохранительной сфере

Квалификация выпускника специалист по защите информации

Курс 5, семестр 10

Формы обучения очная

прием 2021/2022

Разработчик(и) программы практики

ФИО	Ученая степень, звание, должность	Контактная информация (служебныеE-mail и телефон)
Камалова Г.Г	Доцент, дюн кафедры информационной безопасности в управлении	916-004

Экспертиза рабочей программы

Первый уровень
(оценка качества содержания программы, соответствие целям и задачам ООП ВО)

Руководитель ООП ВО	Подпись руководителя ООО ВО
Зам. директора по учебной работе	Лапшина Л.П.

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Второй уровень
(оценка качества содержания программы и применяемых педагогических технологий)

Наименование кафедры	№ протокола, дата	Зав. кафедрой
Кафедра информационной безопасности в управлении	№ 6 от 02.02.2021 г.	Камалова Г.Г

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Третий уровень
(соответствие целям подготовки и учебному плану образовательной программы)

Методическая комиссия	№ протокола, дата	Председатель МК
ИПСУБ	№ 3 от 10.02.2021 г.	Кайшев А.В.

Выписка из решения:
Программа практики составлена в соответствии с требованиями ФГОС ВО специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки от 26.11.2020 г. № 1461. Составители учли все рекомендации УМУ УдГУ. Программа рекомендуется к использованию в учебном процессе.

Программа практики составлена в соответствии с требованиями ФГОС ВО ФГОС ВО по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного Приказом Минобрнауки РФ от 26.11.2020 г. № 1461

1. Указание вида практики, способа и формы (форм) ее проведения.

Вид практики: производственная

Тип практики: преддипломная

Способ проведения практики: стационарная

Форма (формы) проведения: непрерывная

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.

Соотнесение планируемых результатов обучения при прохождении практики с планируемыми результатами освоения образовательной программы (компетенции из учебного плана) представлено в таблице 1.

Таблица 1

Планируемые результаты освоения ОП (компетенции)		**Планируемые результаты обучения при прохождении практики**		
Код	**Содержание компетенции**	**Знания**	**Умения**	**Навыки, опыт деятельности** *(по производственной практике)*
ОПК-10	ОПК-10. Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач	ОПК-10.1.1 знает принципы	ОПК-10.2.1умеет делать	ОПК-10.3.1 владеет навыками применения автоматизированных средств сбора и анализа информации, основанных на технологиях OSINT и data mining ОПК-10.3.2 владеет навыками анализа надежности защиты информационных систем ОПК-10.2.2 _____
ОПК-5	Способен планировать проведение работ по комплексной защите информации на объекте информатизации	ОПК-5.1.2 знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	ОПК-5.2.2 умеет определить политику контроля доступа работников к информации ограниченного доступа ОПК-5.2.3 умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному	ОПК-5.2.1 ____ умеет ра

Планируемые результаты освоения ОП (компетенции)		Планируемые результаты обучения при прохождении практики		
Код	**Содержание компетенции**	**Знания**	**Умения**	**Навыки, опыт деятельности** *(по производственной практике)*
		ОПК-5.1.1 знает принципы формирования политики информационной безопасности в информационных системах;	режиму в организации	
ОПК-8	Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками ОПК-8.1.2 знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации	ОПК-8.2.2 умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности ОПК-8.1.5 знает методы анализа процессов для определения актуальных угроз	ОПК-8.3.2 _____

3. Указание места практики в структуре образовательной программы:

Преддипломная практика базируется на знаниях, полученных в рамках изученных дисциплин образовательной программы, в рамках преддипломной практики выполняется выпускная квалификационная работа.

4. Указание объема практики в зачетных единицах и ее продолжительности в неделях (либо в астрономических часах).

Общий объем практики составляет 12 зачетных единиц, 432 академических часов.

В том числе:

1. Объем контактной работы с руководителем практики от кафедры составляет 8 час

Продолжительность практики 8 недель.

5. Содержание практики:

Цель практики: приобретение практических навыков обеспечения защиты информации на предприятия различных форм собственности и выполнение выпускной квалификационной работы.

Задачи практики:

- исследование процессов организации с целью выявлению объектов защиты, угроз и уязвимостей информационных систем,
- анализ нормативно-правовых актов и лучших практик, методов и средств защиты информации от выявленных угроз и уязвимостей,
- разработка предложений в части организационных и технических мер защиты информации с учетом выявленных угроз и уязвимостей.

База проведения практики:

Местом прохождения производственной практики могут служить государственные, коммерческие и некоммерческие организации; информационные подразделения предприятий различных сфер деятельности, а также научно-производственные организации. Договоры на проведение практики заключены:

Министерство информатизации и связи Удмуртской Республики

Администрация г.Ижевска

Администрации МО

АУ УР «Ресурсный информационный центр Удм.Республики»

Министерство Внутренних Дел УР

Управление Судебного Департамента в УР

Управление Федеральной Налоговой Службы РФ по УР

Кафедра информационной безопасности в управлении ФГБОУ ВО "Удмуртского государственного университета"

Общие задания по практике (виды работ, выполняемые в ходе практики):

руководителями практики от института и предприятия выдается практиканту индивидуальное задание, связанное с темой ВКР, направленное на углубленную разработку отдельных его частей.

Этапы прохождения практики:

1.Подготовительный этап:

До начала прохождения практики руководителем практики со стороны университета обозначаются перед студентами конкретные задачи их практической деятельности, структура плана индивидуальной работы, форма и содержание отчетной документации.

Со стороны руководителя практики организации проводится инструктаж по ОТ и пожарной безопасности

2.Ознакомительный этап включает знакомство с базой практики, с нормативной документацией, предметом деятельности, сбор и систематизация материала для выполнения выпускной квалификационной работы.

3.Основной этап прохождения практики состоит из выполнения заданий практики: общих и индивидуальных, определяемых руководителями практик со стороны организации и университета, оформление выпускной квалификационной работы.

4. Заключительный этап включает подготовку студентами отчетных документов по практике (индивидуальная книжка обучающего по практике, отчет о проделанной работе, проект выпускной квалификационной работы) и защита отчета по практике.

6. Указание форм отчетности по практике:

Виды и формы текущего контроля прохождения практики обучающегося дифференцированный зачет

Виды и формы итоговой отчетности индивидуальная книжка по практике обучающегося и отчет о проделанной работе.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике:

Средства оценки сформированности компетенций: отчет о проделанной работе студента, отзыв руководителя со стороны организации где студент проходил практику.

Виды заданий для оценки уровня компетенций: проект выпускной квалификационной работы

Виды работ для оценки уровня компетенций: отчет о практике должен содержать сведения о выполненных студентом работах в период практики (результаты исследований с последующими выводами).

Уровни сформированности компетенций

- **пороговый уровень** дает общее представление о практической деятельности, умеет использовать знания о выполнении практических действий, умеет выполнять отдельные операции по виду деятельности, овладел некоторыми, методами и способами решения практических задач (соответствует оценке «удовлетворительно»);
- **базовый** позволяет решать типовые задачи, принимать профессиональные и управленческие решения, овладел основными навыками практической деятельности, приобрел опыт профессиональной деятельности, умеет принимать профессиональные и управленческие решения, умеет разрешать возникающие трудности в процессе выполнения деятельности (соответствует оценке «хорошо»);
- **повышенный уровень** предполагает готовность решать практические профессиональные задачи повышенной сложности, овладел всеми компонентами компетенции и приобрел высокий опыт деятельности, без затруднений решает возникающие трудности в процессе прохождения практики, овладел способностью принимать профессиональные и управленческие решения (соответствует оценке «отлично»).

8. Учебно-методическая литература и ресурсы сети Интернет, необходимых для проведения практики:

Основная литература:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
Указ Президента РФ от 05 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
Указ Президента РФ от 31 декабря 2015 № 683 «О Стратегии национальной безопасности Российской Федерации».
Постановление Правительства Российской Федерации от 3 ноября 1994 № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г.
Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992.
Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден Гостехкомиссией России, 1992. .
Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.
Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.
Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.
ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
ГОСТ Р 56546-2015 Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.
ГОСТ Р 56545-2015 Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.
ГОСТ Р 54583-2011/ISO/IEC/TR 15443-3:2007 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия.
ГОСТ Р 54582-2011/ISO/IEC/TR 15443-2:2005 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия.

ГОСТ Р 53647.6-2012 Национальный стандарт Российской Федерации. Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных.
ГОСТ Р 53114-2008 Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
ГОСТ Р 53113.1-2008 Национальный стандарт Российской Федерации. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.
ГОСТ Р 53113.2-2009 Национальный стандарт Российской Федерации. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.
ГОСТ Р 51275-2006 Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
ГОСТ Р ИСО/МЭК 15408-3-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
ГОСТ Р ИСО/МЭК 15408-2-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
ГОСТ Р ИСО/МЭК 18045-2013 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
ГОСТ Р 50922-2006 Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.
ГОСТ Р 52069.0-2013 Национальный стандарт Российской Федерации. Защита информации. Система стандартов. Основные положения.
ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998.
ГОСТ Р 51241-98 Защита информации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Госстандарт России, 1998.
ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Ростехрегулирование, 2006.
ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Росстандарт, 2012.
ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по реализации системы менеджмента информационной безопасности. Росстандарт, 2012.
ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Госстандарт СССР, 1990.
ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Интернет-ресурсы:

www.fstec.ru; www.gost.ru; http://protect.gost.ru.
Электронно-библиотечная система Znaniumhttp://www.znanium.com
Научная электронная библиотека eLibrary.ruhttp://elibrary.ru
Электронно-библиотечная система BOOK.RUhttp://www.book.ru
Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/

9. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости):

Информационные технологии используемые в организации для обеспечения функционирования процессов.

Программное обеспечение, используемое в организации в части обеспечения информационной безопасности.
Информационные справочные системы СПС «Консультант Плюс», «Гарант»**10. Описание материально-технической базы, необходимой для проведения практики:**
Место проведения практики: структурные подразделения в организации (рабочее