Утверждена в составе Основной
профессиональной образовательной
программы высшего образования

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Тип практики

эксплуатационная практика

Направление подготовки (специальность)

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направленность (профиль) программы

«направленность (профиль) N 7 "Техническая защита информации"»

1. Общие положения.

Программа производственной практики: эксплуатационная практика (далее – производственная практика) разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) по направлению подготовки (специальности) 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (утв. приказом Минобрнауки России от 01.12.2016 № 1515), локальными актами Университета.

2. Место практики в структуре основной профессиональной образовательной программы, объем практики.

Производственная практика относится к вариативной части учебного плана основной профессиональной образовательной программы (далее – ОПОП) по направлению подготовки (специальности) 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, направленность (профиль) «направленность (профиль) N 7 "Техническая защита информации"».

Объем практики составляет 3 зачетных единицы (далее - з.е.), или 108 академических часов.

3. Вид, способы и формы проведения практики; базы проведения практики.

Вид практики – производственная

Тип практики – эксплуатационная практика – определяется видами профессиональной деятельности, к которым готовится обучающийся в соответствии с ФГОС ВО и ОПОП.

Способы проведения практики (при наличии) – стационарная, выездная

Формы проведения практики: дискретно по видам практики

Базами проведения практики являются профильные организации, в том числе их структурные подразделения, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках ОПОП, на основании договоров, заключенных между Университетом и профильными организациями.

Практика может быть организована непосредственно в Университете, в том числе в его структурном подразделении.

Для руководства практикой, проводимой в Университете, обучающемуся назначается руководитель практики от Университета.

Для руководства практикой, проводимой в профильной организации, назначаются руководитель практики от Университета и руководитель практики от профильной организации.

4. Цели и задачи практики. Планируемые результаты обучения при прохождении практики.

Цель практики определяется видами профессиональной деятельности и компетенциями, которые должны быть сформированы у обучающегося в соответствии с ОПОП.

Цель (-и) практики:

Закрепление, расширение, углубление и систематизация знаний, умений и навыков, полученных при изучении дисциплин профессионального цикла базовой и вариативной частей, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта. Производственная практика обеспечивает последовательность процесса формирования у студентов системы профессиональных компетенций в соответствии с профилем подготовки бакалавров, прививает студентам навыки самостоятельной работы по избранной профессии, дает возможность определения темы курсовой работы и ее выполнения.

Задачи практики:

- закрепление и расширение теоретических и практических знаний;
- развитие профессиональных навыков и навыков деловой коммуникации;
- изучение информационной структуры предприятия, как объекта информатизации;
- сбор необходимых материалов для написания отчета по практике;
- проведение анализа и обобщения результатов собственных исследований;
- получение практических данных, для написания курсовой работы, приобретения навыков их обработки.

Данные задачи производственной практики, соотносятся со следующими видами и задачами профессиональной деятельности:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;

администрирование подсистем информационной безопасности объекта;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

проведение экспериментов по заданной методике, обработка и анализ результатов;

проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей с учетом требований защиты информации;

совершенствование системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;

контроль эффективности реализации политики информационной безопасности объекта.

Производственная практика направлена на формирование следующих общекультурных, общепрофессиональных, профессиональных компетенций обучающегося в соответствии с выбранными видами профессиональной деятельности, к которым готовятся обучающийся в соответствии с ОПОП:

Планируемые результаты обучения при прохождении практики, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование компетенции	Планируемые результаты обучения

ОК-6 Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия ОПК-5 Способность использовать нормативные правовые акты в профессиональной деятельности ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПК-3 Способность администрировать подсистемы информационной безопасности объекта защиты ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПК-9 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности ПК-10 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-11 Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов ПК-12 Способность принимать участие в проведении экспериментальных исследований системы защиты информации	Знать: должностные обязанности сотрудников в области защиты информации; основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ; основные понятия и методы в области управленческой деятельности; аппаратные средства вычислительной техники; операционные системы, основы администрирования вычислительных сетей; системы управления базами данных; современные средства разработки и анализа программного обеспечения, операционные системы, правовые нормы по вопросам сертификации и лицензирования в области защиты информации; принципы организации информационных систем в соответствии с требованиями по защите информации; криптографические стандарты и их использование в информационных системах; принципы формирования политики информационной безопасности в информационных системах; основные методы управления информационной безопасностью; основные подходы к анализу исходных данных и проектированию системы защиты информации; основные методики оценки рисков и проведения технико-экономического обоснования; свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления; задачи органов защиты информации на предприятиях; организацию работы и нормативные правовые акты по сертификации средств защиты информации; основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности; классификацию и особенности применения технических средств защиты информации от утечки по техническим каналам; классификацию и особенности применения технических средств защиты информации от несанкционированного доступа и средства антивирусной защиты. Уметь: работать в команде, распределять обязанности по выполнению работ; использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации, нести персональную ответственность за нарушения нормативно-правовых требований, предпринимать необходимые меры по восстановлению нарушенных прав; настраивать и обслуживать средства защиты информации; применять программные средства системного, прикладного и специального назначения; развертывать, конфигурировать и настраивать вычислительные сети; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; применять отечественные и

	зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; разрабатывать частные политики информационной безопасности информационных систем; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем; оценивать информационные риски в информационных системах; проводить расчеты для технико-экономического обоснования проектных решений разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; квалифицированно исследовать состав документации предприятии (организации); разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по профилю своей деятельности; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности; устанавливать и настраивать технические средства защиты информации от утечки по техническим каналам; устанавливать и настраивать технические средства защиты информации от несанкционированного доступа и средства антивирусной защиты. Владеть: навыками командной работы, способностью выражать свои мысли и мнения в деловой форме общения; навыками быстрого поиска законодательных требований в информационных источниках; навыками принятия решений, навыками дискуссии по профессиональной тематике; навыками работы использования технических средств идентификации и проверки подлинности пользователей компьютерных систем, навыками проведения оценки защищенности помещений от утечки; навыками защиты от разрушающих программных воздействий; навыками рационального выбора средств и методов защиты информации объектов информатизации; навыками настройки и администрирования распространенных операционных систем и вычислительных сетей, построенных на их основе; навыками использования типовых криптографических алгоритмов; методами формирования требований по защите информации; навыками представления результатов научных исследований по вопросам обеспечения информационной безопасности по профилю своей деятельности с использованием современных технических средств в устной и письменной формах.

5. Содержание практики.

Производственная практика проходит в три этапа:

подготовительный (ознакомительный), основной, заключительный.

№ п/п	Этапы практики и их содержание
Подготовительный (ознакомительный) этап	
Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации, прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка. Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики.	
Основой этап	
Ознакомление с деятельностью предприятия. Определение методов и средств защиты информации, используемых на предприятии. Выполнение практических заданий. Сбор материалов для отчетной документации. Производственная практика предполагает: производственный инструктаж; выполнение производственных заданий; сбор, обработка и систематизация фактического и литературного материала; наблюдения; измерения и другие, выполняемые обучающимся самостоятельно виды работ. На каждом рабочем месте проводится инструктаж по ТБ. Студент должен усвоить полученный материал и расписаться в соответствующем журнале. Находясь на практике, студент подчиняется правилам внутреннего распорядка, установленным для работников предприятия. В начале практики руководитель от предприятия совместно со студентом составляют краткий план прохождения практики с учетом тематики примерных практических заданий рекомендованных данной программой практики, профилем и технической оснащенностью данного предприятия. План прохождения практики согласовывается с руководителем практики от Университета. Производственная практика предполагает непосредственное участие студентов в деятельности предприятия. Студент обязан добросовестно и качественно выполнять порученную ему работу. Методическое и консультационное обеспечение осуществляет руководитель практики от Университета или заведующий кафедрой информационной безопасности.	
Заключительный этап	
Подготовка отчетной документации, получение характеристики о работе и (или) характеристики – отзыва руководителя практики от университета, представление отчетной документации на кафедру, прохождение промежуточной аттестации по практике. Систематизация и анализ выполненных заданий.	

6. Формы отчетности по практике.

Формой промежуточной аттестации по практике является зачет с оценкой.

По результатам прохождения практики обучающийся представляет, следующую отчетную документацию:

- дневник производственной практики;
- отчет о прохождении производственной практики;
- материалы практики (при наличии);

Руководитель практики от Университета представляет характеристику – отзыв. Руководитель практики от профильной организации представляет характеристику работы обучающегося.

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

Фонд оценочных средств представлен в приложении к программе практики (Приложение 1).

8. Учебная литература и ресурсы сети Интернет.

а) основная литература:

Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. ;Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=362895

Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. ;Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=276557

Носов Л.С. Техническая защита информации [Электронный ресурс] : Учебное пособие. Ч. 1 : Инженерно-техническая защита информации / Л. С. Носов, А. Р. Биричевский. - Сыктывкар : Изд-во СыктГУ, 2012. - 77 с.URL:http://e-library.syktsu.ru/megapro/Download/MObject/343/978-5-87237-830-3 Носов Л.С., Биричевский А.Р. Техническая защита информации. Часть 1. Инженерно-техническая защита информации. Учебное пособие.pdf

Носов Л.С. Техническая защита информации [Электронный ресурс] : Учебное пособие. Ч. 2 : Техническая защита информации / Л. С. Носов, А. Р. Биричевский, Д. Н. Едомский. - Сыктывкар : Изд-во СыктГУ, 2012. - 78 с.URL:http://e-library.syktsu.ru/megapro/Download/MObject/344/978-5-87237-831-0 Носов Л.С., Биричевский А.Р. Техническая защита информации. Часть 2. Технические средства защиты информации. Учебное пособие.pdf

Титов, А.А. Технические средства защиты информации : учебное пособие / А.А. ;Титов. – Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 194 с. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=208661

Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. ;Бурькова ; Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. – Оренбург : Оренбургский государственный университет, 2017. – 158 с. : табл., схем. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=481730

Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А.М. ;Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=480636

Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. ;Громов, О.Г. ;Иванова, К.В. ;Стародубов, А.А. ;Кадыков ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=499013

Аверченков, В.И. Аудит информационной безопасности: учебное пособие для вузов / В.И. ;Аверченков. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 269 с. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=93245

Методологические основы построения защищенных автоматизированных систем : учебное пособие / А.В. ;Душкин, О.В. ;Ланкин, С.В. ;Потехецкий и др. ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2013. – 258 с. : табл., ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=255851

Инструментальный контроль и защита информации : учебное пособие / Н.А. ;Свинарев, О.В. ;Ланкин, А.П. ;Данилкин и др. ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2013. – 192 с. : табл., ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=255905

б) дополнительная литература:

Монаппа, К. А. Анализ вредоносных программ / К. А. Монаппа ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2019. — 452 с. — ISBN 978-5-97060-700-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL:https://e.lanbook.com/book/123709?category=1545

Спицын, В.Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. ;Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. : ил.,табл., схем. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=208694

Артемов, А.В. Информационная безопасность: курс лекций / А.В. ;Артемов ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная

академия безопасности и выживания, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=428605
Иванов, А.В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок : учебное пособие : [16+] / А.В. ;Иванов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 64 с. : ил., табл. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=575420

в) Интернет-ресурсы:

https://elibrary.ru/ – национальная библиографическая база данных научного цитирования (профессиональная база данных)
Системы дистанционного обучения СГУ им. Питирима Сорокина на базе Moodle - http://lms-moodle.syktsu.ru
Сайт ФСТЭК России – www.fstec.ru
Журнал «Безопасность информационных технологий» https://bit.mephi.ru/index.php/bit
Сайт ФСБ России – www.fsb.ru
Журнал «Информация и безопасность» http://kafedrasib.ru/index.php/informatsiya-bezopasnost
Журнал «Труды СПИРАН» http://proceedings.spiiras.nw.ru/ojs/index.php/sp
Журнал «Бизнес и информационные технологии». – http://bit.samag.ru
Банк данных угроз ФСТЭК России https://bdu.fstec.ru
Справочная правовая система «КонсультантПлюс» www.consultant.ru
Журнал «Системный администратор» http://samag.ru/
Портал ИСПДн.РУ http://www.ispdn.ru
Среда электронного обучения СГУ им. Питирима Сорокина http:// http://eios.syktsu.ru/
Основы теории информации и криптографии https://www.intuit.ru/studies/courses/2256/140/info
Журнал «Информационные технологии». – http://www.novtex.ru/IT
Журнал «Информационные технологии и вычислительные системы». – http://www.jitcs.ru
Журнал «Прикладная информатика». – http://www.appliedinformatics.ru

г) периодические издания и реферативные базы данных (при необходимости):

9. Информационные технологии, используемые при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости).

Система управления обучением Moodle, операционная система MS Windows 7 и выше; программные средства, входящие в состав офисного пакета MS Office (Word, Excel, Access, Publisher, PowerPoint); программы для просмотра документов, графические редакторы, браузеры, справочно-правовая система «Консультант Плюс».

10. Материально-техническая база, необходимая для проведения практики.

Материально-техническая база проведения практики представляет собой оборудование и технические средства обучения в объеме, позволяющем выполнять виды работ в соответствии с видом (-ами) профессиональной деятельности, к которому (-ым) готовится обучающиеся в результате освоения ОПОП в соответствии с ФГОС ВО.3

Сведения о материально-технической базе практики содержатся в справке о материально-технических условиях реализации образовательной программы.

11. Особенности организации практики для обучающихся с ограниченными возможностями здоровья и инвалидов.

Организация практики для обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется в соответствии с законодательством Российской Федерации.

Для обучающихся с ограниченными возможностями здоровья и инвалидов выбор места и способ прохождения практики устанавливается Университетом с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья, а также требований по доступности.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике.

Промежуточная аттестация по практике представляет собой комплексную оценку формирования, закрепления, развития практических навыков и компетенций по профилю образовательной программы, связанных с видом (-ами) профессиональной деятельности, к выполнению которых готовятся обучающиеся в соответствии с ОПОП.4

Фонд оценочных средств предназначен для оценки:

1) уровня освоения компетенций, соответствующих этапу прохождения практики;

2) соответствия запланированных и фактически достигнутых результатов освоения практики каждым студентом.

Критерии оценивания результатов промежуточной аттестации обучающихся по практике (с учетом характеристики работы обучающегося и/или характеристики – отзыва):

Форма промежуточной аттестации – «дифференцированный зачет» (зачет с оценкой)

Критерии оценивания	
Отлично	обучающийся выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, показал глубокую теоретическую, методическую, профессионально-прикладную подготовку, умело применил полученные знания во время прохождения практики, показал владение современными методами исследования профессиональной деятельности, использовал профессиональную терминологию, ответственно относился к своей работе; отчет по практике соответствует предъявляемым требования.
Хорошо	обучающийся выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, однако допустил несущественные ошибки, показал глубокую теоретическую, методическую, профессионально-прикладную подготовку, умело применил полученные знания во время прохождения практики, показал владение современными методами исследования профессиональной деятельности, использовал профессиональную терминологию, ответственно относился к своей работе; отчет по практике в целом соответствует предъявляемым требования, однако имеются несущественные ошибки в оформлении
Удовлетворительно	обучающийся выполнил индивидуальное задание в соответствии с программой практики, однако допустил существенные ошибки (могут быть нарушены сроки выполнения индивидуального задания), в процессе работы не проявил достаточной самостоятельности, инициативы и заинтересованности, демонстрирует недостаточный объем знаний и низкий уровень их применения на практике; низкий уровень владения профессиональной терминологией и методами исследования профессиональной деятельности; допущены значительные ошибки в оформлении отчета по практике.

Неудовлетворительно	обучающийся не выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, показал низкий уровень теоретической, методической, профессионально-прикладной подготовки, не применяет полученные знания во время прохождения практики, не показал владение современными методами исследования профессиональной деятельности, не использовал профессиональную терминологию,; отчет по практике не соответствует предъявляемым требования.

Виды контролируемых работ и оценочные средства

№п/п	Виды контролируемых работ по этапам	Код контролируемой компетенции (части компетенции)	Оценочные средства
1.	Подготовительный (ознакомительный) этап Допуске к прохождению практики (отметка в журнале инструктажа). Присутствие на установочной конференции.	ОК-6 ОПК-5 ПК-1 ПК-2 ПК-3 ПК-4 ПК-7 ПК-8 ПК-9 ПК-10 ПК-11 ПК-12	Дневник практики, отчет о прохождении практики, материалы практики (при наличии)
2.	Основной этап Пошаговый анализ выполнения практических заданий. Оформление отчетной документации. Согласование отчета с руководителем практики от предприятия. Примерные практические задания: 1. ознакомиться с историей, традициями и сферами деятельности предприятия согласно уставу или положению о предприятии и пройти инструктаж по технике безопасности на рабочем месте; 2. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 3. определить виды информации ограниченного доступа, обрабатываемые предприятием; 4. ознакомиться с формами организации производственного процесса и его технологическим обеспечением; 5. выявить угрозы безопасности предприятия; 6. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 7. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 8. изучить методы и средства защиты информации, применяемые на предприятии; 9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических		

	средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 10. разработать модель угроз для конкретной информационной системы предприятия; 11. изучить основные обязанности должностных лиц в области защиты информации; 12. проанализировать методы контроля в области защиты информации, используемые в организации; 13. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 14. предложить перечень мероприятий по улучшению системы защиты информации на предприятии. 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 19. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 20. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 21. спроектировать систему физической защиты информации; 22. разработать политику информационной безопасности предприятия; 23. проанализировать систему компьютерной безопасности предприятия; 24. изучить систему контроля и управления доступом предприятия; 25. ознакомиться с системой защиты персональных данных в организации; 26. изучить виды правонарушений при совершении компьютерных преступлений;		
3.	Заключительный этап Анализ отчетной документации за период практики. Отчет о прохождении практики на итоговой конференции. Оценка работы. Отчет		

	оформляется с помощью печатающих устройств на одной стороне листа бумаги формата А4. Размер шрифта 12-14 через 1-1,5 интервала. При написании текста следует оставлять поля слева - 30 мм, справа - 10 мм, сверху и снизу - 20 мм. Все страницы должны иметь сквозную нумерацию: первой страницей является титульный лист. На титульном листе номер не ставится. Номер страницы проставляется в низу по центру. Отчет о практике является обязательным документом студентов-практикантов. По форме он должен включать титульный лист и текст отчета. Отчет обязательно должен содержать не только информацию о выполнении заданий программы практики, но и анализ этой информации, выводы и рекомендации, разработанные каждым студентом самостоятельно. Оформленный итоговый отчет должен быть сброшюрован в папку со скоросшивателем. Титульный лист должен быть подписан руководителями практики и студентом-практикантом. Отчёт может содержать приложения: - материалы, собранные студентом в период прохождения практики (копии нормативно правовых и организационных документов, а также те документы, в составлении которых студент, принимал непосредственное участие в объёме, предусмотренном заданием); - схемы, таблицы, аналитические расчёты, статистические данные, иллюстрации и т.п. Отчет готовится в течение всей практики и проверяется преподавателем-руководителем практики до защиты практики. Оформленный отчет о практике, подлежит обязательной защите студентом в установленные сроки. Аттестация по итогам производственной практики проводится на основании материалов отчета о практике, дневника производственной практики и листа экспертной оценки, оформленных в соответствии с установленными требованиями. Прием зачета по практике производит комиссия. В состав комиссии входят заведующий кафедрой, руководитель практики от Университета, руководитель практики от предприятия и другие преподаватели, назначенные распоряжением директора института.		

	По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).		

Утверждена в составе Основной
профессиональной образовательной
программы высшего образования

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

Тип практики

практика по получению первичных профессиональных умений и навыков

Направление подготовки (специальность)

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направленность (профиль) программы

«направленность (профиль) N 7 "Техническая защита информации"»

1. Общие положения.

Программа учебной практики: практика по получению первичных профессиональных умений и навыков (далее – учебная практика) разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) по направлению подготовки (специальности) 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (утв. приказом Минобрнауки России от 01.12.2016 № 1515), локальными актами Университета.

2. Место практики в структуре основной профессиональной образовательной программы, объем практики.

Учебная практика относится к вариативной части учебного плана основной профессиональной образовательной программы (далее – ОПОП) по направлению подготовки (специальности) 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, направленность (профиль) «направленность (профиль) N 7 "Техническая защита информации"».

Объем практики составляет 3 зачетных (-ые) единиц (-ы) (далее - з.е.), или 108 академических часов.

3. Вид, способы и формы проведения практики; базы проведения практики.

Вид практики – учебная

Тип практики – практика по получению первичных профессиональных умений и навыков– определяется видом (-ами) профессиональной деятельности, к которому (-ым) готовится обучающийся в соответствии с ФГОС ВО и ОПОП.

Способы проведения практики (при наличии) – стационарная, выездная

Формы проведения практики: дискретно по периодам проведения практики

Базами проведения практики являются профильные организации, в том числе их структурные подразделения, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках ОПОП, на основании договоров, заключенных между Университетом и профильными организациями.

Практика может быть организована непосредственно в Университете, в том числе в его структурном подразделении.

Для руководства практикой, проводимой в Университете, обучающемуся назначается руководитель практики от Университета.

Для руководства практикой, проводимой в профильной организации, назначаются руководитель практики от Университета и руководитель практики от профильной организации.

4. Цели и задачи практики. Планируемые результаты обучения при прохождении практики.

Цели практики определяются видами профессиональной деятельности и компетенциями, которые должны быть сформированы у обучающегося в соответствии с ОПОП.

Цели практики:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла базовой и вариативной частей, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;

- изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения;

- изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты.

Задачи практики:

- закрепление на практике знаний, умений и навыков, полученных в процессе теоретического обучения;

- развитие профессиональных навыков и навыков деловой коммуникации;

- сбор необходимых материалов для написания отчета по практике.

Данные задачи учебной практики, соотносятся со следующими видами и задачами профессиональной деятельности:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

организационно-управленческая деятельность:

организация работы малых коллективов исполнителей с учетом требований защиты информации.

Учебная практика направлена на формирование следующих общекультурных, общепрофессиональных, профессиональных компетенций обучающегося в соответствии с выбранными видами профессиональной деятельности, к которым готовятся обучающиеся в соответствии с ОПОП:

Планируемые результаты обучения при прохождении практики, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование компетенции	Планируемые результаты обучения
ОК-6 Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия ОПК-5 Способность использовать нормативные правовые акты в профессиональной деятельности ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПК-9 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности ПК-11 Способность проводить эксперименты по	Знать: должностные обязанности сотрудников в области защиты информации; основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ; основные понятия и методы в области управленческой деятельности; виды информации и ее носителей, классификацию угроз информации, уязвимости информации, структуру и содержание информационных процессов предприятия, технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам; аппаратные средства вычислительной техники; операционные системы, основы администрирования вычислительных сетей; системы управления базами данных; современные средства разработки и анализа программного обеспечения, операционные системы, правовые нормы по вопросам сертификации и лицензирования в области защиты информации; свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления; задачи органов защиты информации на предприятиях; организацию работы и нормативные правовые акты по сертификации средств защиты информации;

заданной методике, обработку, оценку погрешности и достоверности их результатов ПК-12 Способность принимать участие в проведении экспериментальных исследований системы защиты информации	основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности; классификацию и особенности применения технических средств защиты информации от несанкционированного доступа и средства антивирусной защиты. Уметь: работать в команде, распределять обязанности по выполнению работ; использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации, нести персональную ответственность за нарушения нормативно-правовых требований, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и оценивать угрозы информационной безопасности объекта; разрабатывать нормативно-методические документы по защите информации; настраивать и обслуживать средства защиты информации; применять программные средства системного, прикладного и специального назначения; квалифицированно исследовать состав документации предприятии (организации); разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по профилю своей деятельности; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности; устанавливать и настраивать технические средства защиты информации от несанкционированного доступа и средства антивирусной защиты. Владеть: навыками командной работы, способностью выражать свои мысли и мнения в деловой форме общения; навыками быстрого поиска законодательных требований в информационных источниках; навыками принятия решений, навыками дискуссии по профессиональной тематике; методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы; навыками работы использования технических средств идентификации и проверки подлинности пользователей компьютерных систем, навыками проведения оценки защищенности помещений от утечки; навыками защиты от разрушающих программных воздействий; навыками рационального выбора средств и методов защиты информации объектов информатизации; навыками представления результатов научных исследований по вопросам обеспечения информационной безопасности по профилю своей деятельности с использованием современных технических средств в устной и письменной формах.

5. Содержание практики.

Учебная практика проходит в три этапа:

подготовительный (ознакомительный), основной, заключительный.

№ п/п	Этапы практики и их содержание
Подготовительный (ознакомительный) этап	
Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации, прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка. Ознакомление с порядком защиты отчета по учебной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики.	
Основой этап	
Выполнение практических заданий. Работа с программным обеспечением. Сбор материалов для отчетной документации. Учебная практика студентов проводится в форме самостоятельной практической работы под руководством преподавателя. Студент при прохождении практики получает от руководителя указания, рекомендации и разъяснения по всем вопросам, связанным с организацией и прохождением практики, отчитывается о выполняемой работе в соответствии с практическим заданием практики. По итогам выполнения каждого практического задания студентом-практикантом составляется отчет о выполнении задания в письменной форме, состоящий из титульного листа и текста отчета: цель работы, ход выполнения работы, вывод. Отчет должен отражать полученные практикантом организационно-технические знания и навыки. Он составляется на основании выполняемой работы, личных наблюдений и исследований. Отчет должен быть выполнен технически грамотно, иллюстрирован эскизами, схемами, фотографиями. Примерный объем отчета 5-6 страниц. Отчет оформляется с помощью печатающих устройств на одной стороне листа бумаги формата А4. Размер шрифта 12-14 через 1-1,5 интервала. При написании текста следует оставлять поля слева - 30 мм, справа - 10 мм, сверху и снизу - 20 мм. Все страницы должны иметь сквозную нумерацию: первой страницей является титульный лист. На титульном листе номер не ставится. Номер страницы проставляется внизу по центру. Отчет о выполнении задания проверяется преподавателем-руководителем практики. Отчет может сдаваться в электронной форме без предоставления печатного варианта.	
Заключительный этап	
Подготовка отчетной документации, получение характеристики о работе и (или) характеристики – отзыва руководителя практики от университета, представление отчетной документации на кафедру, прохождение промежуточной аттестации по практике. По окончании практики студент предоставляет на кафедру итоговый отчет о прохождении учебной практики (далее - отчет), по содержанию включающий в себя результаты выполненных работ. Отчет обязательно должен содержать не только информацию о выполнении заданий программы практики, но и анализ этой информации, выводы и рекомендации, разработанные каждым студентом самостоятельно. Отчет о практике является обязательным документом студентов-практикантов. Оценка результатов по итогам учебной практики проводится на основании материалов отчета о практике, оформленного в соответствии с установленными требованиями. По форме он должен включать титульный лист и текст отчета. Титульный лист должен быть подписан руководителем практики и студентом-практикантом. Оформленный итоговый отчет должен быть сброшюрован в папку со скоросшивателем. Текст отчета должен содержать: 1. содержание 2. описание целей прохождения учебной практики. 3. описание индивидуального задания (постановка целей выполнения). 4. ход выполнения индивидуальных заданий (пояснительный текст, скриншоты). 5. вывод по итогам выполнения индивидуальных заданий. Отчёт может содержать приложения: - материалы, собранные студентом в период прохождения практики (копии нормативно правовых и организационных документов, а также те документы, в составлении которых студент, принимал непосредственное участие в объёме, предусмотренном заданием); - схемы, таблицы, аналитические расчёты, статистические данные, иллюстрации и т.п. Отчет готовится в течение всей практики и проверяется преподавателем-руководителем практики до защиты отчета по практике. Оформленный отчет о практике, подлежит обязательной защите студентом в установленные сроки. По итогам защиты отчета выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).	

6. Формы отчетности по практике.

Формой промежуточной аттестации по практике является зачет с оценкой.

По результатам прохождения практики обучающийся представляет, следующую отчетную документацию:

- отчеты по заданиям (в электронном виде);
- отчет о прохождении учебной практики;
- материалы практики (при наличии);

Руководитель практики от Университета представляет характеристику – отзыв. Руководитель практики от профильной организации представляет характеристику работы обучающегося.

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

Фонд оценочных средств представлен в приложении к программе практики (Приложение 1).

8. Учебная литература и ресурсы сети Интернет.

а) основная литература:

Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз ; перевод с английского А. В. Добровольская. — Москва : ДМК Пресс, 2020. — 308 с. — ISBN 978-5-97060-649-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL:https://e.lanbook.com/book/131682?category=1545

Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL:https://e.lanbook.com/book/131717?category=1545

Сычев, Ю.Н. Основы информационной безопасности: учебно-практическое пособие / Ю.Н. ;Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=90790

Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. ;Громов, О.Г. ;Иванова, К.В. ;Стародубов, А.А. ;Кадыков ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=499013

Методологические основы построения защищенных автоматизированных систем : учебное пособие / А.В. ;Душкин, О.В. ;Ланкин, С.В. ;Потехецкий и др. ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2013. – 258 с. : табл., ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=255851

б) дополнительная литература:

Монаппа, К. А. Анализ вредоносных программ / К. А. Монаппа ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2019. — 452 с. — ISBN 978-5-97060-700-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL:https://e.lanbook.com/book/123709?category=1545

Спицын, В.Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. ;Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. : ил.,табл., схем. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=208694

Артемов, А.В. Информационная безопасность: курс лекций / А.В. ;Артемов ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=428605

в) Интернет-ресурсы:

Системы дистанционного обучения СГУ им. Питирима Сорокина на базе Moodle - http://lms.syktsu.ru

Журнал «Проблемы информационной безопасности. Компьютерные системы» http://jisp.ru/

Сайт ФСТЭК России – www.fstec.ru

Журнал «Безопасность информационных технологий» https://bit.mephi.ru/index.php/bit

Сайт ФСБ России – www.fsb.ru

Журнал «Информация и безопасность» http://kafedrasib.ru/index.php/informatsiya-bezopasnost

Журнал «Труды СПИРАН» http://proceedings.spiiras.nw.ru/ojs/index.php/sp

Банк данных угроз ФСТЭК России https://bdu.fstec.ru

Портал ИСПДн.РУ http://www.ispdn.ru

Среда электронного обучения СГУ им. Питирима Сорокина http:// http://eios.syktsu.ru/

Основы теории информации и криптографии

https://www.intuit.ru/studies/courses/2256/140/info

Журнал «Информационные технологии». – http://www.novtex.ru/IT

Журнал «Бизнес и информационные технологии». – http://bit.samag.ru

г) периодические издания и реферативные базы данных (при необходимости):

9. Информационные технологии, используемые при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости).

Система управления обучением Moodle, операционная система MS Windows 7 и выше; программные средства, входящие в состав офисного пакета MS Office (Word, Excel, Access, Publisher, PowerPoint); программы для просмотра документов, графические редакторы, браузеры, справочно-правовая система «Консультант Плюс».

10. Материально-техническая база, необходимая для проведения практики.

Материально-техническая база проведения практики представляет собой оборудование и технические средства обучения в объеме, позволяющем выполнять виды работ в соответствии с видом (-ами) профессиональной деятельности, к которому (-ым) готовится обучающиеся в результате освоения ОПОП в соответствии с ФГОС ВО.3

Сведения о материально-технической базе практики содержатся в справке о материально-технических условиях реализации образовательной программы.

11. Особенности организации практики для обучающихся с ограниченными возможностями здоровья и инвалидов.

Организация практики для обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется в соответствии с законодательством Российской Федерации.

Для обучающихся с ограниченными возможностями здоровья и инвалидов выбор места и способ прохождения практики устанавливается Университетом с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья, а также требований по доступности.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике.

Промежуточная аттестация по практике представляет собой комплексную оценку формирования, закрепления, развития практических навыков и компетенций по профилю образовательной программы, связанных с видом (-ами) профессиональной деятельности, к выполнению которых готовятся обучающиеся в соответствии с ОПОП.4

Фонд оценочных средств предназначен для оценки:

1) уровня освоения компетенций, соответствующих этапу прохождения практики;

2) соответствия запланированных и фактически достигнутых результатов освоения практики каждым студентом.

Критерии оценивания результатов промежуточной аттестации обучающихся по практике (с учетом характеристики работы обучающегося и/или характеристики – отзыва):

Форма промежуточной аттестации – «дифференцированный зачет» (зачет с оценкой)

Критерии оценивания	
Отлично	обучающийся выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, показал глубокую теоретическую, методическую, профессионально-прикладную подготовку, умело применил полученные знания во время прохождения практики, показал владение современными методами исследования профессиональной деятельности, использовал профессиональную терминологию, ответственно относился к своей работе; отчет по практике соответствует предъявляемым требования.
Хорошо	обучающийся выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, однако допустил несущественные ошибки, показал глубокую теоретическую, методическую, профессионально-прикладную подготовку, умело применил полученные знания во время прохождения практики, показал владение современными методами исследования профессиональной деятельности, использовал профессиональную терминологию, ответственно относился к своей работе; отчет по практике в целом соответствует предъявляемым требования, однако имеются несущественные ошибки в оформлении
Удовлетворительно	обучающийся выполнил индивидуальное задание в соответствии с программой практики, однако допустил существенные ошибки (могут быть нарушены сроки выполнения индивидуального задания), в процессе работы не проявил достаточной самостоятельности, инициативы и заинтересованности, демонстрирует недостаточный объем знаний и низкий уровень их применения на практике; низкий уровень владения профессиональной терминологией и методами исследования профессиональной деятельности; допущены значительные ошибки в оформлении отчета по практике.

Неудовлетворительно	обучающийся не выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, показал низкий уровень теоретической, методической, профессионально-прикладной подготовки, не применяет полученные знания во время прохождения практики, не показал владение современными методами исследования профессиональной деятельности, не использовал профессиональную терминологию,; отчет по практике не соответствует предъявляемым требования.

Виды контролируемых работ и оценочные средства

№п/п	Виды контролируемых работ по этапам	Код контролируемой компетенции (части компетенции)	Оценочные средства
1.	Подготовительный (ознакомительный) этап Допуск к прохождению практики после прохождения инструктажа (отметка в журнале техники безопасности). Присутствие на установочной конференции.	ОК-6 ОПК-5 ПК-1 ПК-2 ПК-7 ПК-8 ПК-9 ПК-11 ПК-12	Отчеты по заданиям, отчет о прохождении практики, материалы практики (при наличии)
2.	Основной этап Выполнить следующие примерные практические работы: 1. Изучить тему «Виды угроз информации», используя различные источники информации (библиотечный фонд, интернет ресурсы, лекционные материалы и т.п.). При изучении темы дать письменные ответы на представленные вопросы с указанием ссылки на источник заимствования. Вопросы: 1. Что такое угроза безопасности информации. 2. Приведите примеры организационных угроз. 3. Приведите примеры технологических угроз. 4. Какие каналы утечки информации существуют в компьютерных классах? Задание: Определите и классифицируйте угрозы безопасности вашего ПК 2. Изучите тему «Вредоносное программное обеспечение». Вопросы: 1. В чем состоит проблема вирусного заражения программ? 2. Приведите классификацию вредоносного программного обеспечения. 3. Опишите способы их обнаружения и наносимый ущерб? 4. Какие вредоносные программные закладки кроме вирусов существуют? 5. Какие существуют методы борьбы с компьютерными вирусами? Задание: Раскройте сущность приведенного вируса: Руткит Boot-вирус Макровирус Полиморфный 3. Изучите тему «Антивирусные программы». Вопросы: 1. Какие		

	основные антивирусные программы вы знаете, кратко охарактеризуйте их. (не менее 6 программ). 2. Каким образом происходит лечение зараженных дисков? 3. Что такое программа – полифаг? 4. Что такое программа - детектор? Задание: Дайте сравнительную характеристику не менее 5 антивирусных программ по не менее чем 5 критериям. 4. Определение порядка допуска должностных лиц и граждан Российской Федерации к государственной тайне и заполнение форм учетной документации, необходимой для оформления такого допуска. 5. Определение общего порядка обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения. 6. Структурная характеристика нормативно-правовых актов в области обеспечения защиты персональных данных. 7. Состав и назначение, порядок создания, утверждения и исполнения должностных инструкций. Составить штатное расписание сотрудников предприятия и утвердить должностные инструкции к нему. 8. Разработка пакета организационно-распорядительных документов для организации защиты конфиденциальной информации на предприятии. 9. Сравнительная характеристика антивирусных программ. Установка и настройка антивирусных программ: Dr.Web, NOD 32. Представить их сравнительный анализ в форме отчета и сделать вывод. 10. Сравнительный анализ программно-аппаратных средств защиты информации: Аккорд, Аура, Соболь, КриптоПро, Аргус, Ручей-М, SecretNet, Dallas Lock, Acronis, XSpider, MaxPatrol, eToken, RuToken, VipNet CUSTOM. Сравнительные характеритситки: Фирма производитель, тип продукта (программный, аппаратный и др.), уровень защиты по виду тайны (ГТ, КИ, ПДн, и др.), наличие сертификата ФСТЭК или ФСБ, стоимость (от-до) 11. Установка и настройка программно-аппаратной системы защиты информации «Аккорд», «Аура», «Dallas Lock» и др. По итогам выполнения каждого практического задания студентом-практикантом составляется отчет о		

	выполнении задания в письменной форме, состоящий из титульного листа и текста отчета: цель работы, ход выполнения работы, вывод. Примерный объем отчета 5-6 страниц. Каждое выполненное практическое задание оценивается «зачет/незачет» по следующим основным критериям: 1. Уровень выполнения задания: соответствует формированию закрепленной компетенции. 2. Полнота раскрытия темы задания, обоснованность выводов, предложений. 3. Качество оформления отчета. 4. Степень самостоятельности в работе: изложение, оригинальность составленных таблиц, схем и других материалов. 5. Научно-исследовательский подход, грамотность, стилистическая правильность текста.		
3.	Заключительный этап Подготовка отчета о прохождении учебной практики. Защита отчета.		

Утверждена в составе Основной
профессиональной образовательной
программы высшего образования

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Тип практики

преддипломная практика

Направление подготовки (специальность)

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направленность (профиль) программы

«направленность (профиль) N 7 "Техническая защита информации"»

1. Общие положения.

Программа производственной практики: преддипломная практика (далее – производственная практика) разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) по направлению подготовки (специальности) 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (утв. приказом Минобрнауки России от 01.12.2016 № 1515), локальными актами Университета.

2. Место практики в структуре основной профессиональной образовательной программы, объем практики.

Производственная практика относится к вариативной части учебного плана основной профессиональной образовательной программы (далее – ОПОП) по направлению подготовки (специальности) 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, направленность (профиль) «направленность (профиль) N 7 "Техническая защита информации"».

Объем практики составляет 12 зачетных единиц (далее - з.е.), или 432 академических часов.

3. Вид, способы и формы проведения практики; базы проведения практики.

Вид практики – производственная

Тип практики – преддипломная практика – определяется видами профессиональной деятельности, к которым готовится обучающийся в соответствии с ФГОС ВО и ОПОП.

Способы проведения практики (при наличии) – стационарная, выездная

Формы проведения практики: дискретно по видам практики

Базами проведения практики являются профильные организации, в том числе их структурные подразделения, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках ОПОП, на основании договоров, заключенных между Университетом и профильными организациями.

Практика может быть организована непосредственно в Университете, в том числе в его структурном подразделении.

Для руководства практикой, проводимой в Университете, обучающемуся назначается руководитель практики от Университета.

Для руководства практикой, проводимой в профильной организации, назначаются руководитель практики от Университета и руководитель практики от профильной организации.

4. Цели и задачи практики. Планируемые результаты обучения при прохождении практики.

Цели практики определяются видами профессиональной деятельности и компетенциями, которые должны быть сформированы у обучающегося в соответствии с ОПОП.

Цели практики:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла базовой и вариативной частей, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;

- изучение информационной структуры предприятия, как объекта информатизации;

- изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;

- формирование навыков самостоятельного решения поставленных производственных задач;

- выбор темы выпускной квалификационной работы и ее выполнение.

Задачи практики:

- закрепление и расширение теоретических и практических знаний;

- развитие профессиональных навыков и навыков деловой коммуникации;

- сбор необходимых материалов для написания отчета по практике;

- проведение анализа и обобщения результаты собственных исследований;

- получение практических данных, для написания выпускной квалификационной работы, приобретения навыков их обработки.

Данные задачи преддипломной практики, соотносятся со следующими видами и задачами профессиональной деятельности:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

участие в проведении аттестации объектов, помещений, технических средств,

систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;

администрирование подсистем информационной безопасности объекта;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

проведение экспериментов по заданной методике, обработка и анализ результатов;

проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей с учетом требований защиты информации;

участие в совершенствовании системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;

контроль эффективности реализации политики информационной безопасности объекта.

Производственная практика направлена на формирование следующих общекультурных, общепрофессиональных, профессиональных компетенций обучающегося в соответствии с выбранными видами профессиональной деятельности, к которым готовятся обучающийся в соответствии с ОПОП:

Планируемые результаты обучения при прохождении практики, соотнесенные с

планируемыми результатами освоения образовательной программы

Код и наименование компетенции	Планируемые результаты обучения
ОК-1 Способность использовать основы философских знаний для формирования мировоззренческой позиции ОК-2 Способность использовать основы экономических знаний в различных сферах деятельности ОК-3 Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма ОК-4 Способность использовать основы правовых знаний в различных сферах деятельности ОК-5 Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики ОК-6 Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия ОК-7 Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности ОК-8 Способность к самоорганизации и самообразованию ОК-9 Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности ОПК-1 Способность анализировать физические явления и процессы для решения профессиональных задач ОПК-2 Способность применять соответствующий математический аппарат для решения профессиональных задач ОПК-3 Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач ОПК-4 Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации ОПК-5 Способность использовать нормативные правовые акты в профессиональной деятельности ОПК-6 Способность применять приемы первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности ОПК-7 Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знать: должностные обязанности сотрудников в области защиты информации; основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ; основные понятия и методы в области управленческой деятельности; использовать в практической деятельности правовые знания; виды информации и ее носителей, классификацию угроз информации, уязвимости информации, структуру и содержание информационных процессов предприятия, технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам; аппаратные средства вычислительной техники; операционные системы, основы администрирования вычислительных сетей; системы управления базами данных; современные средства разработки и анализа программного обеспечения, операционные системы, правовые нормы по вопросам сертификации и лицензирования в области защиты информации; принципы организации информационных систем в соответствии с требованиями по защите информации; криптографические стандарты и их использование в информационных системах; принципы формирования политики информационной безопасности в информационных системах; организацию работы и нормативные правовые акты по аттестации объектов информатизации; методы аттестации уровня защищенности информационных систем; методы и средства контроля эффективности технической защиты информации; основные методы управления информационной безопасностью; основные подходы к анализу исходных данных и проектированию системы защиты информации; основные методики оценки рисков и проведения технико-экономического обоснования; свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления; задачи органов защиты информации на предприятиях; организацию работы и нормативные правовые акты по сертификации средств защиты информации; основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности; отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; основные методы экспериментальных исследований оценки защищенности объектов информатизации;

ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПК-3 Способность администрировать подсистемы информационной безопасности объекта защиты ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ПК-5 Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ПК-6 Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПК-9 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности ПК-10 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-11 Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов ПК-12 Способность принимать участие в проведении экспериментальных исследований системы защиты информации ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ПК-14 Способность организовать работу малого коллектива исполнителей в профессиональной деятельности ПК-15 Способность организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	основные понятия об измерениях и единицах физических величин; основные виды средств измерения и их классификацию; методы измерений; технические каналы утечки информации; возможности технических разведок; способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации; принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); основные понятия и методы в области управленческой деятельности; содержание управленческой работы руководителя подразделения; правовые основы организации защиты государственной тайны и конфиденциальной информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации; основные методы аналитического обоснования необходимости создания системы технической защиты объекта информатизации; классификацию и особенности применения технических средств защиты информации от утечки по техническим каналам; классификацию и особенности применения технических средств защиты информации от несанкционированного доступа и средства антивирусной защиты; основные понятия в области аттестации объектов информатизации; основные методы оценки защищенности объектов информатизации от утечки по техническим каналам и несанкционированного доступа к информации. Уметь: работать в команде, распределять обязанности по выполнению работ; анализировать основные правовые акты и осуществлять правовую оценку информации, нести персональную ответственность за нарушения нормативно-правовых требований, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и оценивать угрозы информационной безопасности объекта; разрабатывать нормативно-методические документы по защите информации; настраивать и обслуживать средства защиты информации; применять программные средства системного, прикладного и специального назначения; развертывать, конфигурировать и настраивать вычислительные сети; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; применять отечественные и зарубежные стандарты в области криптографических методов компьютерной

	безопасности для проектирования, разработки и оценки защищенности компьютерных систем; разрабатывать частные политики информационной безопасности информационных систем; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем; применять методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; оценивать информационные риски в информационных системах; проводить расчеты для технико-экономического обоснования проектных решений разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; квалифицированно исследовать состав документации предприятии (организации); разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по профилю своей деятельности; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; проводить эксперименты по заданной методике, обрабатывать и оценивать погрешности измерений; проводить оценку достоверности экспериментальных результатов классифицировать основные виды средств измерений; применять основные методы и принципы измерений; применять методы и средства обеспечения единства и точности измерений; применять аналоговые и цифровые измерительные приборы, измерительные генераторы; применять методические оценки защищённости информационных объектов; анализировать и оценивать угрозы информационной безопасности объекта; проводить мониторинг угроз безопасности информационных систем; формировать, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности; осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; пользоваться нормативными документами ФСБ России и ФСТЭК России в области защиты информации; применять методы аналитического обоснования необходимости создания системы технической

	защиты объекта информатизации; устанавливать и настраивать технические средства защиты информации от утечки по техническим каналам; устанавливать и настраивать технические средства защиты информации от несанкционированного доступа и средства антивирусной защиты; проводить оценку защищенности объектов информатизации от утечки информации по техническим каналам и несанкционированного доступа к информации. Владеть: навыками командной работы, способностью выражать свои мысли и мнения в деловой форме общения; навыками быстрого поиска законодательных требований в информационных источниках; навыками принятия решений, навыками дискуссии по профессиональной тематике; методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы; навыками работы использования технических средств идентификации и проверки подлинности пользователей компьютерных систем, навыками проведения оценки защищенности помещений от утечки по техническим каналам; навыками защиты от разрушающих программных воздействий; навыками рационального выбора средств и методов защиты информации объектов информатизации; навыками настройки и администрирования распространенных операционных систем и вычислительных сетей, построенных на их основе; навыками использования типовых криптографических алгоритмов; навыками реализации политики информационной безопасности объектов защиты; навыками применения комплексного подхода к обеспечению информационной безопасности объекта защиты; навыками организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; методами формирования требований по защите информации; навыками представления результатов научных исследований по вопросам обеспечения информационной безопасности по профилю своей деятельности с использованием современных технических средств в устной и письменной формах; методами анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; навыками проведения физического эксперимента и обработки его результатов; методами расчета и инструментального контроля показателей технической защиты информации; методами и средствами выявления угроз безопасности

	объектам информатизации; методами технической защиты информации; методами формирования требований по защите информации; методами мониторинга и аудита угроз информационной безопасности информационных систем; методами организации и управления деятельностью служб защиты информации на предприятии; навыками обоснования, выбора, реализации и контроля результатов управленческого решения; навыками организации и обеспечения режима коммерческой тайны и/или режима секретности; навыками подготовки аналитического обоснования необходимости создания системы технической защиты объекта информатизации; навыками обслуживания технических средств защиты информации от утечки по техническим каналам; навыками обслуживания технических средств защиты информации от несанкционированного доступа и средства антивирусной защиты; навыками проведения специального обследования объектов информатизации и оценки защищенности объектов информатизации от утечки информации по техническим каналам и несанкционированного доступа к информации; навыками проведения аттестации объектов информатизации.

5. Содержание практики.

Производственная практика проходит в три этапа:

подготовительный (ознакомительный), основной, заключительный.

№ п/п	Этапы практики и их содержание
	Подготовительный (ознакомительный) этап
	Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации, прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка. Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики.
	Основой этап
	Ознакомление с деятельностью предприятия. Определение методов и средств защиты информации, используемых на предприятии. Выполнение практических заданий. Сбор материалов для отчетной документации. Преддипломная практика предполагает: производственный инструктаж, в т.ч. инструктаж по технике безопасности; выполнение производственных заданий; сбор, обработка и систематизация фактического и литературного материала; наблюдения; измерения и другие, выполняемые обучающимся самостоятельно виды работ. На каждом рабочем месте проводится инструктаж по ТБ. Студент должен усвоить полученный материал и расписаться в соответствующем журнале. Находясь на практике, студент подчиняется правилам внутреннего распорядка, установленным для работников предприятия. В начале практики руководитель от предприятия совместно со студентом составляют план прохождения практики с учетом тематики примерных практических заданий рекомендованных данной программой практики, профилем и технической оснащенностью данного предприятия. План прохождения практики согласовывается с руководителем практики от Университета. Преддипломная практика предполагает непосредственное участие студентов в деятельности предприятия. Студент обязан добросовестно и качественно выполнять порученную ему работу. Методическое и консультационное обеспечение осуществляет руководитель практики от Университета или заведующий кафедрой информационной безопасности.
	Заключительный этап
	Подготовка отчетной документации, получение характеристики о работе и (или) характеристики – отзыва руководителя практики от университета, представление отчетной документации на кафедру, прохождение

промежуточной аттестации по практике. Систематизация и анализ выполненных заданий.

6. Формы отчетности по практике.

Формой промежуточной аттестации по практике является зачет с оценкой.

По результатам прохождения практики обучающийся представляет, следующую отчетную документацию:

- дневник производственной практики;
- отчет о прохождении производственной практики;
- материалы практики (при наличии);
- лист экспертной оценки

Руководитель практики от Университета представляет характеристику – отзыв. Руководитель практики от профильной организации представляет характеристику работы обучающегося.

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

Фонд оценочных средств представлен в приложении к программе практики (Приложение 1).

8. Учебная литература и ресурсы сети Интернет.

а) основная литература:

Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. ;Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=362895

Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. ;Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=276557

Носов Л.С. Техническая защита информации [Электронный ресурс] : Учебное пособие. Ч. 1 : Инженерно-техническая защита информации / Л. С. Носов, А. Р. Биричевский. - Сыктывкар : Изд-во СыктГУ, 2012. - 77 с.URL:http://e-library.syktsu.ru/megapro/Download/MObject/343/978-5-87237-830-3 Носов Л.С.,

Биричевский А.Р. Техническая защита информации. Часть 1. Инженерно-техническая защита информации. Учебное пособие.pdf

Носов Л.С. Техническая защита информации [Электронный ресурс] : Учебное пособие. Ч. 2 : Техническая защита информации / Л. С. Носов, А. Р. Биричевский, Д. Н. Едомский. - Сыктывкар : Изд-во СыктГУ, 2012. - 78 с.URL:http://e-library.syktsu.ru/megapro/Download/MObject/344/978-5-87237-831-0 Носов Л.С., Биричевский А.Р. Техническая защита информации. Часть 2. Технические средства защиты информации. Учебное пособие.pdf

Титов, А.А. Технические средства защиты информации : учебное пособие / А.А. ;Титов. – Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 194 с. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=208661

Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. ;Бурькова ; Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. – Оренбург : Оренбургский государственный университет, 2017. – 158 с. : табл., схем. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=481730

Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А.М. ;Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=480636

Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. ;Громов, О.Г. ;Иванова, К.В. ;Стародубов, А.А. ;Кадыков ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=499013

Аверченков, В.И. Аудит информационной безопасности: учебное пособие для вузов / В.И. ;Аверченков. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 269 с. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=93245

Методологические основы построения защищенных автоматизированных систем : учебное пособие / А.В. ;Душкин, О.В. ;Ланкин, С.В. ;Потехецкий и др. ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2013. – 258 с. : табл., ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=255851

Инструментальный контроль и защита информации : учебное пособие / Н.А. ;Свинарев, О.В. ;Ланкин, А.П. ;Данилкин и др. ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2013. – 192 с. : табл., ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=255905

б) дополнительная литература:

Монаппа, К. А. Анализ вредоносных программ / К. А. Монаппа ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2019. — 452 с. — ISBN 978-5-97060-700-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL:https://e.lanbook.com/book/123709?category=1545

Спицын, В.Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. ;Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. : ил.,табл., схем. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=208694

Артемов, А.В. Информационная безопасность: курс лекций / А.В. ;Артемов ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=428605

Иванов, А.В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок : учебное пособие : [16+] / А.В. ;Иванов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 64 с. : ил., табл. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book_red&id=575420

в) Интернет-ресурсы:

https://elibrary.ru/ – национальная библиографическая база данных научного цитирования (профессиональная база данных)

Журнал «Системы управления бизнес-процессами». – http://journal.itmane.ru

Системы дистанционного обучения СГУ им. Питирима Сорокина на базе Moodle - http://lms-moodle.syktsu.ru

Российский образовательный портал http://www.edu.ru/

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций https://rkn.gov.ru

Журнал «Проблемы информационной безопасности. Компьютерные системы» http://jisp.ru/

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://www.gost.ru

Сайт ФСТЭК России – www.fstec.ru

Журнал «Безопасность информационных технологий» https://bit.mephi.ru/index.php/bit

Сайт ФСБ России – www.fsb.ru

Журнал «Информация и безопасность» http://kafedrasib.ru/index.php/informatsiya-bezopasnost

Журнал «Труды СПИРАН» http://proceedings.spiiras.nw.ru/ojs/index.php/sp

Журнал «Прикладная информатика». – http://www.appliedinformatics.ru

Журнал «Бизнес-информатика». – https://bijournal.hse.ru

Журнал «Бизнес и информационные технологии». – http://bit.samag.ru

Журнал «Программная инженерия». http://novtex.ru/prin/rus/

Банк данных угроз ФСТЭК России https://bdu.fstec.ru

Справочная правовая система «КонсультантПлюс» www.consultant.ru

Журнал «Системный администратор» http://samag.ru/

Портал ИСПДн.РУ http://www.ispdn.ru

Среда электронного обучения СГУ им. Питирима Сорокина http:// http://eios.syktsu.ru/

Журнал «Информационные технологии». – http://www.novtex.ru/IT

Журнал «Информационные технологии и вычислительные системы». – http://www.jitcs.ru

Журнал «Системный администратор». – http://samag.ru

г) периодические издания и реферативные базы данных (при необходимости):

9. Информационные технологии, используемые при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости).

Система управления обучением Moodle, операционная система MS Windows 7 и выше; программные средства, входящие в состав офисного пакета MS Office (Word, Excel, Access, Publisher, PowerPoint); программы для просмотра документов, графические редакторы, браузеры, справочно-правовая система «Консультант Плюс».

10. Материально-техническая база, необходимая для проведения практики.

Материально-техническая база проведения практики представляет собой оборудование и технические средства обучения в объеме, позволяющем выполнять виды работ в соответствии с видом (-ами) профессиональной деятельности, к которому (-ым) готовится обучающиеся в результате освоения ОПОП в соответствии с ФГОС ВО.3

Сведения о материально-технической базе практики содержатся в справке о материально-технических условиях реализации образовательной программы.

11. Особенности организации практики для обучающихся с ограниченными возможностями здоровья и инвалидов.

Организация практики для обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется в соответствии с законодательством Российской Федерации.

Для обучающихся с ограниченными возможностями здоровья и инвалидов выбор места и способ прохождения практики устанавливается Университетом с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья, а также требований по доступности.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике.

Промежуточная аттестация по практике представляет собой комплексную оценку формирования, закрепления, развития практических навыков и компетенций по профилю образовательной программы, связанных с видом (-ами) профессиональной деятельности, к выполнению которых готовятся обучающиеся в соответствии с ОПОП.4

Фонд оценочных средств предназначен для оценки:

1) уровня освоения компетенций, соответствующих этапу прохождения практики;

2) соответствия запланированных и фактически достигнутых результатов освоения практики каждым студентом.

Критерии оценивания результатов промежуточной аттестации обучающихся по практике (с учетом характеристики работы обучающегося и/или характеристики – отзыва):

Форма промежуточной аттестации – «дифференцированный зачет» (зачет с оценкой)

Критерии оценивания	
Отлично	обучающийся выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, показал глубокую теоретическую, методическую, профессионально-прикладную подготовку, умело применил полученные знания во время прохождения практики, показал владение современными методами исследования профессиональной деятельности, использовал профессиональную терминологию, ответственно относился к своей работе; отчет по практике соответствует предъявляемым требования.
Хорошо	обучающийся выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, однако допустил несущественные ошибки, показал глубокую теоретическую, методическую, профессионально-прикладную подготовку, умело применил полученные знания во время прохождения практики, показал владение современными методами исследования профессиональной деятельности, использовал профессиональную терминологию, ответственно относился к своей работе; отчет по практике в целом соответствует предъявляемым требования, однако имеются несущественные ошибки в оформлении
Удовлетворительно	обучающийся выполнил индивидуальное задание в соответствии с программой практики, однако допустил существенные ошибки (могут быть нарушены сроки выполнения индивидуального задания), в процессе работы не проявил достаточной самостоятельности, инициативы и заинтересованности, демонстрирует недостаточный объем знаний и низкий уровень их применения на практике; низкий уровень владения профессиональной терминологией и методами исследования профессиональной деятельности; допущены значительные ошибки в оформлении отчета по практике.

Неудовлетворительно	обучающийся не выполнил индивидуальное задание в соответствии с программой практики в установленные сроки, показал низкий уровень теоретической, методической, профессионально-прикладной подготовки, не применяет полученные знания во время прохождения практики, не показал владение современными методами исследования профессиональной деятельности, не использовал профессиональную терминологию,; отчет по практике не соответствует предъявляемым требования.

Виды контролируемых работ и оценочные средства

№п/п	Виды контролируемых работ по этапам	Код контролируемой компетенции (части компетенции)	Оценочные средства
1.	Подготовительный (ознакомительный) этап Допуске к прохождению практики (отметка в журнале инструктажа). Присутствие на установочной конференции.	ОК-1 ОК-2 ОК-3 ОК-4 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОПК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10 ПК-11 ПК-12 ПК-13 ПК-14 ПК-15	Дневник практики, отчет о прохождении практики, материалы практики (при наличии), лист экспертной оценки
2.	Основной этап Пошаговый анализ выполнения практических заданий. Оформление отчетной документации. Согласование отчета с руководителем практики от предприятия. Примерные практические задания: 1. ознакомиться с историей, традициями и сферами деятельности предприятия согласно уставу или положению о предприятии и пройти инструктаж по технике безопасности на рабочем месте; 2. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 3. определить виды информации ограниченного доступа, обрабатываемые предприятием; 4. ознакомиться с формами организации производственного процесса и его технологическим обеспечением; 5. выявить угрозы безопасности предприятия; 6. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 7. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 8. изучить методы и средства защиты информации, применяемые на предприятии; 9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических		

	средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 10. разработать модель угроз для конкретной информационной системы предприятия; 11. изучить основные обязанности должностных лиц в области защиты информации; 12. проанализировать методы контроля в области защиты информации, используемые в организации; 13. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 14. предложить перечень мероприятий по улучшению системы защиты информации на предприятии. 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 19. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 20. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 21. спроектировать систему физической защиты информации; 22. разработать политику информационной безопасности предприятия; 23. проанализировать систему компьютерной безопасности предприятия; 24. изучить систему контроля и управления доступом предприятия; 25. изучить систему защиты персональных данных в организации; 26. изучить виды правонарушений при совершении компьютерных преступлений; 27. провести анализ рисков информационной безопасности; 28. разработать программное решение для обеспечения информационной безопасности; 29. провести исследования		

	вредоносного кода; 30. исследовать проблемы безопасности при использовании мобильных устройств; 31. изучить обеспечение информационной безопасности при использовании СЭД; 32. исследовать криптографические методы защиты информации; 33. исследовать способы защиты мультисервисных сетей.		
3.	Заключительный этап Анализ отчетной документации за период практики. Отчет о прохождении практики на итоговой конференции. Оценка работы. Отчет оформляется с помощью печатающих устройств на одной стороне листа бумаги формата А4. Размер шрифта 12-14 через 1-1,5 интервала. При написании текста следует оставлять поля слева - 30 мм, справа - 10 мм, сверху и снизу - 20 мм. Все страницы должны иметь сквозную нумерацию: первой страницей является титульный лист. На титульном листе номер не ставится. Номер страницы проставляется в низу по центру. Отчет о практике является обязательным документом студентов-практикантов. По форме он должен включать титульный лист и текст отчета. Отчет обязательно должен содержать не только информацию о выполнении заданий программы практики, но и анализ этой информации, выводы и рекомендации, разработанные студентом самостоятельно. Оформленный итоговый отчет должен быть сброшюрован в папку со скоросшивателем. Титульный лист должен быть подписан руководителями практики и студентом-практикантом. Отчёт может содержать приложения: - материалы, собранные студентом в период прохождения практики (копии нормативно правовых и организационных документов, а также те документы, в составлении которых студент, принимал непосредственное участие в объёме, предусмотренном заданием); - схемы, таблицы, аналитические расчёты, статистические данные, иллюстрации и т.п. Отчет готовится в течение всей практики и проверяется преподавателем-руководителем практики до защиты практики. Оформленный отчет о практике, подлежит обязательной		

	защите студентом в установленные сроки. По окончании преддипломной практики руководитель практики от предприятия дает отзыв о прохождении практики студентом в листе экспертной оценки. В отзыве должна быть дана характеристика студента со стороны овладения им знаний, умений и навыков для решения производственных задач в области обеспечения информационной безопасности, произведена оценка уровня сформированности компетенций в различных видах профессиональной деятельности и отмечены достоинства и недостатки в его профессиональной подготовке. Аттестация по итогам преддипломной практики проводится на основании материалов отчета о практике, дневника преддипломной практики и листа экспертной оценки, оформленных в соответствии с установленными требованиями. Прием зачета по практике производит комиссия. В состав комиссии входят заведующий кафедрой, руководитель практики от Университета, руководитель практики от предприятия и другие преподаватели, назначенные распоряжением директора института. По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).		