Китайгородский Михаил Дмитриевич

Подписано цифровой подписью: Китайгородский Михаил Дмитриевич
Дата: 2023.11.15 14:48:49 +03'00'

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

«Техническая защита информации»

1. Общие положения

Программа производственной практики преддипломная практика (далее – производственная практика) разработана в соответствии с федеральным государственным образовательным стандартом высшего образования (далее – ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, локальными актами университета и с учетом профессионального(-ых) стандарта(-ов) «Специалист по защите информации в автоматизированных системах» (утв. приказом Минтруда России от 15.09.2016 № 522н) и «Специалист по технической защите информации» (утв. приказом Минтруда России от 01.11.2016 № 599н).».

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

Производственная практика относится к обязательной части учебного плана основной профессиональной образовательной программы (далее – ОПОП) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, направленность (профиль) «Техническая защита информации».

Объем практики составляет 12 зачетных (-ые) единиц (-ы) (далее - з.е.), или 432 академических часов , в том числе в форме практической подготовки 432 академических часа (-ов).

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

Вид практики – производственная.

Тип практики – преддипломная практика – определяется типом (-ами) задач профессиональной деятельности, к которому(-ым) готовится выпускник в соответствии с ФГОС ВО и ОПОП.

Способ (-ы) проведения практики непрерывно. Базами проведения практики являются профильные организации, в том числе их структурные подразделения, деятельность которых соответствует профилю образовательной программы, на основании договоров, заключенных между университетом и профильной организацией.

Практика может быть организована непосредственно в университете, в том числе в его структурном подразделении, предназначенном для проведения практической подготовки.

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 типом(-ами) задач профессиональной деятельности и компетенциями, которые должны быть сформированы у обучающегося в соответствии с ОПОП.

Цель 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 универсальных, общепрофессиональных и профессиональных компетенций (выбрать нужное) выпускника в соответствии с выбранным(-и) типом(-ами) задач профессиональной деятельности, к которому(-ым) готовятся обучающиеся в соответствии с ОПОП.

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

Содержание и шифр компетенции	Планируемые результаты обучения		
	Знать	Уметь	Владеть
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	принципы сбора, отбора и обобщения информации	соотносить разнородные явления и систематизировать их в рамках избранных видов деятельности	способностью грамотно, логично, аргументированно формировать собственные суждения и оценки
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	правовые нормы, необходимые для достижения поставленной цели при реализации проекта	определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность, исходя из имеющихся ресурсов, соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности	навыками отбора оптимальных технологий целедостижения; навыками работы с нормативными документами
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	различные приёмы и способы социализации личности и социального взаимодействия	строить отношения с окружающими людьми, с коллегами	способностью определять свою роль в команде на основе использования стратегии сотрудничества для достижения поставленной цели

УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	основы коммуникации, нормы, правила и особенности её осуществления в устной и письменной формах на русском и иностранном(ых) языке(ах)	применять правила и нормы деловой коммуникации на русском и иностранном(ых) языке(ах)	навыками применения коммуникативных технологий на русском и иностранном(ых) языке(ах) для академического и профессионального взаимодействия
УК-5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	основные категории философии, законы исторического развития, основы межкультурной коммуникации	анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	навыками коммуникации с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм
УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда	планировать своё рабочее время и время для саморазвития, формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей	выстраивать траекторию саморазвития посредством обучения по дополнительным образовательным программам
УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	основы здорового образа жизни, здоровьесберегающих технологий, физической культуры	выполнять комплекс физкультурных упражнений	практический опыт занятий физической культурой
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	основы безопасности жизнедеятельности, телефоны служб спасения	оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности	навыками поддержания безопасных условий жизнедеятельности
УК-9 Способен принимать обоснованные экономические решения в различных областях	базовые принципы функционирования экономики и экономического развития, цели и формы участия	применять методы личного экономического и финансового планирования для достижения текущих и	инструментами управления личными финансами для достижения поставленных

жизнедеятельности	государства в экономике	долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски	финансовых целей
УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	Иметь представление о понятии и сущности экстремизма, терроризма, коррупции; формах их проявления в современном обществе; их общественной опасности; основы системы противодействия этим явлениям в России, в том числе базовые положения предметного российского законодательства, основные виды правонарушений экстремистского, террористического, коррупционного характера, виды и меры юридической ответственности за их совершение; о необходимости противодействия экстремистским, террористическим, коррупционным проявлениям.	Уметь определять признаки экстремистской, террористической, коррупционной деятельности и давать им правовую оценку; идентифицировать конкретные органы публичной власти и иные субъекты, в компетенцию которых входит противодействие различным формам проявления указанных деструктивных социальных явлений; использовать систему мер противодействия экстремистским, террористическим и коррупционным проявлениям в области своей профессиональной деятельности.	Владеть навыками реализации правовых актов в области противодействия экстремистским, террористическим и коррупционным проявлениям в сфере профессиональной деятельности.
ПК-1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	методы, средства и технологии обеспечения защиты информации в автоматизированных системах	применять методы, средства и технологии обеспечения защиты информации в автоматизированных системах	навыками обеспечения защиты информации в автоматизированных системах в процессе их эксплуатации
ПК-2 Внедрение систем защиты информации автоматизированных систем	подходы к внедрению систем защиты информации в автоматизированных системах	устанавливать и настраивать средства защиты информации	навыками внедрения систем защиты информации в автоматизированных системах
ПК-3 Проведение	методы и средства	проводить измерения по	навыками проведения

контроля защищенности информации	контроля защищенности информации от утечки по техническим каналам и от несанкционированного доступа; нормативные правовые акты и методические документы по контролю защищенности	заданной методике	контроля защищенности информации; навыками оформления документации по результатам контроля

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, 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.
	Практическая подготовка
	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.
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;
- Лист экспертной оценки

Руководитель практики от Университета и руководитель практики от профильной организации – базы практики представляют характеристику-отзыв / характеристику работы обучающегося.

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

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

8. Учебная литература и ресурсы сети Интернет.

а) основная литература:

Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / 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. – 255 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

б) дополнительная литература:

С получением библиографческого описания возникла проблема, URL:https://e.lanbook.com/book/123709?category=1545

Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие : [16+] / 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:

Портал ИСПДн.РУ http://www.ispdn.ru

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

Сайт ФСБ России – www.fsb.ru

Справочная правовая система «КонсультантПлюс» www.consultant.ru

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

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

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

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

Сайт ФСТЭК России – www.fstec.ru

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

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

Информационно-правовой портал ГАРАНТ www.garant.ru

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

Основы теории информации и криптографии https://www.intuit.ru/studies/courses/2256/140/info

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

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

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

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

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

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

Официальный сервер органов государственной власти РФ www.gov.ru

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

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://www.gost.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 «КонсультантПлюс».

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 типом(-ами) задач профессиональной деятельности, к которому(-ым) готовится обучающиеся в результате освоения ОПОП в соответствии с ФГОС ВО.

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 типом(-ами) задач профессиональной деятельности, к решению которых готовятся обучающиеся в соответствии с ОПОП.

Фонд оценочных средств предназначен для оценки:

1) соответствия запланированных и фактически достигнутых результатов освоения практики каждым студентом;

2) уровня освоения компетенций, соответствующих этапу прохождения практики.

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.	УК-1 УК-2 УК-3 УК-4 УК-5 УК-6 УК-7 УК-8 УК-9 УК-10 ПК-1 ПК-2 ПК-3	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.		
	Практическая подготовка 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).		

Приложение 2

Фонд оценочных средств по практической подготовке

Задания по практической подготовке

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.

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

«Техническая защита информации»

1. Общие положения

Программа производственной практики эксплуатационная практика (далее – производственная практика) разработана в соответствии с федеральным государственным образовательным стандартом высшего образования (далее – ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, локальными актами университета и с учетом профессионального(-ых) стандарта(-ов) «Специалист по защите информации в автоматизированных системах» (утв. приказом Минтруда России от 15.09.2016 № 522н) и «Специалист по технической защите информации» (утв. приказом Минтруда России от 01.11.2016 № 599н).».

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

Производственная практика относится к обязательной части учебного плана основной профессиональной образовательной программы (далее – ОПОП) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, направленность (профиль) «Техническая защита информации».

Объем практики составляет 6 зачетных (-ые) единиц (-ы) (далее - з.е.), или 216 академических часов , в том числе в форме практической подготовки 216 академических часа (-ов).

4. Вид и способы проведения практики; базы проведения практики.

Вид практики – производственная.

Тип практики – эксплуатационная практика – определяется типом (-ами) задач профессиональной деятельности, к которому(-ым) готовится выпускник в соответствии с ФГОС ВО и ОПОП.

Способ (-ы) проведения практики непрерывно. Базами проведения практики являются профильные организации, в том числе их структурные подразделения, деятельность которых соответствует профилю образовательной программы, на основании договоров, заключенных между университетом и профильной организацией.

Практика может быть организована непосредственно в университете, в том числе в его структурном подразделении, предназначенном для проведения практической подготовки.

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 типом(-ами) задач профессиональной деятельности и компетенциями, которые должны быть сформированы у обучающегося в соответствии с ОПОП.

Цель 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 универсальных, общепрофессиональных и профессиональных компетенций (выбрать нужное) выпускника в соответствии с выбранным(-и) типом(-ами) задач профессиональной деятельности, к которому(-ым) готовятся обучающиеся в соответствии с ОПОП.

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

Содержание и шифр компетенции	Планируемые результаты обучения		
	Знать	Уметь	Владеть
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	принципы сбора, отбора и обобщения информации	соотносить разнородные явления и систематизировать их в рамках избранных видов деятельности	способностью грамотно, логично, аргументированно формировать собственные суждения и оценки
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	правовые нормы, необходимые для достижения поставленной цели при реализации проекта	определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность, исходя из имеющихся ресурсов, соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности	навыками отбора оптимальных технологий целедостижения; навыками работы с нормативными документами
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	различные приёмы и способы социализации личности и социального взаимодействия	строить отношения с окружающими людьми, с коллегами	способностью определять свою роль в команде на основе использования стратегии сотрудничества для достижения поставленной цели
УК-4 Способен	основы коммуникации,	применять правила и	навыками применения

осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	нормы, правила и особенности её осуществления в устной и письменной формах на русском и иностранном(ых) языке(ах)	нормы деловой коммуникации на русском и иностранном(ых) языке(ах)	коммуникативных технологий на русском и иностранном(ых) языке(ах) для академического и профессионального взаимодействия
УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда	планировать своё рабочее время и время для саморазвития, формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей	способностью выстраивать траекторию саморазвития посредством обучения по дополнительным образовательным программам
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	основы безопасности жизнедеятельности, телефоны служб спасения	оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности	навыками поддержания безопасных условий жизнедеятельности
УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике	применять методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски	инструментами управления личными финансами для достижения поставленных финансовых целей
УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма,	Иметь представление о понятии и сущности экстремизма, терроризма, коррупции; формах их проявления в	Уметь определять признаки экстремистской, террористической, коррупционной деятельности и давать им правовую	Владеть навыками реализации правовых актов в области противодействия экстремистским, террористическим и

коррупционному поведению и противодействовать им в профессиональной деятельности	современном обществе; их общественной опасности; основы системы противодействия этим явлениям в России, в том числе базовые положения предметного российского законодательства, основные виды правонарушений экстремистского, террористического, коррупционного характера, виды и меры юридической ответственности за их совершение; о необходимости противодействия экстремистским, террористическим, коррупционным проявлениям.	оценку; идентифицировать конкретные органы публичной власти и иные субъекты, в компетенцию которых входит противодействие различным формам проявления указанных деструктивных социальных явлений; использовать систему мер противодействия экстремистским, террористическим и коррупционным проявлениям в области своей профессиональной деятельности.	коррупционным проявлениям в сфере профессиональной деятельности.
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	основные понятия информатики; назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных	использовать программные и аппаратные средства персонального компьютера; применять программные средства системного, прикладного и специального назначения	навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.); навыками обеспечивать работоспособности операционных систем и прикладных программ
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для	основные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства и методы использования	применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства	навыками решения задач профессиональной деятельности с использованием информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе

решения задач профессиональной деятельности;			отечественного производства
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности;	необходимые математические методы	определять и применять необходимые математические методы	навыками решения задач профессиональной деятельности с использованием необходимые математические методы
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	физические законы и модели	определять и применять необходимые физические законы и модели	навыками решения задач профессиональной деятельности с использованием необходимых физических законов и моделей
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	основы организационного и правового обеспечения информационной безопасности; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; основные нормативные правовые акты в области информационной безопасности и защиты информации	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; пользоваться нормативными документами по защите информации	навыками работы с нормативными правовыми актами; навыками работы с нормативными правовыми актами по технической защите информации
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	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	пользоваться нормативными документами ФСБ России и ФСТЭК России в области защиты информации	навыками организации и обеспечения режима коммерческой тайны и/или режима секретности

ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;	современные средства разработки и анализа программного обеспечения на языках высокого уровня; методы программирования и методы разработки эффективных алгоритмов решения прикладных задач	выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные	навыками разработки программ на языке программирования высокого уровня; основными подходами к организации процесса разработки программного обеспечения
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности	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	навыками представления результатов научных исследований по вопросам обеспечения информационной безопасности по профилю своей деятельности с использованием современных технических средств в устной и письменной формах
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	современные средства криптографической и технической защиты информации	использовать и настраивать современные средства криптографической и технической защиты информации	навыками решения задач профессиональной деятельности с использованием современных средства криптографической и технической защиты информации
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	принципы формирования политики информационной безопасности в информационных системах	разрабатывать частные политики информационной безопасности информационных систем; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	навыками реализации политики информационной безопасности объектов защиты; навыками применения комплексного подхода к обеспечению информационной безопасности объекта защиты
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов;	основные методы экспериментальных исследований оценки защищенности объектов информатизации; основные понятия об измерениях и единицах физических величин; основные виды средств измерения и их классификацию; методы измерений	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;	навыками проведения физического эксперимента и обработки его результатов; методами расчета и инструментального контроля показателей технической защиты информации

		применять методы и средства обеспечения единства и точности измерений; применять аналоговые и цифровые измерительные приборы, измерительные генераторы; применять методические оценки защищенности информационных объектов	
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	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	оценивать информационные риски в информационных системах; проводить расчёты для технико-экономического обоснования проектных решений; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем	методами управления информационной безопасностью информационных систем; методами оценки информационных рисков
ОПК-13 Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	основные закономерности исторического процесса; этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира с древности до наших дней, выдающихся деятелей отечественной истории; различные оценки и периодизации Отечественной истории	соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; извлекать уроки из исторических событий и на их основе принимать осознанные решения; осуществлять эффективный поиск информации и критику источников; получать, обрабатывать и сохранять источники информации; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории	представлениями о событиях российской и всемирной истории, основанными на принципе историзма; навыками анализа исторических источников; приёмами ведения дискуссии и полемики
ОПК-3.1 Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам	классификацию и особенности применения технических средств защиты информации от утечки по техническим каналам	устанавливать и настраивать технические средства защиты информации от утечки по техническим каналам	навыками испытания и обслуживания технических средств защиты информации от утечки по техническим каналам
ОПК-3.2 Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств	классификацию и особенности применения технических средств защиты информации от несанкционированного доступа и средства	устанавливать и настраивать технические средства защиты информации от несанкционированного доступа и средства	навыками испытания и обслуживания технических средств защиты информации от несанкционированного доступа и средства

защиты информации от несанкционированного доступа	антивирусной защиты	антивирусной защиты	антивирусной защиты
ОПК-3.3 Способен проводить контроль эффективности защиты информации от утечки по техническим каналам	основные понятия в области аттестации объектов информатизации; - основные методы оценки защищенности объектов информатизации от утечки по техническим каналам	проводить оценку защищенности объектов информатизации от утечки информации по техническим каналам	навыками проведения специального обследования объектов информатизации и оценки защищенности объектов информатизации от утечки информации по техническим каналам
ОПК-3.4 Способен проводить контроль защищенности информации от несанкционированного доступа	основные понятия в области аттестации объектов информатизации; основные методы оценки защищенности объектов информатизации от несанкционированного доступа к информации	проводить оценку защищенности объектов информатизации от несанкционированного доступа к информации	навыками проведения оценки защищенности объектов информатизации от несанкционированного доступа к информации
ПК-1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	методы, средства и технологии обеспечения защиты информации в автоматизированных системах	применять методы, средства и технологии обеспечения защиты информации в автоматизированных системах	навыками обеспечения защиты информации в автоматизированных системах в процессе их эксплуатации
ПК-2 Внедрение систем защиты информации автоматизированных систем	подходы к внедрению систем защиты информации в автоматизированных системах	устанавливать и настраивать средства защиты информации	навыками внедрения систем защиты информации в автоматизированных системах
ПК-3 Проведение контроля защищенности информации	методы и средства контроля защищенности информации от утечки по техническим каналам и от несанкционированного доступа; нормативные правовые акты и методические документы по контролю защищенности	проводить измерения по заданной методике	навыками проведения контроля защищенности информации; навыками оформления документации по результатам контроля

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, 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.
Практическая подготовка	
	Примерные практические задания: 1. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 2. определить виды информации ограниченного доступа, обрабатываемые предприятием; 3. ознакомиться с формами организации производственного процесса и его технологическим обеспечением; 4. выявить угрозы безопасности предприятия; 5. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 6. изучить методы и средства защиты информации, применяемые на предприятии; 7. 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; 8. разработать модель угроз для конкретной информационной системы предприятия; 9. проанализировать методы контроля в области защиты информации, используемые в организации; 10. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 11. предложить перечень мероприятий по улучшению системы защиты информации на предприятии. 12. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 13. провести анализ безопасности программных продуктов, используемых на предприятии; 14. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 15. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 16. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 17. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 18. спроектировать систему физической защиты информации; 19. разработать политику информационной безопасности предприятия; 20. проанализировать систему компьютерной безопасности предприятия; 21. изучить систему контроля и управления доступом предприятия; 22. ознакомиться с системой защиты персональных данных в организации; 23. изучить виды правонарушений при совершении компьютерных преступлений.
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;

Руководитель практики от Университета и руководитель практики от профильной организации – базы практики представляют характеристику-отзыв / характеристику работы обучающегося.

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

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

8. Учебная литература и ресурсы сети Интернет.

а) основная литература:

Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие : [16+] / 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

Программно-аппаратные средства защиты информационных систем : учебное пособие : [16+] / Ю. ;Ю. ;Громов, О. ;Г. ;Иванова, К. ;В. ;Стародубов, А. ;А. ;Кадыков. – 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:

Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие : [16+] / 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:

Информационно-правовой портал ГАРАНТ www.garant.ru

Сайт ФСБ России – www.fsb.ru

Справочная правовая система «КонсультантПлюс» www.consultant.ru

Сайт ФСТЭК России – www.fstec.ru

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

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

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

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

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

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

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

Портал ИСПДн.РУ http://www.ispdn.ru

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

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://www.gost.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 «КонсультантПлюс».

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 типом(-ами) задач профессиональной деятельности, к которому(-ым) готовится обучающиеся в результате освоения ОПОП в соответствии с ФГОС ВО.

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 типом(-ами) задач профессиональной деятельности, к решению которых готовятся обучающиеся в соответствии с ОПОП.

Фонд оценочных средств предназначен для оценки:

1) соответствия запланированных и фактически достигнутых результатов освоения практики каждым студентом;

2) уровня освоения компетенций, соответствующих этапу прохождения практики.

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.	УК-1 УК-2 УК-3 УК-4 УК-6 УК-8 УК-9 УК-10 ОПК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ОПК-8 ОПК-9 ОПК-10 ОПК-11	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	ОПК-12 ОПК-13 ОПК-3.1 ОПК-3.2 ОПК-3.3 ОПК-3.4 ПК-1 ПК-2 ПК-3	

	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.		
	Практическая подготовка Примерные практические задания: 1. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 2. определить виды информации ограниченного доступа, обрабатываемые предприятием; 3. ознакомиться с формами организации производственного процесса и его технологическим обеспечением; 4. выявить угрозы безопасности предприятия; 5. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 6. изучить методы и средства защиты информации, применяемые на предприятии; 7. 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; 8. разработать модель угроз для конкретной информационной системы предприятия; 9. проанализировать методы контроля в области защиты информации, используемые в организации; 10. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 11. предложить перечень мероприятий по улучшению системы защиты информации на предприятии. 12. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 13. провести анализ безопасности программных продуктов, используемых на предприятии; 14. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 15. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 16. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 17. спроектировать систему ИТЗИ кабинета руководителя организации или		

	выделенного помещения; 18. спроектировать систему физической защиты информации; 19. разработать политику информационной безопасности предприятия; 20. проанализировать систему компьютерной безопасности предприятия; 21. изучить систему контроля и управления доступом предприятия; 22. ознакомиться с системой защиты персональных данных в организации; 23. 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).		

Приложение 2

Фонд оценочных средств по практической подготовке

Задания по практической подготовке

Примерные практические задания:

1. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие;

2. определить виды информации ограниченного доступа, обрабатываемые предприятием;

3. ознакомиться с формами организации производственного процесса и его технологическим обеспечением;

4. выявить угрозы безопасности предприятия;

5. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации;

6. изучить методы и средства защиты информации, применяемые на предприятии;

7. 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;

8. разработать модель угроз для конкретной информационной системы предприятия;

9. проанализировать методы контроля в области защиты информации, используемые в организации;

10. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия;

11. предложить перечень мероприятий по улучшению системы защиты информации на предприятии.

12. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности;

13. провести анализ безопасности программных продуктов, используемых на предприятии;

14. изучить возможные методы прогнозирования появления уязвимостей в программном коде;

15. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД;

16. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации;

17. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения;

18. спроектировать систему физической защиты информации;

19. разработать политику информационной безопасности предприятия;

20. проанализировать систему компьютерной безопасности предприятия;

21. изучить систему контроля и управления доступом предприятия;

22. ознакомиться с системой защиты персональных данных в организации;

23. изучить виды правонарушений при совершении компьютерных преступлений.

Утверждена в составе Основной
профессиональной образовательной
программы высшего образования

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

Тип практики

учебно-лабораторная практика

Направление подготовки (специальность)

10.03.01 Информационная безопасность

Направленность (профиль) программы

«Техническая защита информации»

1. Общие положения

Программа учебной практики учебно-лабораторная практика (далее – учебная практика) разработана в соответствии с федеральным государственным образовательным стандартом высшего образования (далее – ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, локальными актами университета и с учетом профессионального(-ых) стандарта(-ов) «Специалист по защите информации в автоматизированных системах» (утв. приказом Минтруда России от 15.09.2016 № 522н) и «Специалист по технической защите информации» (утв. приказом Минтруда России от 01.11.2016 № 599н).

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

Учебная практика относится к обязательной части учебного плана основной профессиональной образовательной программы (далее – ОПОП) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, направленность (профиль) «Техническая защита информации».

Объем практики составляет 3 зачетных (-ые) единиц (-ы) (далее - з.е.), или 108 академических часов , в том числе в форме практической подготовки 108 академических часа (-ов).

5. Вид и способы проведения практики; базы проведения практики.

Вид практики – учебная.

Тип практики – учебно-лабораторная практика – определяется типом (-ами) задач профессиональной деятельности, к которому(-ым) готовится выпускник в соответствии с ФГОС ВО и ОПОП.

Способ (-ы) проведения практики путем чередования с реализацией иных компонентов образовательной программы. Базами проведения практики являются профильные организации, в том числе их структурные подразделения, деятельность которых соответствует профилю образовательной программы, на основании договоров, заключенных между университетом и профильной организацией.

Практика может быть организована непосредственно в университете, в том числе в его структурном подразделении, предназначенном для проведения практической подготовки.

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 типом(-ами) задач профессиональной деятельности и компетенциями, которые должны быть сформированы у обучающегося в соответствии с ОПОП.

Цель 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 универсальных, общепрофессиональных и профессиональных компетенций (выбрать нужное) выпускника

в соответствии с выбранным(-и) типом(-ами) задач профессиональной деятельности, к которому(-ым) готовятся обучающиеся в соответствии с ОПОП.

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

Содержание и шифр компетенции	Планируемые результаты обучения		
	Знать	Уметь	Владеть
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	принципы сбора, отбора и обобщения информации	соотносить разнородные явления и систематизировать их в рамках избранных видов деятельности	способностью грамотно, логично, аргументированно формировать собственные суждения и оценки
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	правовые нормы, необходимые для достижения поставленной цели при реализации проекта	определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность, исходя из имеющихся ресурсов, соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности	навыками отбора оптимальных технологий целедостижения; навыками работы с нормативными документами
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	различные приёмы и способы социализации личности и социального взаимодействия	строить отношения с окружающими людьми, с коллегами	способностью определять свою роль в команде на основе использования стратегии сотрудничества для достижения поставленной цели
УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда	планировать своё рабочее время и время для саморазвития, формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей	способностью выстраивать траекторию саморазвития посредством обучения по дополнительным образовательным программам
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития	основы безопасности жизнедеятельности, телефоны служб спасения	оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности	навыками поддержания безопасных условий жизнедеятельности

общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов			
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	основные понятия информатики; назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных	использовать программные и аппаратные средства персонального компьютера; применять программные средства системного, прикладного и специального назначения	навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.); навыками обеспечивать работоспособности операционных систем и прикладных программ
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	основные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства и методы использования	применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства	навыками решения задач профессиональной деятельности с использованием информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	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	пользоваться нормативными документами ФСБ России и ФСТЭК России в области защиты информации	навыками организации и обеспечения режима коммерческой тайны и/или режима секретности

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	основные методы поиска информации по ключевым словам; основные источники информации по вопросам обеспечения информационной безопасности	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	навыками представления результатов научных исследований по вопросам обеспечения информационной безопасности по профилю своей деятельности с использованием современных технических средств в устной и письменной формах
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	современные средства криптографической и технической защиты информации	использовать и настраивать современные средства криптографической и технической защиты информации	навыками решения задач профессиональной деятельности с использованием современных средства криптографической и технической защиты информации
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	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	оценивать информационные риски в информационных системах; проводить расчёты для технико-экономического обоснования проектных решений; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем	методами управления информационной безопасностью информационных систем; методами оценки информационных рисков
ОПК-3.2 Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа	классификацию и особенности применения технических средств защиты информации от несанкционированного доступа и средства антивирусной защиты	устанавливать и настраивать технические средства защиты информации от несанкционированного доступа и средства антивирусной защиты	навыками испытания и обслуживания технических средств защиты информации от несанкционированного доступа и средства антивирусной защиты
ПК-1 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	методы, средства и технологии обеспечения защиты информации в автоматизированных системах	применять методы, средства и технологии обеспечения защиты информации в автоматизированных системах	навыками обеспечения защиты информации в автоматизированных системах в процессе их эксплуатации

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, 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.
Практическая подготовка	
	Разработка пакета организационно-распорядительных документов для организации защиты конфиденциальной информации на предприятии. Установка и настройка программно-аппаратной системы защиты информации «Аккорд», «Аура», «Dallas Lock» и др.
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:

- дневник учебной практики;
- отчет о прохождении учебной практики;

Руководитель практики от Университета и руководитель практики от профильной организации – базы практики представляют характеристику-отзыв / характеристику работы обучающегося.

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

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

8. Учебная литература и ресурсы сети Интернет.

а) основная литература:

https://biblioclub.ru/index.php?page=book&id=90790 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

https://biblioclub.ru/index.php?page=book_red&id=499013 Программно-аппаратные средства защиты информационных систем : учебное пособие : [16+] / Ю. ;Ю. ;Громов, О. ;Г. ;Иванова, К. ;В. ;Стародубов, А. ;А. ;Кадыков. – 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

https://biblioclub.ru/index.php?page=book&id=255851 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:

в) Интернет-ресурсы:

Портал ИСПДн.РУ http://www.ispdn.ru

Журнал «Системный администратор» http://samag.ru/
Сайт ФСБ России – www.fsb.ru
Справочная правовая система «КонсультантПлюс» www.consultant.ru
Журнал «Труды СПИРАН» http://proceedings.spiiras.nw.ru/ojs/index.php/sp
Журнал «Бизнес и информационные технологии». – http://bit.samag.ru
Журнал «Информационные технологии и вычислительные системы». – http://www.jitcs.ru
Журнал «Проблемы информационной безопасности. Компьютерные системы» http://jisp.ru/
Сайт ФСТЭК России – www.fstec.ru
Журнал «Информационные технологии». – http://www.novtex.ru/IT
Банк данных угроз ФСТЭК России https://bdu.fstec.ru
Информационно-правовой портал ГАРАНТ www.garant.ru
Журнал «Безопасность информационных технологий» https://bit.mephi.ru/index.php/bit
Журнал «Прикладная информатика». – http://www.appliedinformatics.ru
Журнал «Информация и безопасность» http://kafedrasib.ru/index.php/informatsiya-bezopasnost
Журнал «Правоведение» http://www.jurisprudence-media.ru/
Журнал «Системный администратор». – http://samag.ru
Журнал «Системы управления бизнес-процессами». – http://journal.itmane.ru
Журнал «Программная инженерия». – http://www.novtex.ru/prin/rus
Журнал «Бизнес-информатика». – https://bijournal.hse.ru
Интернет-Университет Информационных Технологий http://www.intuit.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 «КонсультантПлюс».

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 типом(-ами) задач профессиональной деятельности, к которому(-ым) готовится обучающиеся в результате освоения ОПОП в соответствии с ФГОС ВО.

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 типом(-ами) задач профессиональной деятельности, к решению которых готовятся обучающиеся в соответствии с ОПОП.

Фонд оценочных средств предназначен для оценки:

1) соответствия запланированных и фактически достигнутых результатов освоения практики каждым студентом;

2) уровня освоения компетенций, соответствующих этапу прохождения практики.

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.	УК-1 УК-2 УК-3 УК-6 УК-8 ОПК-1 ОПК-2 ОПК-6 ОПК-8 ОПК-9 ОПК-12 ОПК-3.2 ПК-1	Отчет о прохождении практики
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.		
	Практическая подготовка Разработка пакета организационно-распорядительных документов для организации защиты конфиденциальной информации на предприятии. Установка и настройка программно-аппаратной системы защиты информации «Аккорд», «Аура», «Dallas Lock» и др.		
3	Заключительный этап Подготовка отчета о прохождении учебной практики. Защита отчета.		

Приложение 2

Фонд оценочных средств по практической подготовке

Задания по практической подготовке

Средство защиты от несанкционированного доступа "Аура". Скачайте и разверните виртуальную машину Windows XP. Установите средство защиты от НСД "Аура". Документацию и информацию, а так-же ограничения демо-версии можно найти на странице производителя. Задание после установки: 1. В системе должно быть 2 пользователя: a. User1: максимальный уровень «Для служебного пользования». b. User2: максимальный уровень «Секретно». 2. Должны быть следующие объекты доступа (и соответствующие права и уровни): a. C:\Документы\User1 (Доступ только у User1): i. Открыто (уровень «Открыто»). ii. Для служебного пользования (уровень «Для служебного пользования»). b. C:\Документы\User2 (Доступ только у User2): i. Открыто (уровень «Открыто»). ii. Для служебного пользования (уровень «Для служебного пользования»). iii. Секретно (уровень «Секретно»). c. C:\Документы\Общие (Доступ у всех): i. Открыто (уровень «Открыто»). ii. Для служебного пользования (уровень «Для служебного пользования»). 3. Включить ЗПС и контроль потоков. Включить разграничение доступа, регистрацию действий пользователя, контроль целостности в соответствии с требованиями класса 1В (то, что можно реализовать средствами СЗИ от НСД). 4. Проверку работы всех систем продемонстрировать в виде отчета со скрин-шотами. Смотрите п. 6.2 документации администратора (с. 50) и раздел 17. Там особенности установки при мандатном доступе. Провести анализ ИСПДн "1С: Университет" с использованием методических документов ФСТЭК «Базовая модель угроз безопасности ПДн в ИСПДн» и «Методика определения актуальных угроз безопасности ПДн в ИСПДн»: 1. Провести категорирование информации в ИСПДн "1С: Университет". 2. Провести анализ угроз для рассмотренной ИСПДн "1С: Университет". 3. Провести оценку актуальности выявленных угроз. 4. Определить уровень защищенности ИСПДн "1С: Университет" в соответствии с ПП1119. 5. Предложить мероприятия по обеспечению безопасности ПДн в ИСПДн "1С: Университет" в соответствии с Приказом ФСТЭК № 21 (с учетом дополнений). 6. Анализ угроз и перечень мер загрузить сюда Дополнительные данные по ИСПДн "1С: Университет": 1) Сервер располагается в серверной главного корпуса. 2) Клиенты только в директоратах. Доступ в директораты аналогичен доступу в директорат ИТНИТ. 3)

Максимальный уровень опасности - "средний". 4) При построении модели угроз и оценке актуальности исходите из Ваших субъективных представлений об угрозах.