

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
**федеральное государственное автономное образовательное учреждение высшего
образования «Балтийский федеральный университет имени Иммануила Канта»**
Образовательно-научный кластер «Институт высоких технологий»
Высшая школа физических проблем и технологий

Аннотации программ практик

Шифр: 10.03.01

Направление подготовки: «Информационная безопасность»
Профиль: «Организация и технология защиты информации»

Квалификация (степень) выпускника: бакалавр

Калининград
2023

Аннотации программ практик по направлению подготовки

11.03.02 «Информационная безопасность»

профилю подготовки «Организация и технология защиты информации»

АННОТАЦИЯ рабочей программы практики «Учебно-лабораторная практика» по направлению подготовки 10.03.01 Информационная безопасность профилю подготовки «Организация и технология защиты информации» квалификация выпускника бакалавр	
Вид практики	Учебная.
Тип практики	Учебно-лабораторная практика
Способ проведения практики	Стационарная.
Форма проведения практики	Рассредоточенная
Цель практики	Цель практики: закрепление и расширение теоретических и практических знаний, полученных за время обучения; изучение литературы и нормативно-методической документации по профилю подготовки; ознакомление с содержанием основных работ и исследований, выполняемых в области информационной безопасности; приобретение заданных компетенций для будущей профессиональной деятельности; приобретение первоначальных практических навыков выполнения работ по обслуживанию технических средств защиты информации
Компетенции, формируемые в результате освоения практики	ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности
Результаты освоения образовательной программы (ИДК)	ОПК-2.1. Ориентируется в современных информационных технологиях и программных средствах, в том числе отечественного производства, подходящих для решения задач профессиональной деятельности ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства для решения определенных задач профессиональной деятельности ОПК-2.3. Применяет определенные современные информационные технологии и программные средства, в том числе отечественного производства, при решении конкретных задач профессиональной деятельности ОПК-3.1. Обладает знаниями основ высшей математики, методов численного моделирования, вычислительной техники и языков и технологий программирования ОПК-3.2. Анализирует и выбирает методы высшей математики и численного моделирования для решения конкретных задач профессиональной деятельности ОПК-3.3. Применяет законы высшей математики, методы численного моделирования, вычислительную технику и навыки программирования для решения задач профессиональной деятельности ОПК-4.1. Обладает фундаментальными знаниями основных физических законов, методов получения, накопления, передачи и обработки информации ОПК-4.2. Применяет физические законы для решения задач профессиональной деятельности ОПК-4.3. Выполняет теоретические и экспериментальные исследования объектов профессиональной деятельности ОПК-7.1. Имеет представление об языках и средах программирования; библиотеках программных модулей, шаблонах, классах объектов, используемых при разработке программного обеспечения ОПК-7.2. Анализирует требования, предъявляемые к программному обеспечению, создает блок-схемы алгоритмов функционирования разрабатываемых программных продуктов

	ОПК-7.3. Разрабатывает технические спецификации на программные компоненты и их взаимодействие, владеет языками и средами программирования для разработки алгоритмов и программ для решения задач профессиональной деятельности
Знания, умения и навыки, получаемые в процессе прохождения практики	<p>Знать:</p> <p>основные принципы организации аппаратного обеспечения персональных компьютеров;</p> <p>основных понятий, сущности, принципов организации и особенностей различных операционных систем, в т.ч. системы команд, загрузка программ, управление памятью, адресация, внешние события, многозадачность, синхронизация, обработка транзакций, внешние устройства и управление ими, файловые системы, безопасность</p> <p>о дискретной математике как особом способе познания мира;</p> <p>о моделировании на основе понятий и представлений дискретной математики;</p> <p>о перспективе развития изучаемых разделов дисциплины</p> <p>основы схемотехники и элементную базу цифровых электронных устройств, архитектуру, условия и способы использования микропроцессоров и микропроцессорных систем в специальных радиотехнических системах и устройствах</p> <p>основные концептуальные положения объектно-ориентированного программирования</p> <p>Уметь:</p> <p>устанавливать, настраивать, администрировать и эффективно использовать операционные системы на рабочих станциях и серверах</p> <p>использовать математические модели систем и процессов на основе дискретной математики и проводить необходимые расчеты в рамках построенной модели</p> <p>проводить анализ структурных схем в специальных радиотехнических системах и устройствах</p> <p>разрабатывать программы методом логической декомпозиции</p> <p>Владеть:</p> <p>современными средствами администрирования клиентских и серверных операционных систем</p> <p>методами математической логики, теории множеств, комбинаторики, теории графов, и конечных автоматов</p> <p>методами исследования типовых цифровых устройств, микропроцессоров и микропроцессорных систем</p> <p>практическими навыками работы со стандартными компьютерными программами, используемыми при разработке программного обеспечения</p>
Структура и содержание практики	<p>Подготовительный этап (инструктаж по технике безопасности).</p> <p>Основной этап</p> <p>Сбор фактического и литературного материала, выполнение практических задач.</p> <p>Основной этап</p> <p>Обработка, систематизация фактического и литературного материала</p> <p>Основной этап</p> <p>Цикл 3: индивидуальное задание (вариативно).</p> <p>Заключительный этап</p> <p>Заключительный этап</p> <p>Обработка и анализ полученной информации по итогам тематических экспериментов;</p> <p>Подготовка отчетной документации по итогам производственной практики.</p>
Разработчики	Ветров Игорь Анатольевич, к. т. н., доцент института физико-математических наук и информационных технологий

АННОТАЦИЯ рабочей программы практики «Производственная эксплуатационная практика» по направлению подготовки 10.03.01 Информационная безопасность профилю подготовки «Организация и технология защиты информации» квалификация выпускника бакалавр	
Вид практики	Производственная (нужное выбрать).
Тип практики	Производственная эксплуатационная практика
Способ проведения практики	Стационарная.
Форма проведения практики	Дискретная.
Цель практики	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
Компетенции, формируемые в результате освоения практики	ПК-1. Способен к выполнению работ по установке, настройке, обеспечению бесперебойной работы и техническому обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации ПК-2. Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПК-4. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПК-5. Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПК-6. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности ПК-10. Способен организовывать работу и управлять персоналом, обслуживающим программные, программно-аппаратные (в том числе криптографические) и технические средства и системы защиты информации
Результаты освоения образовательной программы (ИДК)	ПК-1.1. Имеет представление о составе работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-1.2. Выполняет работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-1.3. Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-2.1. Имеет представление о составе программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования ПК-2.2. Осуществляет проверку работоспособности программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования ПК-2.3. Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПК-3.1. Знаком с составом контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПК-3.2. Осуществляет организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПК-3.3. Проводит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации

	<p>ПК-4.1. Имеет представление о составе данных, необходимых для проектирования подсистем и средств обеспечения информационной безопасности</p> <p>ПК-4.2. Осуществляет анализ исходных данных для проектирования и использовать инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности</p> <p>ПК-4.3. Выполняет процедуры технико-экономического обоснования соответствующих проектных решений</p> <p>ПК-5.1. Знаком с составом рабочей технической документации, действующими нормативными и методическими документами</p> <p>ПК-5.2. Применяет технологические платформы, сервисы и информационные ресурсы создания технической документации</p> <p>ПК-5.3. Выполняет работы, связанные с сопровождением технической документации</p> <p>ПК-6.1. Знаком с методами поиска и анализа научно-технической информации</p> <p>ПК-6.2. Анализирует и выбирает необходимую информацию в области информационной безопасности</p> <p>ПК-6.3. Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографию по научно-исследовательской работе с учетом требований информационной безопасности</p> <p>ПК-10.1. Имеет представление о целях и задачах управления персоналом по обеспечению защиты сетей; методике выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД</p> <p>ПК-10.2. Осуществляет постановку задач персоналу по обеспечению защиты СССР от НСД и организывает их выполнение</p> <p>ПК-10.3. Определяет цели, приоритеты, обязанности и полномочия персонала, обслуживающего сооружения и СССР, средства и системы их защиты от НСД</p>
<p>Знания, умения и навыки, получаемые в процессе прохождения практики</p>	<p>Знать:</p> <p>основные понятия теории инфокоммуникационных технологий и методы построения моделей систем связи, основные стандарты построения многоканальных телекоммуникационных систем, принципы устройства стационарных систем связи, построения и функционирования систем передачи информации, современные тенденции развития в области техники и технологий основ цифровых систем передачи (ЦСП), принципы построения многоканальных телекоммуникационных систем, методики и алгоритмы расчета основных разновидностей сетей, сооружений и средств инфокоммуникаций, средства автоматизации расчетов, приемы монтажа и настройки инфокоммуникационного оборудования для организации обмена трафиком на сетях связи базовые принципы, лежащие в основе наиболее распространённых формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах;</p> <p>инструменты в операционных системах, посредством которых в данной системе можно реализовать ту или иную политику безопасности;</p> <p>отечественные и зарубежные стандарты для оценки эффективности систем защиты информации в операционных системах;</p> <p>основные этапы при проведении анализа безопасности компьютерной системы;</p> <p>наиболее популярные на сегодняшний день программно-аппаратные средства защиты информации;</p> <p>принципы функционирования различных программно-аппаратных средств защиты информации</p> <p>методы анализа и оценки защищённости автоматизированных систем;</p> <p>национальные и международные стандарты в области аудита и оценки информационной безопасности;</p> <p>этапы и процедуры аудита информационной безопасности автоматизированных систем управления</p> <p>архитектуру основных типов современных компьютерных систем;</p> <p>структуру и принципы работы современных и перспективных микропроцессоров;</p> <p>принципы работы элементов и функциональных узлов электронной аппаратуры;</p> <p>принципы построения и работы ПЭВМ</p> <p>принципы метрологического обеспечения, стандартизации и сертификации;</p> <p>способы и приёмы наладки, настройки, регулировки и испытания оборудования, тестирование, настройка и обслуживание аппаратно-программных средств;</p> <p>методы и способы проведение всех видов измерений параметров оборудования и сквозных каналов и трактов (настроечных, приёмосдаточных, эксплуатационных и аварийных);</p>

принципы оформления и делопроизводства в области метрологического обеспечения, стандартизации и сертификации телекоммуникаций
современные подходы к управлению информационной безопасностью и направлениях их развития;
основные стандарты, регламентирующие управление информационной безопасностью;
принципы построения систем управления информационной безопасностью;
принципы разработки процессов управления информационной безопасностью;
взаимосвязи отдельных процессов управления информационной безопасностью в рамках общей системы управления информационной безопасностью;
подходы к интеграции системы управления информационной безопасностью в общую систему управления предприятием
назначение, виды и принципы построения организации и управления службы защиты информации

Уметь:

рассчитывать основные характеристики телекоммуникационных систем, учитывать тенденции развития основ цифровых систем передачи (ЦСП), собирать, анализировать исходные данные и квалифицированно проводить расчеты наиболее важных параметров многоканальных телекоммуникационных систем, применять стратегии и сценарии построения и модернизации многоканальных телекоммуникационных систем, проводить типовые расчеты основных разновидностей сетей, сооружений и средств инфокоммуникаций, определять системные принципы развития перечня услуг, сигнализации, нумерации и технического обслуживания, собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов, организовать монтаж и настройку инфокоммуникационного оборудования для организации информационного обмена на сетях связи
строить теоретические модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учётом различных факторов;
анализировать параметры компьютерной системы на соответствие стандартам безопасности;
применять специализированные программные и аппаратные средства для оценки надёжности компьютерной системы;
настраивать различные программно-аппаратные средства защиты информации в соответствии с рекомендациями производителя;
разрабатывать собственные программные средства защиты информации наподобие имеющихся аналогов
разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем;
применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем;
применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы;
проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления
определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств;
работать с современной элементной базой электронной аппаратуры.
определять направления использования ЭВМ определенного класса для решения служебных задач
самостоятельно работать на компьютере и в компьютерных сетях, моделировать на компьютере устройства, системы и процессы с использованием универсальных пакетов прикладных компьютерных программ;
применять принципы метрологического обеспечения и способы инструментальных измерений, используемых в области инфокоммуникационных технологий и систем связи;
организовать и осуществить проверку технического состояния и ресурса оборудования; применять современные методы их обслуживания и ремонта
анализировать текущее состояние информационной безопасности на предприятии с целью разработки требований к разрабатываемым процессам управления информационной безопасностью;

определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью;
применять процессный подход к управлению информационной безопасностью в различных сферах деятельности;
используя современные методы и средства разрабатывать процессы управления информационной безопасностью, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
практически решать задачи формализации разрабатываемых процессов управления информационной безопасностью;
разрабатывать и внедрять системы управления информационной безопасностью и оценивать ее эффективность
применять современные компьютерные технологии для решения профессиональных задач
ориентироваться в сети научных и образовательных порталов сети Интернет;
обрабатывать результаты полученных измерений с помощью математических программных продуктов

Владеть:

способностью использовать нормативную документацию при технической эксплуатации инфокоммуникационных систем, навыками работы с Российской и зарубежной научно-исследовательской литературой по тематике основ цифровых систем передачи (ЦСП), навыками работы с научно-технической информацией для применения отечественного и зарубежного опыта по тематике проекта, первичными навыками типовых расчетов основных разновидностей сетей, сооружений и средств инфокоммуникации, теоретическими и экспериментальными методами исследования с целью освоения новых перспективных технологий передачи цифровых сигналов, сравнительной оценкой различных способов построения многоканальных телекоммуникационных систем, оценкой влияния различных факторов на основные параметры каналов и трактов, первичными навыками типовых расчетов основных разновидностей сетей, сооружений и средств инфокоммуникаций
навыками по реализации формальных моделей безопасности на практике;
приёмами по выявлению «слабых» мест в системе безопасности различных компьютерных систем;
навыками по анализу отчётов, которые предоставляют в ходе своей работы автоматизированные средства, предназначенные для проверки системы безопасности;
навыками по использованию программно-аппаратных средств защиты информации для решения различных практических задач;
навыками работы в команде
способами контроля эффективности реализации политики информационной безопасности организации;
анализом недостатков в функционировании системы защиты информации автоматизированной системы;
способами оценки защищённости автоматизированной системы;
методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации
навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности;
навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования;
навыками формирования структуры СВТ и выбора режимов их функционирования
основными приёмами технической эксплуатации и метрологического обеспечения аппаратуры и систем телекоммуникаций
навыками управления информационной безопасностью простых объектов;
терминологией и процессным подходом построения систем управления информационной безопасностью;
навыками анализа активов организации, их угроз информационной безопасности и уязвимостей в рамках области деятельности системы управления информационной безопасностью;
навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом
навыками работы с пакетами прикладных программ компьютерного моделирования;

	компьютерными технологиями, необходимыми для обмена научной информации
Структура и содержание практики	<p>Подготовительный этап Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации.</p> <p>Прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка</p> <p>Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики.</p> <p>Основной этап</p> <p>Ознакомление с деятельностью предприятия.</p> <p>Основной этап</p> <p>Определение методов и средств защиты информации, используемых на предприятии.</p> <p>Основной этап</p> <p>Выполнение практических заданий. Сбор материалов для отчетной документации. данного предприятия.</p> <p>Заключительный этап</p> <p>Обработка и анализ полученной информации по итогам тематических экспериментов;</p> <p>Подготовка отчетной документации по итогам производственной практики.</p>
Разработчики	Ветров Игорь Анатольевич, к. т. н., доцент института физико-математических наук и информационных технологий

АННОТАЦИЯ рабочей программы практики «Производственная технологическая практика» по направлению подготовки 10.03.01 Информационная безопасность профилю подготовки «Организация и технология защиты информации» квалификация выпускника бакалавр	
Вид практики	Производственная
Тип практики	Производственная технологическая практика
Способ проведения практики	Стационарная
Форма проведения практики	Дискретная
Цель практики	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.
Компетенции, формируемые в результате освоения практики	ПК-4. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПК-5. Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПК-6. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности ПК-7. Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

	<p>ПК-9. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации</p>
<p>Результаты освоения образовательной программы (ИДК)</p>	<p>ПК-4.1. Имеет представление о составе данных, необходимых для проектирования подсистем и средств обеспечения информационной безопасности ПК-4.2. Осуществляет анализ исходных данных для проектирования и использовать инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности ПК-4.3. Выполняет процедуры технико-экономического обоснования соответствующих проектных решений ПК-5.1. Знаком с составом рабочей технической документации, действующими нормативными и методическими документами ПК-5.2. Применяет технологические платформы, сервисы и информационные ресурсы создания технической документации ПК-5.3. Выполняет работы, связанные с сопровождением технической документации ПК-6.1. Знаком с методами поиска и анализа научно-технической информации ПК-6.2. Анализирует и выбирает необходимую информацию в области информационной безопасности ПК-6.3. Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографию по научно-исследовательской работе с учетом требований информационной безопасности ПК-7.1. Знаком с требованиями стандартов в области информационной безопасности ПК-7.2. Создает и ведет справочный ресурс для анализа информационной безопасности объектов ПК-7.3. Осуществляет подготовку технических отчетов по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-9.1. Знаком с нормативными документами в области организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности ПК-9.2. Определяет состав мер по обеспечению информационной безопасности и осуществлять стратегическое планирование процессом их реализации ПК-9.3. Осуществляет организацию и поддержку выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации</p>
<p>Знания, умения и навыки, получаемые в процессе прохождения практики</p>	<p>Знать: архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры; принципы построения и работы ПЭВМ принципы метрологического обеспечения, стандартизации и сертификации; способы и приёмы наладки, настройки, регулировки и испытания оборудования, тестирование, настройка и обслуживание аппаратно-программных средств; методы и способы проведение всех видов измерений параметров оборудования и сквозных каналов и трактов (настроечных, приёмодаточных, эксплуатационных и аварийных); принципы оформления и делопроизводства в области метрологического обеспечения, стандартизации и сертификации телекоммуникаций современные подходы к управлению информационной безопасностью и направлениях их развития; основные стандарты, регламентирующие управление информационной безопасностью; принципы построения систем управления информационной безопасностью; принципы разработки процессов управления информационной безопасностью; взаимосвязи отдельных процессов управления информационной безопасностью в рамках общей системы управления информационной безопасностью; подходы к интеграции системы управления информационной безопасностью в общую систему управления предприятием понятие безопасности информации; основы метрологии и сертификации; правоведение; правовое обеспечение и стандартизацию информационной безопасности Уметь:</p>

определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств;

работать с современной элементной базой электронной аппаратуры.

определять направления использования ЭВМ определенного класса для решения служебных задач

самостоятельно работать на компьютере и в компьютерных сетях, моделировать на компьютере устройства, системы и процессы с использованием универсальных пакетов прикладных компьютерных программ;

применять принципы метрологического обеспечения и способы инструментальных измерений, используемых в области инфокоммуникационных технологий и систем связи;

организовать и осуществить проверку технического состояния и ресурса оборудования; применять современные методы их обслуживания и ремонта

анализировать текущее состояние информационной безопасности на предприятии с целью разработки требований к разрабатываемым процессам управления информационной безопасностью;

определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью;

применять процессный подход к управлению информационной безопасностью в различных сферах деятельности;

используя современные методы и средства разрабатывать процессы управления информационной безопасностью, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;

практически решать задачи формализации разрабатываемых процессов управления информационной безопасностью;

разрабатывать и внедрять системы управления информационной безопасностью и оценивать ее эффективность

разрабатывать организационные и нормативно-методические материалы в целях обеспечения информационной безопасности; унифицировать тексты документов;

оформлять документы в соответствии с требованиями государственных стандартов;

применять отечественные и зарубежные стандарты по обеспечению информационной безопасности; разрабатывать и внедрять новейшие информационные технологии

Владеть:

навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности;

навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования;

навыками формирования структуры СВТ и выбора режимов их функционирования

основными приемами технической эксплуатации и метрологического обеспечения аппаратуры и систем телекоммуникаций

навыками управления информационной безопасностью простых объектов;

терминологией и процессным подходом построения систем управления информационной безопасностью;

навыками анализа активов организации, их угроз информационной безопасности и уязвимостей в рамках области деятельности системы управления информационной безопасностью;

навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом

методикой формирования комплексных мер по защите информации на основе современного законодательства и международных актов и стандартов;

методикой использования компьютерной техники и информационных технологий при составлении и оформлении документации, связанной с международными и Российскими актами и стандартами информационной безопасности

навыками управления информационной безопасностью простых объектов;

терминологией и процессным подходом построения систем управления информационной безопасностью;

навыками анализа активов организации, их угроз информационной безопасности и уязвимостей в рамках области деятельности системы управления информационной безопасностью;

навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом

Структура и содержание практики	<p>Подготовительный этап Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации.</p> <p>Прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка</p> <p>Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики.</p> <p>Основной этап</p> <p>Ознакомление с деятельностью предприятия.</p> <p>Основной этап</p> <p>Определение методов и средств защиты информации, используемых на предприятии.</p> <p>Основной этап</p> <p>Выполнение практических заданий. Сбор материалов для отчетной документации. данного предприятия.</p> <p>Заключительный этап</p> <p>Обработка и анализ полученной информации по итогам тематических экспериментов;</p> <p>Подготовка отчетной документации по итогам производственной практики.</p>
Разработчики	Ветров Игорь Анатольевич, к. т. н., доцент института физико-математических наук и информационных технологий

<p>АННОТАЦИЯ рабочей программы практики «Производственная преддипломная практика» по направлению подготовки 10.03.01 Информационная безопасность профилю подготовки «Организация и технология защиты информации» квалификация выпускника бакалавр</p>	
Вид практики	Производственная
Тип практики	Производственная преддипломная практика
Способ проведения практики	Стационарная.
Форма проведения практики	Дискретная.
Цель практики	Цель практики: углубление профессиональных знаний и адаптация их к условиям конкретного производства, закрепление профессиональных компетенций, приобретение дополнительного опыта практической работы, сбор и обработка материала для написания ВКР
Компетенции, формируемые в результате освоения практики	<p>ПК-1. Способен к выполнению работ по установке, настройке, обеспечению бесперебойной работы и техническому обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации</p> <p>ПК-2. Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p> <p>ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p> <p>ПК-4. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</p> <p>ПК-5. Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p> <p>ПК-6. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>

	<p>ПК-7. Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p> <p>ПК-8. Способен проводить исследования на побочные электромагнитные излучения и наводки технических средств обработки информации, защищенности акустической речевой информации от утечки по техническим каналам</p>
<p>Результаты освоения образовательной программы (ИДК)</p>	<p>ПК-1.1. Имеет представление о составе работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации</p> <p>ПК-1.2. Выполняет работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации</p> <p>ПК-1.3. Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации</p> <p>ПК-2.1. Имеет представление о составе программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования</p> <p>ПК-2.2. Осуществляет проверку работоспособности программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования</p> <p>ПК-2.3. Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p> <p>ПК-3.1. Знаком с составом контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p> <p>ПК-3.2. Осуществляет организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p> <p>ПК-3.3. Проводит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации</p> <p>ПК-4.1. Имеет представление о составе данных, необходимых для проектирования подсистем и средств обеспечения информационной безопасности</p> <p>ПК-4.2. Осуществляет анализ исходных данных для проектирования и использовать инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности</p> <p>ПК-4.3. Выполняет процедуры технико-экономического обоснования соответствующих проектных решений</p> <p>ПК-5.1. Знаком с составом рабочей технической документации, действующими нормативными и методическими документами</p> <p>ПК-5.2. Применяет технологические платформы, сервисы и информационные ресурсы создания технической документации</p> <p>ПК-5.3. Выполняет работы, связанные с сопровождением технической документации</p> <p>ПК-6.1. Знаком с методами поиска и анализа научно-технической информации</p> <p>ПК-6.2. Анализирует и выбирает необходимую информацию в области информационной безопасности</p> <p>ПК-6.3. Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографию по научно-исследовательской работе с учетом требований информационной безопасности</p> <p>ПК-7.1. Знаком с требованиями стандартов в области информационной безопасности</p> <p>ПК-7.2. Создает и ведет справочный ресурс для анализа информационной безопасности объектов</p> <p>ПК-7.3. Осуществляет подготовку технических отчетов по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p> <p>ПК-8.1. Знаком с нормативными правовыми актами, методическими документами, национальными стандартами в области аттестации объектов информатизации на соответствие требованиям по защите информации;</p> <p>ПК-8.2. Имеет представление о технических каналах утечки информации, возникающих за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем</p>

	<p>ПК-8.3. Проводит контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; оценивает защищенность информации от утечки за счет побочных электромагнитных излучений и наводок</p> <p>ПК-8.4. Подготавливает отчетные материалы по результатам контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (протоколы оценки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок)</p>
<p>Знания, умения и навыки, получаемые в процессе прохождения практики</p>	<p>Знать:</p> <p>основные понятия теории инфокоммуникационных технологий и методы построения моделей систем связи, основные стандарты построения многоканальных телекоммуникационных систем, принципы устройства станционных систем связи, построения и функционирования систем передачи информации, современные тенденции развития в области техники и технологий основ цифровых систем передачи (ЦСП), принципы построения многоканальных телекоммуникационных систем, методики и алгоритмы расчета основных разновидностей сетей, сооружений и средств инфокоммуникаций, средства автоматизации расчетов, приемы монтажа и настройки инфокоммуникационного оборудования для организации обмена трафиком на сетях связи базовые принципы, лежащие в основе наиболее распространённых формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; инструменты в операционных системах, посредством которых в данной системе можно реализовать ту или иную политику безопасности; отечественные и зарубежные стандарты для оценки эффективности систем защиты информации в операционных системах; основные этапы при проведении анализа безопасности компьютерной системы; наиболее популярные на сегодняшний день программно-аппаратные средства защиты информации; принципы функционирования различных программно-аппаратных средств защиты информации</p> <p>методы анализа и оценки защищённости автоматизированных систем; национальные и международные стандарты в области аудита и оценки информационной безопасности; этапы и процедуры аудита информационной безопасности автоматизированных систем управления</p> <p>архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры; принципы построения и работы ПЭВМ</p> <p>принципы метрологического обеспечения, стандартизации и сертификации; способы и приёмы наладки, настройки, регулировки и испытания оборудования, тестирование, настройка и обслуживание аппаратно-программных средств; методы и способы проведение всех видов измерений параметров оборудования и сквозных каналов и трактов (настроечных, приёмосдаточных, эксплуатационных и аварийных);</p> <p>принципы оформления и делопроизводства в области метрологического обеспечения, стандартизации и сертификации телекоммуникаций</p> <p>современные подходы к управлению информационной безопасностью и направлениях их развития;</p> <p>основные стандарты, регламентирующие управление информационной безопасностью;</p> <p>принципы построения систем управления информационной безопасностью;</p> <p>принципы разработки процессов управления информационной безопасностью;</p> <p>взаимосвязи отдельных процессов управления информационной безопасностью в рамках общей системы управления информационной безопасностью;</p> <p>подходы к интеграции системы управления информационной безопасностью в общую систему управления предприятием</p> <p>понятие безопасности информации; основы метрологии и сертификации; правоведение; правовое обеспечение и стандартизацию информационной безопасности</p> <p>принципы действия и особенностях излучений антенн и устройств многоканальных систем связи;</p> <p>способы формирования распределений полей излучения</p> <p>Уметь:</p>

рассчитывать основные характеристики телекоммуникационных систем, учитывать тенденции развития основ цифровых систем передачи (ЦСП), собирать, анализировать исходные данные и квалифицированно проводить расчеты наиболее важных параметров многоканальных телекоммуникационных систем, применять стратегии и сценарии построения и модернизации многоканальных телекоммуникационных систем, проводить типовые расчеты основных разновидностей сетей, сооружений и средств инфокоммуникаций, определять системные принципы развития перечня услуг, сигнализации, нумерации и технического обслуживания, собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов, организовать монтаж и настройку инфокоммуникационного оборудования для организации информационного обмена на сетях связи строить теоретические модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учётом различных факторов;

анализировать параметры компьютерной системы на соответствие стандартам безопасности;

применять специализированные программные и аппаратные средства для оценки надёжности компьютерной системы;

настраивать различные программно-аппаратные средства защиты информации в соответствии с рекомендациями производителя;

разрабатывать собственные программные средства защиты информации наподобие имеющихся аналогов

разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем;

применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем;

применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы;

проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления

определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств;

работать с современной элементной базой электронной аппаратуры.

определять направления использования ЭВМ определенного класса для решения служебных задач

самостоятельно работать на компьютере и в компьютерных сетях, моделировать на компьютере устройства, системы и процессы с использованием универсальных пакетов прикладных компьютерных программ;

применять принципы метрологического обеспечения и способы инструментальных измерений, используемых в области инфокоммуникационных технологий и систем связи;

организовать и осуществить проверку технического состояния и ресурса оборудования; применять современные методы их обслуживания и ремонта

анализировать текущее состояние информационной безопасности на предприятии с целью разработки требований к разрабатываемым процессам управления информационной безопасностью;

определять цели и задачи, решаемые разрабатываемыми процессами управления информационной безопасностью;

применять процессный подход к управлению информационной безопасностью в различных сферах деятельности;

используя современные методы и средства разрабатывать процессы управления информационной безопасностью, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;

практически решать задачи формализации разрабатываемых процессов управления информационной безопасностью;

разрабатывать и внедрять системы управления информационной безопасностью и оценивать ее эффективность

разрабатывать организационные и нормативно-методические материалы в целях обеспечения информационной безопасности; унифицировать тексты документов; оформлять документы в соответствии с требованиями государственных стандартов;

применять отечественные и зарубежные стандарты по обеспечению информационной безопасности; разрабатывать и внедрять новейшие информационные технологии
оценивать и производить компьютерный расчет затухания полей, излучаемых приемными и излучающими устройствами;
проводить инструментальные измерения и обосновать диапазонные свойства РЭС к выбору частот для совместной беспомеховой работе в заданной электромагнитной обстановке

Владеть:

способностью использовать нормативную документацию при технической эксплуатации инфокоммуникационных систем, навыками работы с Российской и зарубежной научно-исследовательской литературой по тематике основ цифровых систем передачи (ЦСП), навыками работы с научно-технической информацией для применения отечественного и зарубежного опыта по тематике проекта, первичными навыками типовых расчетов основных разновидностей сетей, сооружений и средств инфокоммуникации, теоретическими и экспериментальными методами исследования с целью освоения новых перспективных технологий передачи цифровых сигналов, сравнительной оценкой различных способов построения многоканальных телекоммуникационных систем, оценкой влияния различных факторов на основные параметры каналов и трактов, первичными навыками типовых расчетов основных разновидностей сетей, сооружений и средств инфокоммуникаций
навыками по реализации формальных моделей безопасности на практике; приёмами по выявлению «слабых» мест в системе безопасности различных компьютерных систем;
навыками по анализу отчётов, которые предоставляют в ходе своей работы автоматизированные средства, предназначенные для проверки системы безопасности;
навыками по использованию программно-аппаратных средств защиты информации для решения различных практических задач;
навыками работы в команде
способами контроля эффективности реализации политики информационной безопасности организации;
анализом недостатков в функционировании системы защиты информации автоматизированной системы;
способами оценки защищённости автоматизированной системы;
методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации
навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности;
навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования;
навыками формирования структуры СВТ и выбора режимов их функционирования
основными приёмами технической эксплуатации и метрологического обеспечения аппаратуры и систем телекоммуникаций
навыками управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления информационной безопасностью;
навыками анализа активов организации, их угроз информационной безопасности и уязвимостей в рамках области деятельности системы управления информационной безопасностью;
навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом
методикой формирования комплексных мер по защите информации на основе современного законодательства и международных актов и стандартов;
методикой использования компьютерной техники и информационных технологий при составлении и оформлении документации, связанной с международными и Российскими актами и стандартами информационной безопасности
компьютерными методами расчета затухания полей от излучающих устройств;
компьютерными методами проведения оценочных работ по ЭМС РЭС
методами работы с измерительной аппаратурой по измерению внутрисистемных и межсистемных взаимных влияний РЭС

<p>Структура и содержание практики</p>	<p>Организационный этап</p> <ol style="list-style-type: none"> 1. Определение базы прохождения практики. 2. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения практики. 3. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 4. Ознакомление с правилами внутреннего распорядка на базе прохождения практики. 5. Получение и согласование индивидуального задания по прохождению практики. 6. Разработка и утверждение индивидуальной программы практики и графика выполнения исследования. 7. Получение документации по практике (программы практики, индивидуального задания на практику, плана-графика прохождения практики и дневника практики с направлением на практику) в сроки, определенные программой. 8. Изучение правовых основ, базовых нормативных и локальных правовых актов, регулирующих деятельность базы практики. <p>Основной этап</p> <ol style="list-style-type: none"> 1. Выполнение производственных заданий. <ul style="list-style-type: none"> • Ознакомление с конкретными видами деятельности в соответствии с положениями структурных подразделений и должностными инструкциями. • Ознакомление с задачами отдела/службы организации базы практики. • Сбор информации и материалов в соответствии с заданием на практику. • Выполнение заданий, поставленных руководителями практики. • Обработка, систематизация и анализ фактического и теоретического материала. 2. Подготовка материалов для ВКР: <ul style="list-style-type: none"> • разработка и анализ эффективности средств и методов защиты информации в информационных системах; • проведение компьютерных экспериментов, демонстрирующих работоспособность программ защиты информации, и получение статистических оценок эффективности разработанных моделей и алгоритмов. <p>Заключительный этап</p> <p>Обработка и анализ полученной информации по итогам тематических экспериментов;</p> <p>Подготовка отчетной документации по итогам производственной практики.</p>
<p>Разработчики</p>	<p>Ветров Игорь Анатольевич, к. т. н., доцент института физико-математических наук и информационных технологий</p>