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. Знает современные информационные технологии, информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности ОПК-2.2. Умеет выбирать современные информационные технологии, информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности ОПК-2.3. Имеет навыки применения современных информационных технологий, информационно-коммуникационные технологий, программных средств системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности ОПК-3.1. Знает основы высшей математики, численного моделирования, вычислительной техники и программирования ОПК-3.2. Умеет выбирать методы высшей математики и численного моделирования для решения задач профессиональной деятельности ОПК-3.3. Имеет навыки применения высшей математики, численного моделирования, вычислительной техники и программирования для решения задач профессиональной деятельности ОПК-4.1. Знает фундаментальные законы природы, основные физические законы, методы накопления, передачи и обработки информации ОПК-4.2. Умеет применять физические законы для решения задач профессиональной деятельности ОПК-4.3. Имеет навыки: теоретического и экспериментального исследования объектов профессиональной деятельности ОПК-7.1. Знает языки и среды программирования; библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения ОПК-7.2. Умеет создавать блок-схемы алгоритмов функционирования разрабатываемых программных продуктов; использовать выбранную среду программирования для написания программного кода для решения задач профессиональной деятельности ОПК-7.3. Владеет языками и средами программирования для разработки алгоритмов и программ для решения задач профессиональной деятельности

Знания, умения и навыки, получаемые в процессе прохождения практики	Знать: основные принципы организации аппаратного обеспечения персональных компьютеров; основных понятий, сущности, принципов организации и особенностей различных операционныхсистем, в т.ч. системы команд, загрузка программ, управление памятью, адресация, внешние события, многозадачность, синхронизация, обработкатранзакций, внешние устройства и управление ими,файловые системы, безопасность о дискретной математике как особом способе познания мира; о моделировании на основе понятий и представлений дискретной математики; о перспективе развития изучаемых разделов дисциплины основы схемотехники и элементную базу цифровых электронных устройств, архитектуру, условия и способы использования микропроцессоров и микропроцессорных систем в специальных радиотехнических системах и устройствах основные концептуальные положения объектно-ориентированного программирования Уметь: устанавливать, настраивать, администрировать и эффективно использовать операционные системы на рабочих станциях и серверах использовать математические моделисистем и процессов на основе дискретной математики и проводитьнеобходимые расчеты в рамкахпостроенной модели проводить анализ структурных схем в специальных радиотехнических системах и устройствах разрабатывать программы методом логическойдекомпозиции Владеть: современными средствами администрированияклиентских и серверных операционных систем методами математической логики, теории множеств, комбинаторики, теории графов, и конечных автоматов методами исследования типовых цифровых устройств, микропроцессоров и микропроцессорныхсистем практическими навыками работы со стандартными компьютерными программами, используемыми при разработке программного обеспечения
Структура и содержание практики	Подготовительный этап (инструктаж по технике безопасности). Основной этап Сбор фактического и литературного материала, выполнение практических задач. Основной этап Обработка, систематизация фактического и литературного материала Основной этап Цикл 3: индивидуальное задание (вариативно). Заключительный этап Заключительный этап Обработка и анализ полученной информации по итогам тематических экспериментов; Подготовка отчетной документации по итогам производственной практики.
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	ПКС-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 ПКС-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПКС-3 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПКС-4 Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПКС-5 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПКС-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 ПКС-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)	ПКС -1.1 Знает состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПКС -1.2 Умеет администрировать работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПКС -1.3 Владеет навыками применения средств контроля работ по установке, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПКС -2.1 Знает состав программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования ПКС -2.2 Умеет осуществлять проверки работоспособности программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования ПКС -2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПКС -3.1 Знает состав контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПКС -3.2 Умеет осуществлять организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПКС -3.3 Владеет навыками аттестации объектов вычислительной техники на соответствие требованиям по защите информации

	ПКС -4.1 Имеет представление о составе данных, необходимых для проектирования подсистем и средств обеспечения информационной безопасности ПКС -4.2 Умеет осуществлять анализ исходных данных для проектирования и использовать инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности ПКС -4.3 Владеет навыками проведения процедуры технико-экономического обоснования соответствующих проектных решений ПКС -5.1 Знает состав рабочей технической документации, действующие нормативные и методические документы ПКС -5.2 Умеет применять технологические платформы, сервисы и информационные ресурсы создания технической документации ПКС -5.3 Владеет навыками сопровождения технической документации ПКС -6.1 Знает методы поиска научно-технической информации ПКС -6.2 Способен выбирать необходимую информацию в области информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности ПКС -6.3 Владеет навыками изучения научно-технической литературы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности ПКС -10.1 Знает цели и задачи управления персоналом по обеспечению защиты сетей; методику выработки и реализации управленческого решения по обеспечению защиты сетей электросвязи от НСД ПКС -10.2 Умеет производить постановку задач персоналу по обеспечению защиты СССЭ от НСД и организовывать их выполнение; производить постановку задач персоналу по обеспечению защиты СССЭ от НСД и организовывать их выполнение ПКС -10.3 Владеет навыками формирования целей, приоритетов, обязанностей и полномочий персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД; формирования целей, приоритетов, обязанностей и полномочий персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД
Знания, умения и навыки, получаемые в процессе прохождения практики	Знать: 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

	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 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, приёмосдаточных, 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 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	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. 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. Основной этап Ознакомление с деятельностью предприятия. Основной этап Определение методов и средств защиты информации, используемых на предприятии. Основной этап Выполнение практических заданий. Сбор материалов для отчетной документации. данного предприятия. Заключительный этап Обработка и анализ полученной информации по итогам тематических экспериментов; Подготовка отчетной документации по итогам производственной практики.
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	ПК-4. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в

результате освоения практики	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 ПК-9. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
Результаты освоения образовательной программы (ИДК)	ПК-4.1. Имеет представление о составе данных, необходимых для проектирования подсистем и средств обеспечения информационной безопасности ПК-4.2. Умеет осуществлять анализ исходных данных для проектирования и использовать инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности ПК-4.3. Владеет навыками проведения процедуры технико-экономического обоснования соответствующих проектных решений ПК-5.1. Знает состав рабочей технической документации, действующие нормативные и методические документы ПК-5.2. Умеет применять технологические платформы, сервисы и информационные ресурсы создания технической документации ПК-5.3. Владеет навыками сопровождения технической документации ПК-6.1. Знает методы поиска научно-технической информации. ПК-6.2. Способен выбирать необходимую информацию в области информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности ПК-6.3. Владеет навыками изучения научно-технической литературы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. ПК-7.1. Знает требования стандартов в области информационной безопасности ПК-7.2. Умеет создавать и вести справочный ресурс для анализа информационной безопасности объектов ПК-7.3. Владеет навыками подготовки технических отчетов по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-9.1. Знает нормативные документы в области организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности ПК-9.2. Умеет определять состав мер по обеспечению информационной безопасности и осуществлять стратегическое планирование процессом их реализации ПК-9.3. Владеет навыками организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации
Знания, умения и навыки, получаемые в процессе прохождения практики	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, приёмосдаточных, 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: 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 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 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	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. 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. Основной этап Ознакомление с деятельностью предприятия. Основной этап Определение методов и средств защиты информации, используемых на предприятии. Основной этап Выполнение практических заданий. Сбор материалов для отчетной документации. данного предприятия. Заключительный этап Обработка и анализ полученной информации по итогам тематических экспериментов; Подготовка отчетной документации по итогам производственной практики.
Разработчики	Ветров Игорь Анатольевич, к. т. н., доцент института физико-математических наук и информационных технологий

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	
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	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-7. Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-8. Способен проводить исследования на побочные электромагнитные излучения и наводки технических средств обработки информации, защищенности акустической речевой информации от утечки по техническим каналам
Результаты освоения образовательной программы (ИДК)	ПК -1.1. Знает состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК -1.2. Умеет администрировать работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК -1.3. Владеет навыками применения средств контроля работ по установке, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК -2.1. Знает состав программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования ПК -2.2. Умеет осуществлять проверки 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. Знает состав контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПК -3.2. Умеет осуществлять организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПК -3.3. Владеет навыками аттестации объектов вычислительной техники на соответствие требованиям по защите информации ПК -4.1. Имеет представление о составе данных, необходимых для проектирования подсистем и средств обеспечения информационной безопасности ПК -4.2. Умеет осуществлять анализ исходных данных для проектирования и использовать инструментальные средства проектирования подсистем и средств обеспечения информационной безопасности ПК -4.3. Владеет навыками проведения процедуры технико-экономического обоснования соответствующих проектных решений ПК -5.1. Знает состав рабочей технической документации, действующие нормативные и методические документы ПК -5.2. Умеет применять технологические платформы, сервисы и информационные ресурсы создания технической документации ПК -5.3. Владеет навыками сопровождения технической документации ПК -6.1. Знает методы поиска научно-технической информации ПК -6.2. Способен выбирать необходимую информацию в области информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности ПК -6.3. Владеет навыками изучения научно-технической литературы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности ПК-7.1. Знает требования стандартов в области информационной безопасности ПК-7.2. Умеет создавать и вести справочный ресурс для анализа информационной безопасности объектов ПК-7.3. Владеет навыками подготовки технических отчетов по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-8.1. Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и

	аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом «высокочастотного облучения» основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах ПК-8.2. Умеет проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; проводить оценку защищенности информации от утечки за счет побочных электромагнитных излучений и наводок ПК-8.3. Владеет навыками проведения контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; подготовки отчетных материалов по результатам контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (протоколов оценки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок)
Знания, умения и навыки, получаемые в процессе прохождения практики	Знать: 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 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 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, приёмосдаточных, 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 принципы действия и особенностях излучений антенн и устройств многоканальных систем связи; способы формирования распределений полей излучения 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 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 оценочныхработ по ЭМС РЭС методами работы с измерительной аппаратурой по измерению внутрисистемных и межсистемных взаимныхвлияний РЭС
Структура и содержание практики	Организационный этап 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. Основной этап 1. Выполнение производственных заданий. • 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: • 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. Заключительный этап Обработка и анализ полученной информации по итогам тематических экспериментов; Подготовка отчетной документации по итогам производственной практики.
Разработчики	Ветров Игорь Анатольевич, к. т. н., доцент института физико-математических наук и информационных технологий