МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

Институт физико-математических наук и информационных технологий

Аннотации программ практик

Шифр: 10.03.01

Направление подготовки: «Информационная безопасность»

Профиль: «Организация и технология защиты информации»

Квалификация (степень) выпускника: бакалавр

Калининград

2020

Аннотации программ практик по направлению подготовки

10.03.01 «Информационная безопасность»

профилю подготовки «Организация и технология защиты информации»

АННОТАЦИЯ рабочей программы практики **«Учебная практика по получению первичных профессиональных умений и навыков»** по направлению подготовки 10.03.01 «Информационная безопасность» профилю подготовки «Организация и технология защиты информации»	
Вид практики	Учебная
Тип практики	Учебная практика по получению первичных профессиональных умений и навыков
Способ проведения практики	Стационарная.
Форма проведения практики	Дискретная.
Цель практики	Цели 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	ОК-5. Способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики ОПК-4. Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации ОПК-7. Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты ПК-2. Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПК-4. Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ПК-8. Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПК-9. Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
Знания, умения и навыки, получаемые в процессе прохождения практики	Знать: об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации основные понятия и теоремы теории информации и кодирования; основные принципы и способы кодирования и декодирования; характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования; методы исследования кодов и их применений в ЭВМ и системах защиты информации способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем

	защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности; способы и механизмы администрирования подсистем информационной безопасности, критерии эффективности применения СЗИ структуру системы управления информационной безопасность; приемы управлению информационной безопасностью методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальнойинформации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области компьютерной безопасности; терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности вкомпьютерной сфере; направления создания правовой базы в области информационной безопасности; области примененияполученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при обработке информации,составляющей государственную тайну место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России законодательство Российской Федерации, государственные стандарты и нормативные документы по защите информации, основные общеметодологические принципы теории информационной безопасности стандарты и нормативные документы по защите информации, в том числе международные Уметь: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации вычислять количество информации в сообщениях дискретного источника канала связи; кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость; классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от

	изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы. выделять процессы управления информационной безопасностью защищаемых объектов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью; выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации; обосновывать структуру системы управления информационной безопасностью в зависимости от характера угроз на объекте применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем; пользоваться современной научно-технической информацией по исследуемымпроблемам и задачам; отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в систем е действующего законодательства, в том числе с помощью систем правовой информации; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности систематизировать информацию, формулировать требования к защищаемым системам на основе требований нормативных и правовых документов Владеть: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования средствами визуализации результатов научного исследования, средствами построения информационных ресурсов современными программными пакетами проведения моделирования на базовом уровне навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; способами, механизмами администрирования средств защиты информации и средств, встроенных в ОС; программным обеспечением сканирования уязвимостей и аудита эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации правилами, процедурами, практические приемы и пр. для управления информационной безопасности системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты методами и средствами минимизации угроз за счет совершенствования процессов управления навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках; навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической документацией на компоненты компьютерных систем на русском и иностранном языках; навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации,составления кратких отчетов, рефератов; разработке специализированной проектной и технической документации профессиональной терминологией в области информационной безопасности средствами поиска, методами обобщения нормативных и методических материалов в сфере своей профессиональной деятельности, средствами поиска,

	обобщения научно-технической информации, нормативных и методических материалов, отечественного и зарубежного опыта в сфере своей профессиональной деятельности
Структура и содержание практики	Подготовительный этап (инструктаж по технике безопасности). Основной этап Ознакомительная информация, собрание Основной этап Инструктаж по технике безопасности. Основной этап Сбор фактического и литературного материала, выполнение практических задач Основной этап Обработка, систематизация фактического и литературного материала Индивидуальное задание (вариативно). Заключительный этап Подготовка отчётной документации по итогам практики. Подготовка дневника практики
Разработчики	доцент ИФМНиИТ, кандидат технических наук, доцент Ветров И. А.

АННОТАЦИЯ рабочей программы практики **«Производственная эксплуатационная практика»** по направлению подготовки 10.03.01 «Информационная безопасность» профилю подготовки «Организация и технология защиты информации»	
Вид практики	Производственная.
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. Производственная практика обеспечивает последовательность процесса формирования у студентов системы профессиональных компетенций в соответствии с профилем подготовки бакалавров, прививает студентам навыки самостоятельной работы по избранной профессии, дает возможность определения темы выпускной квалификационной работы и ее выполнения.
Компетенции, формируемые в результате освоения практики	ОПК-4. Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации ОПК-5. Способностью использовать нормативные правовые акты в профессиональной деятельности ОПК-7. Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты ПК-1. Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-2. Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПК-3. Способностью администрировать подсистемы информационной безопасности объекта защиты ПК-4. Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ПК-5. Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ПК-6. Способностью принимать участие в организации и проведении

	контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПК-7. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПК-8. Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПК-9. Способностью 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. Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-11. Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов ПК-12. Способностью принимать участие в проведении экспериментальных исследований системы защиты информации ПК-13. Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ПК-14. Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности ПК-15. Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
Знания, умения и навыки, получаемые в процессе прохождения практики	Знать: об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации структуру системы управления информационной безопасность; приемы управлению информационной безопасностью методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз основные понятия и теоремы теории информации и кодирования; основные принципы и способы кодирования и декодирования; характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования; методы исследования кодов и их применений в ЭВМ и системах защиты информации. основные классы кодов, их параметры и алгоритмы кодирования/декодирования особенности различных подходов к организации информационного обеспечения особенности научного исследования в области информатики и вычислительной техники, важнейшие методологические принципы научного исследования на базовом уровне способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации;

	защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности этапы и модели жизненного цикла информационных систем; корпоративные стандарты и методики; принципы хранения, защиты, передачи и получения информации в корпоративных сетях правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальнойинформации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области компьютерной безопасности 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 терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности вкомпьютерной сфере направления создания правовой базы в области информационной безопасности; области примененияполученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при обработке информации,составляющей государственную тайну основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности физические основы образования технических каналов утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации; основные программные и аппаратные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; методики и стандарты оценки погрешностей измерений; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного

	копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации назначение, виды и принципы построения организации и управления службы защиты информации основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии Уметь: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации выделять процессы управления информационной безопасностью защищаемых объектов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью; выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации; обосновывать структуру системы управления информационной безопасностью в зависимости от характера угроз на объекте вычислять количество информации в сообщениях дискретного источника канала связи; кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость; оценивать количество информации, вероятность ошибки на выходе канала связи и вероятность ошибочного декодирования; выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач проектировать, оценивать и реализовывать информационное обеспечение информационных систем осуществлять корректную постановку задачи исследования в области информатики и вычислительной техники на базовом уровне классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации; обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности разрабатывать структуру распределенных систем; создавать клиент-серверные приложения для распределенных систем; проектировать хранилища данных; выполнять анализ корпоративных данных

	применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем 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 пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфики объекта защиты; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; решать типовые задачи в области структурного анализа информационных процессов и систем; проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; проводить классификацию экспериментов; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки погрешностей результатов экспериментов; применять системы компьютерной математики для решения типовых задач разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять основные теоретико-числовые методы к решению задачам защиты информации

	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 основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии 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 осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; оценивать эффективность системы защиты информации Владеть: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования правилами, процедурами, практические приемы и пр. для управления информационной безопасности системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты методами и средствами минимизации угроз за счет совершенствования процессов управления основными методами кодирования и декодирования информации для различных задач средствами визуализации результатов научного исследования, средствами построения информационных ресурсов современными программными пакетами проведения моделирования на базовом уровне навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей средствами защиты информации в процессе хранения и передачи данных и методами их тестирования; методикой определения эффективности предложенных решений с учетом снижения рисков навыками защиты информации в корпоративных сетях связи навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках 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 навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической документацией на компоненты компьютерных систем на русском и иностранном языках навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации,составления кратких отчетов, рефератов; разработки специализированной проектной и технической документации способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации; навыками установки, настройки и обслуживания программно-аппаратных средств защиты информации; навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов; навыками оценки защищенности объектов информатизации навыками организации охраны на объектах информатизации; навыками применения технических средств защиты информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; умение пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; навыками аналитического и численного решения задач; методами проведения физического эксперимента с последующей обработкой их результатов; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки 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 навыками работы **с** пакетами прикладных программ компьютерного моделирования; компьютерными технологиями, необходимыми для обмена научной информации навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации
Структура и содержание практики	Подготовительный (ознакомительный) этап Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации. Прохождение инструктажа по ознакомлению с требованиями охраны труда,

	техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики. Основной этап Ознакомление с деятельностью предприятия. Определение методов и средств защиты информации, используемых на предприятии. Выполнение практических заданий. Сбор материалов для отчетной документации. данного предприятия. Заключительный этап Подготовка отчетной документации, получение характеристики о работе руководителя практики, представление отчетной документации, прохождение промежуточной аттестации по практике. Систематизация и анализ выполненных заданий.
Разработчики	доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.

АННОТАЦИЯ рабочей программы практики **«Производственная проектно-технологическая практика»** по направлению подготовки 10.03.01 «Информационная безопасность» профилю подготовки «Организация и технология защиты информации»	
Вид практики	Производственная.
Тип практики	Производственная проектно-технологическая практика
Способ проведения практики	Стационарная.
Форма проведения практики	Дискретная.
Цель практики	Цели практики: - закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла базовой и вариативной частей, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; - изучение информационной структуры предприятия, как объекта информатизации; - изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; - формирование навыков самостоятельного решения поставленных производственных задач; - выбор темы выпускной квалификационной работы и ее выполнение.
Компетенции, формируемые в результате освоения практики	ПК-7. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПК-8. Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
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 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 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
Структура и содержание практики	Подготовительный (ознакомительный) этап Проведение установочной конференции в форме контактной работы, знакомство обучающегося с программой практики, индивидуальным заданием, рабочим графиком (планом) проведения практики, с формой и содержанием отчетной документации, прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка. Ознакомление с порядком защиты отчета по производственной практике и требованиями к оформлению отчета по учебной практике. Подбор материала для прохождения практики Основной этап Ознакомление с деятельностью предприятия. Определение методов и средств защиты информации, используемых на предприятии. Выполнение практических заданий. Сбор материалов для отчетной документации, обработка и систематизация фактического и литературного материала; наблюдения; измерения и другие, выполняемые обучающимся самостоятельно виды работ. Заключительный этап Подготовка отчетной документации, получение характеристики о работе и (или) характеристики – отзыва руководителя практики от университета, представление отчетной документации.
Разработчики	доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.

АННОТАЦИЯ рабочей программы практики «**Производственная преддипломная практика»** по направлению подготовки 10.03.01 «Информационная безопасность» профилю подготовки «Организация и технология защиты информации»	
Вид практики	Производственная.
Тип практики	Производственная преддипломная практика
Способ проведения практики	Стационарная
Форма проведения практики	Дискретная
Цель практики	Цели практики: - закрепление знаний и умений, полученных в процессе теоретического обучения, овладение методикой обеспечения информационной безопасности предприятия (организации), проектирования, внедрения и эксплуатации отдельных задач и подсистем комплексной системы защиты информации предприятия (организации). - приобретение практических навыков работы в качестве специалиста ИБ предприятия (организации); приобретение навыков обслуживания средств ЗИ в

	ЭВМ, сетях ЭВМ и автоматизированных информационных системах; приобретение практического опыта разработки компонентов КСЗИ предприятия (организации); - приобретение навыка системного подхода при проектировании КСЗИ и отдельных ее подсистем; - приобретение навыков исследовательской и аналитической работы в области информационной безопасности. - приобретение практических навыков и опыта самостоятельной профессиональной деятельности. - сбор необходимых материалов для написания выпускной квалификационной работы - приобщение студента к социальной среде предприятия с целью приобретения социально-личностных компетенций, необходимых для работы в профессиональной сфере
Компетенции, формируемые в результате освоения практики	ПК-1. Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-2. Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ПК-3. Способностью администрировать подсистемы информационной безопасности объекта защиты ПК-4. Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ПК-5. Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ПК-6. Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ПК-7. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ПК-8. Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов ПК-9. Способностью 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. Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-11. Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов ПК-12. Способностью принимать участие в проведении экспериментальных исследований системы защиты информации ПК-13. Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ПК-14. Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности ПК-15. Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ПКУ-1. Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики
Знания, умения и навыки, получаемые в процессе прохождения практики	**Знать**: теоретические основы построения клиент-серверных веб-приложений, общие методы программирования механизмы реализации сетевых угроз по протоколам передачи данных HTTP, FTP, а также известные уязвимости веб-серверов

	способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности этапы и модели жизненного цикла информационных систем; корпоративные стандарты и методики; принципы хранения, защиты, передачи и получения информации в корпоративных сетях правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальнойинформации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области компьютерной безопасности 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 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 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 терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности вкомпьютерной сфере направления создания правовой базы в области информационной безопасности; области применениянолученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при обработке информации,составляющей государственную тайну основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые

	понятия о методах и средствах защиты информации; международные стандарты информационной безопасности основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности физические основы образования технических каналов утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации; основные программные и аппаратные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности; основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; методики и стандарты оценки погрешностей измерений; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации; назначение, виды и принципы построения организации и управления службы защиты информации основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии **Уметь**: использовать полученные теоретические знания для решения конкретных прикладных задач, программировать клиент-серверные приложения с применением СУБД для обработки данных, находитьи исправлять ошибки в программном коде конфигурировать клиент-серверное программное обеспечение с учетом требуемых параметров сетевой безопасности, анализировать возможные каналы утечки информации классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий

	применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации; обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности разрабатывать структуру распределенных систем; создавать клиент-серверные приложения для распределенных систем; проектировать хранилища данных; выполнять анализ корпоративных данных применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицироватьзащищаемую информацию по видам тайн и степеням конфиденциальности; разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения посовершенствованию системы управления информационной безопасностью компьютерных систем 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 пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфики объекта защиты; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; решать типовые задачи в области структурного анализа информационных процессов и систем; проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; проводить классификацию экспериментов; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки погрешностей результатов экспериментов; применять системы компьютерной математики для решения типовых задач разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять основные теоретико-числовые методы к решению задачам защиты информации

	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 осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; оценивать эффективность системы защиты информации 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**: практическими навыками конфигурирования и администрирования веб-серверов, а также навыками настройки систем управления контентом практическими навыками, по оценке защищенности веб-приложений навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей средствами защиты информации в процессе хранения и передачи данных и методами их тестирования; методикой определения эффективности предложенных решений с учетом снижения рисков навыками защиты информации в корпоративных сетях связи навыками работы с нормативными правовыми актами; навыкамиработы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках 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 навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической документацией на компоненты компьютерных систем на русском и иностранном языках навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации,составления кратких отчетов, рефератов; разработки специализированной проектной и технической документации способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации; навыками установки, настройки и обслуживания программно-аппаратных средств защиты информации; навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками

	консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов; навыками оценки защищенности объектов информатизации навыками организации охраны на объектах информатизации; навыками применения технических средств защиты информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; умение пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; навыками аналитического и численного решения задач; методами проведения физического эксперимента с последующей обработкой их результатов; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки 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 навыками работы **с** пакетами прикладных программ компьютерного моделирования; компьютерными технологиями, необходимыми для обмена научной информации навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации
Структура и содержание практики	Подготовительный (ознакомительный) этап Проведение организационного собрания. Получение задания на практику. Ознакомление с заданием, планирование работы. Проведение инструктажа по ОТ и ТБ на рабочем месте. Основной этап Сбор, обработка и систематизация фактического и литературного материала, в т.ч. лекций, практических занятий, методических указаний и т.д. Индивидуальное задание (вариативно). Практические работы по теме задания на практику Проведение практических работ (например, разработка программных средств, информационных систем, установка и конфигурирование необходимого программного обеспечения и оборудования и др. Заключительный этап Составление отчёта по практике.
Разработчики	доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.