МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Высшая школа компьютерных наук и прикладной математики

АННОТАЦИИ РАБОЧИХ ПРОГРАММ ПРАКТИК

Шифр: 10.05.01

Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»

Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2018

Аннотации рабочих программ практик по
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

АННОТАЦИЯ рабочей программы «Учебная практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности» для студентов 1,2,3 курса очной формы обучения по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Вид практики	Учебная
Тип практики	Учебно-лабораторная
Способ проведения практики	Стационарная
Форма проведения практики	Непрерывная
Цель практики	Целью учебной практики является приобретение практических навыков по реализации базовых теоретико-числовых алгоритмов в математическом пакете, получение навыков по отладке и тестированию разрабатываемых программ, использованию компьютерных технологий и программно-аппаратных средств, применяемых для исследования и обеспечения безопасности компьютерных систем. Знания и практические навыки, полученные из курса учебной практики, используются студентами при выполнении курсовых работ.
Компетенции, формируемые в результате освоения практики	ОК-6 - Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия; ОПК-7 - Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения ОПК-8 - Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач ОПК-10 - Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах ПСК-2.1 - Способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации
Знания, умения и навыки, получаемые в процессе прохождения практики	В результате прохождения практики обучающийся должен: **Знать:** • нормы корректного поведения в обществе; социально-культурные характеристики основных этносов; • современные информационные методики и технологии; перечень и возможности распространённых систем компьютерной алгебры; методы математической обработки информации, используемые при решении задач защиты информации; • языки программирования различного уровня, их назначение и возможности; системы и методы построения компьютерных программ для

	задач защиты информации; перечень и возможности современных инструментальных средств решения задач в области информационной безопасности; • основные математические модели преобразования информации в компьютерных системах; основные алгоритмы обработки информации в её представлении на языках программирования высокого уровня; основные блоки и структуру алгоритмов, реализуемых на языках программирования высокого уровня; • перспективные методы криптографической защиты информации и помехоустойчивого кодирования; принципы функционирования и возможности перспективных инструментальных средств и компьютерных технологий для реализации вычислительных алгоритмов; структуры данных и методы построения вычислительных алгоритмов в алгебраических структурах, специфичных для перспективных систем защиты информации; **Уметь:** • толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей и на этой основе грамотно строить взаимоотношения с членами трудового коллектива; планировать и осуществлять производственную деятельность в коллективе; • грамотно применять математические пакеты компьютерной алгебры для решения вычислительных задач в области защиты информации; использовать инструментарий операционных систем для проектирования простейших криптографических алгоритмов; • правильно строить алгоритмы и компьютерные программы с использованием различных инструментальных средств; • строить вычислительные алгоритмы, используя численные методы моделирования физических явлений и процессов; строить вычислительные алгоритмы на алгебраических структурах с помощью математических пакетов, в частности, с помощью систем компьютерной алгебры; проводить анализ вычислительной эффективности алгоритма, включая анализ быстродействия и объём необходимой памяти • анализировать корректность и быстродействие вычислительных алгоритмов, специфичных для перспективных систем защиты информации; **Владеть:** • навыками урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий при планировании и реализации производственной деятельности трудового коллектива. • практическими навыками применения компьютерных технологий для формирования алгоритмов и проведения вычислений, связанных с защитой информации • языками программирования различного уровня; практическими навыками использования различных систем и методов программирования для решения профессиональных, исследовательских и прикладных задач в области защиты информации. • навыками написания алгоритмов на языках программирования высокого уровня; навыками реализации алгоритмов с помощью математических пакетов, в частности, с помощью систем компьютерной алгебры; навыками анализа вычислительной эффективности алгоритмов • практическими навыками построения вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования.

Структура и содержание практики	**Подготовительный этап:** 1. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения практики. 2. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 3. Ознакомление с правилами внутреннего распорядка на базе прохождения практики. 4. Получение и согласование индивидуального задания по учебной практике. 5. Получение документации по практике (программы практики и индивидуального задания на практику) в сроки, определенные программой. **Производственный этап:** 1. Ознакомление с компьютерными, вычислительными и программно-аппаратными средствами, необходимыми для выполнения задания, побор и анализ литературы в соответствии с заданием. 2. Изучение средств математических пакетов, инструментария операционной системы, свободно распространяемых программных средств для реализации алгоритмов, связанных с защитой информации; изучение программно-аппаратных средств защиты информации. 3. Формальное представления алгоритмов в псевдокоде или в виде блок-схемы. 4. Реализация алгоритмов средствами математического пакета, средствами операционной системы или с помощью свободно распространяемых программных средств. 5. Описание программно-аппаратного средства для защиты от несанкционированного доступа, описание его работы, настройка и тестирование. **Заключительный этап:** 1. Подготовка отчета по учебной практике, представления отчета и прилагаемых документов для защиты. 2. Прохождение промежуточной аттестации по результатам прохождения практики.
Разработчики	Киршанова Е.А., PhD, доцент

АННОТАЦИЯ
рабочей программы
«Производственная практика по получению профессиональных умений и опыта профессиональной деятельности»
для студентов 4,5 курса
очной формы обучения
по специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»
квалификация выпускника: специалист по защите информации

Вид практики	Производственная практика
Тип практики	Проектно-технологическая
Способ проведения практики	Стационарная
Форма проведения практики	Непрерывная
Цель практики	Целью производственной практики является получение профессиональных умений и опыта профессиональной деятельности**.**

	Задачами практики являются: - закрепление, расширение, углубление и систематизация знаний, полученных при изучении дисциплин на основе изучения деятельности конкретной организации; - - приобретение первоначального практического опыта работы; - - подготовка к выполнению ВКР.
Компетенции, формируемые в результате освоения практики	ОК-4 - Способность использовать основы правовых знаний в различных сферах деятельности; ОК-6 - Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия; ОК-7 - Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности; ОПК-5 - Способность использовать нормативные правовые акты в своей профессиональной деятельности; ПК-5 - Способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации ПК-6 - Способность участвовать в разработке проектной и технической документации; ПК-8 - Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы; ПК-9 - Способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы; ПК-10 - Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-11 - Способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации; ПК-12 - Способность проводить инструментальный мониторинг защищенности компьютерных систем; ПК-13 - Способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности; ПК-14 - Способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа; ПК-15 - Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы; ПК-16 - Способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем; ПК-17 - Способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного

	обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение; ПК-18 - Способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-19 - Способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации; ПК-20 - Способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций
Знания, умения и навыки, получаемые в процессе прохождения практики	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать*:** - проблемы и задачи, возникающие в сфере правового регулирования; основные положения законов и иных правовых актов, регулирующих взаимоотношения между субъектами в различных сферах деятельности; функции и сферы ответственности регулирующих органов; - нормы корректного поведения в обществе; социально-культурные характеристики основных этносов; - нормы русского языка и одного из иностранных языков; правила построения докладов и презентаций в профессиональной области защиты информации; - проблемы и задачи, возникающие в сфере правового регулирования информационной безопасности; основные положения законов и иных правовых актов, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; функции и сферы ответственности регулирующих органов в области информационной безопасности; - методы и сертифицированные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем; способы и средства антивирусной защиты; принципы построения и оценки эффективности криптографических алгоритмов, а также разрешённые к применению средства криптографической защиты; процедуры распределения и сертификации криптографических ключей; типовые схемы обеспечения информационной безопасности компьютерных систем; - перечень необходимой проектной и технической документации, регламентирующей построение эффективных систем защиты информации; правила и этапы разработки проектной и технической документации в области обеспечения информационной безопасности компьютерных систем; - современные информационные методики и технологии, методы математической обработки информации, методы теоретического и экспериментального исследования, стандарты и нормативы в области информационной безопасности. ***уметь*:** - правильно толковать законы и иные правовые акты, особенно в сфере профессиональной деятельности, связанной с защитой информации; - толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей и на этой основе грамотно строить взаимоотношения с членами трудового коллектива; планировать и осуществлять производственную деятельность в коллективе;

	- использовать средства Microsoft Office и/или иные компьютерные программы для создания текстов и презентаций; - правильно толковать законы и иные правовые акты в области защиты информации; - осуществлять анализ уровней информационной защищённости компьютерных систем; разрабатывать комплексные проекты обеспечения информационной безопасности компьютерных систем; готовить научно-техническую документацию, презентации, научные публикации по результатам проектирования; - выполнять расчётные работы и подготовку текстовых и графических документов средствами Microsoft Office и/или иными средствами; - грамотно применять изученные математические методы, математические пакеты для обработки, детального анализа и систематизации криптографической информации, строить схемы и модели под-систем информационной безопасности компьютерной системы. ***владеть:*** - применения законов и иных правовых актов в задачах анализа правовых норм и положений в области информационной безопасности. - урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий при планировании и реализации производственной деятельности трудового коллектива. - применения компьютерных средствам создания текстов и презентаций; навыками выступления с докладами и ведения научных дискуссий в профессиональной сфере защиты информации. - применения законов и иных правовых актов в задачах анализа правовых норм и положений, регламентирующих функционирование комплексных систем защиты информации. - решения задач обеспечения информационной безопасности компьютерных систем с использованием всего комплекса программно-аппаратных средств на конкретном рабочем месте в качестве исполнителя или стажера; навыками проектирования систем защиты информации и подготовки соответствующей научно-технической документации. - проектирования подсистем информационной безопасности; навыками организации работы по проектированию систем информационной безопасности. - проектирования систем защиты информации, навыками применения современных компьютерных технологий, построения математических моделей информационных потоков, возникающих при построении криптографической инфра-структуры, навыками оценки эффективности их применения.
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 отчёта по практике: • разработка и исследование математических моделей процессов и объектов, возникающих в системах компьютерной безопасности; • разработка и анализ эффективности вычислительных алгоритмов, реализующих процессы обработки информации в компьютерных системах; • проведение компьютерных экспериментов, демонстрирующих работоспособность компьютерных программ, и получение статистических оценок эффективности разработанных моделей и алгоритмов. 3. Ведение дневника практики. **Заключительный этап:** 1. Выявление возможных недостатков в работе подразделения – места прохождения практики, их оценка и разработка предложений по совершенствованию существующего порядка работы, а также по внедрению новых методов работы. 2. Подготовка отчета о прохождении практики, представления отчета по практики и прилагаемых документов для защиты. 3. Защита отчёта по практике
Разработчики	Доцент, к.т.н., доцент ***Ветров Игорь Анатольевич***

АННОТАЦИЯ
рабочей программы
«Производственная практика (научно-исследовательская работа)»
для студентов 6 курса
очной формы обучения
специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации
квалификация (степень) выпускника: *специалист*

Вид практики	Производственная практика
Тип практики	Научно-исследовательская работа
Способ проведения практики	Стационарная

Форма проведения практики	Непрерывная
Цель практики	***Целью*** НИР является освоение студентом методики проведения всех этапов научно-исследовательской работы – от постановки задачи исследования; через исследование и разработку средств и систем защиты информации, доказательный анализ защищённости компьютерных систем от вредоносных программно-технических воздействий в условиях существования угроз в информационной сфере; через рациональное планирование эксплуатации систем управления и обеспечения информационной безопасности; до подготовки отчётов по теме или её разделу. ***Задачами*** НИР являются: 1) развитие способностей студента к самостоятельной аналитической работе; 2) освоение процедур планирования, проведения и анализа результатов научных исследований в соответствии с заданием на НИР; 3) формирование и развитие у студентов устойчивого интереса к профессиональной деятельности, потребности в самообразовании; 4) разработка научной (теоретической части) выпускной квалификационной работы в соответствии с выбранной темой.
Компетенции, формируемые в результате освоения практики	ОК-8 - Способность к самоорганизации и самообразованию; ОК-9 - Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности; ОПК-1 - Способность анализировать физические явления и процессы при решении профессиональных задач; ОПК-4 - Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами; ОПК-10 - Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах; ПК-1 - Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности; ПК-2 - Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований; ПК-7 - Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем; ПСК-2.3 - Способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.4 - Способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
Знания, умения и навыки, получаемые в процессе	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать*:** - необходимые математические методы для решения задач обеспечения защиты информации;

прохождения практики	- методику разработки программ на языках высокого и низкого уровня; - принципы работы с научной литературой, методы поиска научно-технической информации; - методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты; ***уметь*:** - применять совокупность необходимых математических методов для решения задач обеспечения защиты информации; - применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; - осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов; - решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности; ***владеть:*** - разработкой, обоснованием и реализацией на практике процедур решения задач обеспечения защиты информации; - обоснованным выбором инструментария программирования и способов организации навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы; - навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.
Структура и содержание практики	Организационный этап: 1. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения НИР. 2. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 3. Ознакомление с правилами внутреннего распорядка на базе прохождения НИР. 4. Получение и согласование индивидуального задания по прохождению НИР. 5. Составление индивидуального плана НИР совместно с научным руководителем: выбор и обоснование текущей темы исследования; составление рабочего плана и графика выполнения исследования.

	6. Получение документации по НИР (программа НИР и дневник НИР) в сроки, определенные программой. Основной этап: 1. Подготовка к проведению научного исследования: ознакомление со структурой и принципами работы исследуемых компьютерных систем, взаимосвязей между информационными потоками; постановка целей и конкретных задач; формулировка рабочих гипотез; обзор и анализ литературы по теме исследования, сбор информации. 2. Проведение экспериментального исследования: компьютерное моделирование и статистический анализ уровней защищённости компьютерных систем, вычислительной эффективности алгоритмов, качества псевдослучайных последовательностей. 3. Проведение теоретического исследования: разработка структурных схем, математических моделей, протоколов обмена информацией; анализ свойств математических моделей; анализ и разработка алгоритмов; планирование компьютерных экспериментов; компьютерное моделирование алгоритмов. 4. Обработка, систематизация и анализ полученных теоретических результатов и результатов компьютерного моделирования, проверка корректности разработанных алгоритмов; проверка работоспособности комплекса программ. 5. Анализ возможности публичного представления результатов НИР, возможности внедрения результатов исследования в проектную деятельность, инженерную практику, в производство. Заключительный этап: 1. Подготовка отчета о НИР, представления отчета по НИР и прилагаемых документов для защиты 2. Защита отчёта по практике
Разработчики	Доцент, к.т.н., доцент ***Ветров Игорь Анатольевич***

АННОТАЦИЯ
рабочей программы
«Производственная преддипломная практика»
для студентов 6 курса
очной формы обучения
по специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»
квалификация выпускника: специалист по защите информации

Вид практики	Производственная практика
Тип практики	Преддипломная
Способ проведения практики	Стационарная
Форма проведения практики	Непрерывная
Цель практики	***Целью*** преддипломной практики является 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. ***Задачи*** преддипломной практики: • развитие навыков студента к применению знаний и умений, полученных в результате теоретической подготовки, к выполнению практических заданий в области обеспечения компьютерной безопасности,

	управления информационной безопасностью, эксплуатации технических и программно-аппаратных средств защиты информации; • развитие умения анализировать существующие системы компьютерной (информационной) безопасности на предмет стойкости, эффективности и соответствия нормативным документам; • развитие навыков эскизного и технического проектирования систем (подсистем, элементов) обеспечения компьютерной (информационной) безопасности, систем управления информационной безопасностью, планирования работы систем эксплуатации технических и программно-аппаратных средств защиты информации; • завершение разработки научной (теоретической части) ВКР, а также сбор и подготовка данных для прикладной части ВКР в соответствии с выбранной темой.
Компетенции, формируемые в результате освоения практики	ОК-5 - Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; ОПК-9 - - Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации; ПК-3 - Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; ПК-4 - Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем ПК-8 - Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы ПСК-2.2 - Способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах ПСК-2.5 - Способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации
Знания, умения и навыки, получаемые в процессе прохождения практики	В результате прохождения практики обучающийся должен: ***знать*:** - роль и значение компьютерной безопасности в обеспечении интересов России и её граждан; характер профессиональной деятельности по обеспечению информационной безопасности в условиях информационного противоборства; проблемы и задачи, возникающие при обеспечении информационной безопасности предприятия и защиты персональных данных. - основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; типы и структуру моделей управления информационными потоками в компьютерных системах; классификацию угроз безопасности для компьютерных систем; - отечественные и зарубежные стандарты в области компьютерной безопасности; основные положения законов и иных правовых актов РФ, регулирующих взаимоотношения между субъектами в сфере информационной безопасности - типы и структуру моделей управления информационными потоками в компьютерных системах; классификацию угроз безопасности для компьютерных

	систем; проблемы и задачи в сфере обеспечения информационной безопасности компьютерных систем; - современные информационные методики и технологии, методы математической обработки информации, методы теоретического и экспериментального исследования, стандарты и нормативы в области информационной безопасности; типовую структуру и методы создания подсистем информационной безопасности компьютерных систем различного профиля; - типовые математические методы и алгоритмы, применяемые в системах защиты информации в компьютерных системах; типовые и стандартизованные оценки эффективности средств и методов защиты информации; - номенклатуру и основные характеристики сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; математические методы и алгоритмы, применяемые в программно-аппаратных средствах защиты информации; перспективные математические методы защиты информации; ***уметь*:** - объяснять познавательную и практическую сущность математических, компьютерных и технических методов защиты информации как мотивационной основы профессиональной деятельности - строить модели компьютерных систем с дискреционным управлением доступом; строить модели изолированной программной среды; строить модели компьютерных систем с мандатным управлением доступом; строить модели безопасности информационных потоков; строить модели компьютерных систем с ролевым управлением доступом; - проводить анализ и оценку уровней защищённости компьютерных систем; - строить модели управления информационными потоками в компьютерных системах; проводить анализ и оценку уровней защищённости компьютерных систем; - грамотно применять современные математические методы и математические пакеты для обработки, анализа и систематизации информации в компьютерных системах, строить схемы и модели подсистем информационной безопасности компьютерной системы; - оценивать стойкость различных типов криптосистем; оценивать быстродействие вычислительных алгоритмов; - осуществлять самостоятельную проектно-аналитическую работу; проводить сравнительный анализ эффективности математических методов и алгоритмов; ***владеть*:** - простейшими математическими методами обеспечения информационной безопасности; методикой применения основных правовых актов, регулирующих сферу информационной безопасности. - методикой разработки политики безопасности и построения соответствующих моделей управления информационными потоками в компьютерных системах - методикой анализа и оценки уровней защищённости компьютерных систем с использованием стандартов; навыками подготовки отчётов и представления результатов оценки уровней защищённости компьютерных систем. - методикой разработки моделей безопасности компьютерных систем; методами анализа свойств моделей и получения оценок защищённости компьютерных систем на основе названных моделей; навыками подготовки отчётов и наглядного представления моделей безопасности компьютерных систем. - навыками проектирования подсистем защиты информации с применением современных компьютерных технологий, навыками построения математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, навыками оценки эффективности их применения.

	- методикой доказательства стойкости криптосистем; навыками подсчёта числа арифметических операций для математических моделей в области компьютерной безопасности. - навыками сравнительного анализа эффективности различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.
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 исследование математических моделей процессов и объектов, возникающих в системах компьютерной безопасности; • разработка и анализ эффективности вычислительных алгоритмов, реализующих процессы обработки информации в компьютерных системах; • проведение компьютерных экспериментов, демонстрирующих работоспособность компьютерных программ, и получение статистических оценок эффективности разработанных моделей и алгоритмов. 3. Введение дневника практики. **Заключительный этап:** 1. Выявление возможных недостатков в работе подразделения – места прохождения практики, их оценка и разработка предложений по совершенствованию существующего порядка работы, а также по внедрению новых методов работы. 2. Подготовка отчета о прохождении практики, представления отчета по практики и прилагаемых документов для защиты. 3. Защита отчёта по практике

Разработчики	Доцент, к.т.н., доцент ***Ветров Игорь Анатольевич***