МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. Иммануила Канта

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ Е.П.Ставицкая
«20» марта 2020 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«20» марта 2020 г.

Программа производственной преддипломной практики

для студентов 6 курса
очной формы обучения
специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации
квалификация (степень) выпускника: *специалист*

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
БФУ
Сертификат: 34219E685EE8D891F77F96F99B3B8407
Владелец: Федоров Александр Александрович
Действителен: с 28.12.2022 до 22.03.2024

Калининград
2020

Лист согласования

Составитель: доцент Института физико-математических наук и информационных технологий БОЛТНЕВ ЮРИЙ ФЁДОРОВИЧ.

Рабочая программа обсуждена и утверждена на заседании Учебно-методического совета ИФМНиИТ.

Протокол №____от «____»_____ 201__ г.

Председатель Совета _____ доцент, к.ф.-м.н. А.А.Шпилевой
Менеджер ООП_____Е.П.Ставицкая

Рабочая программа пересмотрена на заседании Учебно-методического совета ИФМНиИТ

Внесены следующие изменения (или изменений не внесено):

1. _____
2. _____
3. _____

Протокол №____от «____»_____ 20__ г.

Председатель Совета _____ доцент, к.ф.-м.н. А.А.Шпилевой
Менеджер ООП_____Е.П.Ставицкая

Содержание

1. Вид практики, способ и формы ее проведения

Вид практики: Производственная преддипломная практика (далее **преддипломная практика** или **практика**).

Преддипломная практика проводится в следующих **формах**:

- непрерывная – в период учебного времени для проведения практики, указанного в календарном учебном графике.

Способы проведения преддипломной практики:

- стационарная на рабочем месте (в компании, с которой заключен договор на прохождение преддипломной практики).

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

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.

В результате освоения ООП обучающийся должен овладеть следующими результатами обучения при прохождении практики:

Код компетенции	**Результаты освоения ООП Содержание компетенций**	**Перечень планируемых результатов обучения при прохождении практики**
ОК-5	Способность понимать	В результате прохождения практики обучающийся должен:

	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.	• ***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. • ***уметь*:** объяснять познавательную и практическую сущность математических, компьютерных и технических методов защиты информации как мотивационной основы профессиональной деятельности; • ***владеть*:** простейшими математическими методами обеспечения информационной безопасности; методикой применения основных правовых актов, регулирующих сферу информационной безопасности.
ОПК-9	Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.	В результате прохождения практики обучающийся должен: • ***знать*:** 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; • ***уметь*:** 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; • ***владеть*:** методикой разработки политики безопасности и построения соответствующих моделей управления информационными потоками в компьютерных системах.
ПК-3	Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	В результате прохождения практики обучающийся должен: • ***знать*:** отечественные и зарубежные стандарты в области компьютерной безопасности; основные положения законов и иных правовых актов РФ, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; • ***уметь*:** проводить анализ и оценку уровней защищённости компьютерных систем; • ***владеть*:** методикой анализа и оценки уровней защищённости компьютерных систем с использованием стандартов; навыками подготовки отчётов и представления результатов оценки уровней защищённости компьютерных систем.
ПК-4	Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.	В результате прохождения практики обучающийся должен: • ***знать*:** 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; • ***уметь*:** строить модели управления информационными пото-

		ками в компьютерных системах; проводить анализ и оценку уровней защищённости компьютерных систем; • ***владеть*:** 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.
ПК-8	Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы.	В результате прохождения практики обучающийся должен: • ***знать*:** 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; • ***уметь*:** 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; • ***владеть*:** 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.
ПСК-2.2	Способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах.	В результате прохождения практики обучающийся должен: • ***знать*:** типовые математические методы и алгоритмы, применяемые в системах защиты информации в компьютерных системах; типовые и стандартизованные оценки эффективности средств и методов защиты информации; • ***уметь*:** оценивать стойкость различных типов криптосистем; оценивать быстродействие вычислительных алгоритмов; • ***владеть*:** методикой доказательства стойкости криптосистем; навыками подсчёта числа арифметических операций для математических моделей в области компьютерной безопасности.
ПСК-2.5	Способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации.	В результате прохождения практики обучающийся должен: • ***знать*:** 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*:** осуществлять самостоятельную проектно-аналитическую работу; проводить сравнительный анализ эффективности математических методов и алгоритмов; • ***владеть*:** навыками сравнительного анализа эффективности

		различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.

3. Место преддипломной практики в структуре ООП

Преддипломная практика относится к базовой части блока 2 «Практики, в том числе научно-исследовательская работа (НИР)» ООП подготовки специалистов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

Логическая и содержательная связь дисциплин и практик, участвующих в формировании представленных в п.2 компетенций, содержится в ниже представленной таблице:

Компетенция	Предшествующие дисциплины	Данная дисциплина	Последующие дисциплины
ОК-5	− Основы информационной безопасности. − Введение в специальность. − История криптографии.	Производственная преддипломная практика	− Процедура защиты ВКП
ОПК-9	− Дискретная математика. − Математическая логика и теория алгоритмов. − Операционные системы. − Модели безопасности компьютерных систем. − Основы построения защищенных компьютерных сетей. − Защита в операционных системах. − Защита программ и данных. − Основы построения защищенных баз данных		− Подготовка к процедуре защиты выпускной квалификационной работы
ПК-3	− Основы информационной безопасности. − Теория псевдослучайных генераторов. − Техническая защита информации. − Основы построения защищенных компьютерных сетей. − Защита в операционных системах. − Защита программ и данных. − Основы построения защищенных баз данных. − Внешний аудит безопасности корпоративных сетей. − Системы тестового вторжения.		− Процедура защиты выпускной квалификационной работы
ПК-4	− Модели безопасности компьютерных систем. − Теория автоматов. − Формальные языки.		− Процедура защиты выпускной квалификационной работы.
ПК-8	− Модели безопасности компьютерных систем. − Организационное и правовое обеспечение информационной безопасности. − Компьютерный практикум по криптографии на эллиптических кривых. − Компьютерный практикум по криптографии на гиперэллиптических кривых. − Криптографические протоколы для защиты		− Подготовка к процедуре защиты выпускной квалификационной работы.

	банковской информации. – Анализ стойкости финансовых протоколов. – Функциональные поля и их приложения. – Локальные поля и их приложения. – Методы и алгоритмы генерации эллиптических кривых для криптографии. – Спаривание на эллиптических кривых. – Производственная практика по получению профессиональных умений и опыта профессиональной деятельности.		
ПСК-2.2	– Быстрые мультипликаторы. – Методы и алгоритмы генерации гиперэллиптических кривых для криптографии. – Компьютерный практикум по методам вычисления дискретного логарифма. – Технология инфраструктуры открытых ключей. – Методы и алгоритмы генерации эллиптических кривых для криптографии. – Спаривание на эллиптических кривых.		– Подготовка к процедуре защиты выпускной квалификационной работы
ПСК-2.5	- Основы построения защищенных компьютерных сетей. - Защита в операционных системах. - Защита программ и данных. - Основы построения защищенных баз данных. - Функциональные поля и их приложения. - Локальные поля и их приложения.		– Подготовка к процедуре защиты выпускной квалификационной работы.

4. Объем практики в зачетных единицах и ее продолжительность в неделях либо в академических или астрономических часах

Производственная преддипломная практика для обучающихся по специальности 10.05.01 – «Компьютерная безопасность», специализация: «Математические методы защиты информации» проводится в 11 семестре в течение 10 недель, трудоемкость преддипломной практики – 15 зачетных единиц.

Объём учебной практики	**Всего часов**	
	Контактные часы	**Самостоятельная работа**
Контактная работа обучающихся с преподавателем (самостоятельная работа студента под руководством преподавателя).	4,0	
Самостоятельная работа обучающихся		535
Промежуточная аттестация – зачет с оценкой	0,25	0,75
Итого	4,25	535,75
Общая трудоемкость практики	540 часов (15 ЗЕ)	

5. Содержание практики

Студенты-практиканты выполняют программу практики в соответствии с планом-графиком практики, утверждаемым руководством базового предприятия и представителями института физико-математических наук и информационных технологий БФУ им. И. Канта.

Ведется дневник практики и составляется заключительный отчет, который защищается после окончания практики и утверждается руководителями практики со стороны базового предприятия и института. В зависимости от специализации базового подразделения, в котором студент проходит практику, осуществляется корректировка направления его деятельности.

Студентам-практикантам должна быть предоставлена возможность ознакомиться с научно-технической документацией и научной литературой, которая касается предмета его исследований. В процессе прохождения практики студенты прослушивают лекции ведущих специалистов базовых предприятий, участвуют в научно-технических семинарах и конференциях при их наличии.

Студенты-практиканты проходят практику в отделах компьютерной безопасности, информационной и технической безопасности, компьютерных лабораториях, в которых работают их руководители и сотрудники подразделений. Они должны иметь доступ к программно-техническим комплексам, программным комплексам, математическому обеспечению и техническим средствам, необходимым для исследований, иметь возможность непосредственных консультаций во время работы со специалистами подразделений. Практиканты ежедневно работают в течение 3-4 часов в отделах предприятия. Объем теоретических занятий и семинаров определяется спецификой базового предприятия.

При прохождении преддипломной практики студенты изучают:

- административную и информационную структуру предприятия;
- основные нормативно-правовые положения в области информационной безопасности и защиты информации, на основании которых обеспечивается информационная безопасность предприятия;
- должностные инструкции сотрудников организации, отвечающих за безопасность;
- применяемые аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, используемых на предприятии;
- потенциальные каналы утечки информации, способы их выявления и методы оценки опасности, современную технологию анализа потенциальных каналов утечки информации;
- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия, современную технологию противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
- криптографические средства, стандарты в области криптографической защиты информации и криптографическую инфраструктуру, используемые на предприятии;

- математические модели и алгоритмы, используемые в современных криптографических системах и системах помехоустойчивого кодирования
- структуру и методы построения современных моделей безопасности компьютерных систем;
- передовой опыт лучших специалистов подразделения;
- менеджмент в области программно-аппаратных и технических средств защиты информации.

При прохождении преддипломной практики студенты разрабатывают и исследуют:

- методы организации и управления деятельности служб защиты информации на предприятии;
- технологию проектирования, построения и эксплуатации систем и подсистем компьютерной безопасности;
- методы анализа уязвимости и защищенности информационных процессов;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- методы и схемы управления информационной безопасностью;
- системы и алгоритмы шифрования информации, их свойства, оценки эффективности и их компьютерные модели;
- математические методы, модели и алгоритмы, используемые при разработке инфраструктуры современных криптосистем с открытым ключом, и их компьютерные модели;
- математические и компьютерные модели псевдослучайных генераторов, их свойства и методы статистического тестирования;
- системы и алгоритмы помехоустойчивого кодирования информации, их свойства, оценки эффективности и их компьютерные модели;
- структуру, принципы функционирования и управления современными системами защиты информации в компьютерных системах
- методы оценки экономической эффективности применения программно-аппаратных и технических средств защиты информации.

При прохождении преддипломной практики возможен следующий перечень индивидуальных заданий:

- На основе стандартов в области информационной безопасности, нормативных документов и с помощью программно-аппаратных средств контроля вторжений произвести анализ и оценку уровня информационной защищённости предприятия или его компьютерной системы.
- Разработать математические модели защищаемых информационных процессов, исследовать их свойства и приложения для создания средств защиты информации и систем, обеспечивающих информационную безопасность объектов.
- Обосновать и выбрать рациональное решение по уровню обеспечения информационной безопасности предприятия с учетом заданных требований и стандартов информационной безопасности; разработать и обосновать рекомендации по совершенствованию существующей системы информационной безопасности предприятия или его компьютерной системы.
- Разработать модификацию системы информационной безопасности предприятия или его компьютерной системы, или адаптировать существующую для обеспечения требуемого уровня безопасности; разработать необходимое программное обеспечение

для модифицированной системы информационной безопасности предприятия или его компьютерной системы.

- Принять участие в разработке технических заданий на проектирование, разработку эскизных, технических и рабочих проектов систем и подсистем защиты информации, с учетом действующих нормативных и методических документов; подробно описать методику и этапы разработки технического задания.
- Принять участие в разработке проектов систем и подсистем управления информационной безопасностью предприятия в соответствии с техническим заданием; подробно описать методику и этапы проектирования.
- Принять участие в экспериментально-исследовательских работах по сертификации средств защиты информации и анализу результатов; подробно описать методику сертификации и порядок проведения соответствующих работ.
- Осуществить сбор и первичную обработку материала для подготовки к написанию выпускной квалификационной работы; разработать и исследовать математические модели, провести компьютерные эксперименты по теме ВКР.

Задание на практику определяется вместе со студентом руководителями практики со стороны института и предприятия в начале практики. В конце практики студент должен представить результаты практики в виде отчета и сдать его руководителю от института. Руководитель практики от института организует защиту отчетов, по результатам которой на основании решения комиссии выставляется промежуточный контроль в виде зачета с оценкой.

Кроме того, при прохождении преддипломной практики на предприятии, учреждении, организации, студент обязан:

- пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка;
- посещать все мероприятия по месту практики;
- подчиняться действующим на предприятии, в учреждении, организации правилам внутреннего трудового распорядка;
- изучить и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии.

Особое внимание следует уделить внедрению результатов, полученных практикантом, по месту практики, а также анализу возможности применения и / или внедрения в производство предполагаемых результатов исследований по теме ВКР.

Краткий план-график преддипломной практики

№ п/п	Этапы (периоды) практики	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
1	Организационно-подготовительный 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.	16	Письменный отчёт. Индивидуальное задание на практику.

№ п/п	Этапы (периоды) практики	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
		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.		
2	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.	500	Письменный отчет. Дневник практики
3	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, пред-	24	Зачет с оценкой.

№ п/п	Этапы (периоды) практики	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
		ставления отчета по практики и прилагаемых документов для защиты.		
	Итого часов		**540**	

6. Формы отчетности по практике

Формы отчетности студентов по преддипломной практике (заверенные подписью и печатью руководителя базы практики и / или руководителя практики от института):

- индивидуальное задание на практику, заверенное руководителями практики от института и организации;
- совместный рабочий график (план) на практику, заверенный руководителями практики от института и организации;
- дневник практики, заверенный руководителем практики от организации;
- отчет о результатах прохождения практики.

Формы отчетности руководителей практики:

- руководитель практики от института не позднее 1 месяца после окончания практики предоставляет в институт отчет о проведенной преддипломной практике;
- руководитель практики от организации предоставляет отзыв о работе каждого студента-практиканта на практике.

Оформление результатов практики (*отчетов, характеристик, дневников*)

По окончании преддипломной практики студент обязан составить письменный отчет и сдать его руководителю практики от института. Отчет о практике должен содержать сведения о конкретной выполненной студентом запланированной работе (в соответствии с индивидуальным заданием на практику) в период прохождения практики, а также краткое описание структуры, целей и задач предприятия, организации, выводы и предложения.

Для оформления отчета студенту выделяется в конце практики 3 дня.

Требования, предъявляемые к оформлению отчета по преддипломной практике

Отчет по преддипломной практике должен состоять из Оглавления, Введения, описание основной части отчета (содержания практики), Заключения, Списка цитированной литературы.

Описание основной части отчета по преддипломной практике должно содержать:

– задание на преддипломную практику, полученное от руководителя;

– описание выполнения заданий, а также текущих поручений руководителя практики.

Рекомендуемый объем отчета не менее 25 страниц. Образец титульного листа прилагается (Приложение 1). Переплет отчета может быть произвольным и исключать рассыпание листов. Оформление отчета – см. Приложение 5.

Представленный студентом отчет рецензируется руководителем практики от института. В случае положительной рецензии он выносится на защиту.

Защита отчета осуществляется перед комиссией, которая состоит из преподавателей и руководителей преддипломной практики.

Порядок аттестации студентов по результатам практики

По окончании преддипломной практики проводится ***дифференцированный зачет*.** При проведении зачета используются следующие критерии итоговой оценки за преддипломную практику:

- полный и аккуратно оформленный в соответствии с требованиями отчет;
- глубокое и всестороннее знание существующей системы, методов и средств обеспечения информационной безопасности, применяемых на предприятии; знание основных документов, регламентирующих функционирование системы информационной безопасности на предприятии;
- грамотная оценка уровня информационной защищённости предприятия и его компьютерной системы;
- наличие разработанного и успешно протестированного программного продукта, реализующего безопасность отдельных компонент компьютерной системы предприятия, либо
- развёрнутые рекомендации по совершенствованию системы информационной безопасности предприятия или его компьютерной системы, либо
- наличие эскизного проекта модификации соответствующей системы информационной безопасности предприятия или его компьютерной системы;
- наличие всей необходимой для написания ВКР информации в соответствии с заданием на ВКР;
- правильные ответы студента на вопросы преподавателя, касающиеся предмета практики.

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

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках преддипломной практики

Компетенция	Этапы формирования компетенции	Показатели оценивания компетенции	Критерии оценивания компетенций	Шкала оценивания	Виды аттестации и виды оценочных

					средств
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.	Начальный этап	***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. ***уметь*:** объяснять познавательную и практическую сущность математических, компьютерных и технических методов защиты информации как мотивационной основы профессиональной деятельности; ***владеть*:** простейшими математическими методами обеспечения информационной безопасности; методикой применения основных правовых актов, регулирующих сферу информационной безопасности.	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** роли и значения компьютерной безопасности в обеспечении интересов России и её граждан; характера профессиональной деятельности по обеспечению информационной безопасности в условиях информационного противоборства; проблем и задач, возникающих при обеспечении информационной безопасности предприятия и защиты персональных данных. ***умение*** объяснять познавательную и практическую сущность математических, компьютерных и технических методов защиты информации как мотивационной основы профессиональной деятельности; ***владение практическими навыками*** применения простейших математических методов обеспечения информационной безопасности; владения методикой применения основных правовых актов, регулирующих сферу информационной безопасности.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** роли и значения компьютерной безопасности в обеспечении интересов России и её граждан; характера профессиональной деятельности по обеспечению информационной безопасности в условиях информационного противоборства; ***умение*** объяснять познавательную и практическую сущность ряда математических, компьютерных и технических методов защиты информации как мотивационной основы профессиональной деятельности; ***владение практическими навыками*** применения некоторых простейших математических методов обеспечения информационной безопасности.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: ***знакомство*** с ролью и значением компьютерной безопасности в обеспечении интересов России и её граждан; с характером профессиональной деятельности по обеспечению информационной безопасности; ***умение*** объяснять практическую сущность некоторых математических, компьютерных и технических методов защиты информации; ***владение некоторыми практическими навыками*** применения отдельных простейших математических методов обеспечения информационной безопасности.	от 50% до 70%	

			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** роли и значения компьютерной безопасности в обеспечении интересов России и её граждан; характера профессиональной деятельности по обеспечению информационной безопасности в условиях информационного противоборства; проблем и задач, возникающих при обеспечении информационной безопасности предприятия и защиты персональных данных. ***неумение*** объяснять познавательную и практическую сущность математических, компьютерных и технических методов защиты информации как мотивационной основы профессиональной деятельности; ***отсутствие практических навыков*** применения простейших математических методов обеспечения информационной безопасности; владения методикой применения основных правовых актов, регулирующих сферу информационной безопасности.	< 50%	
ОПК-9 Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.	Начальный этап	***знать*:** 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; ***уметь*:** 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 мо-	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** понятий и определений, используемых при описании моделей безопасности компьютерных систем; типов и структуры моделей управления информационными потоками в компьютерных системах; классификации угроз безопасности для компьютерных систем; ***умение*** 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; ***владение практическими навыками*** разработки политики безопасности и построения соответствующих моделей управления информационными потоками в компьютерных системах.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** основных понятий и определений, используемых при описании моделей безопасности компьютерных систем; основных типов и структуры моделей управления информационными потоками в компьютерных системах; примерной классификации угроз безопасности для компьютерных систем; ***умение*** строить базовые модели следующих типов: модели компьютерных систем с дискреционным управлением доступом; модели изолированной программной среды; модели компьютер-	от 70% до 85%	

		дели компьютерных систем с ролевым управлением доступом; ***владеть*:** методикой разработки политики безопасности и построения соответствующих моделей управления информационными потоками в компьютерных системах.	ных систем с мандатным управлением доступом; модели безопасности информационных потоков; модели компьютерных систем с ролевым управлением доступом; ***владение практическими навыками*** разработки основных аспектов политики безопасности и построения соответствующих моделей управления информационными потоками в компьютерных системах.		
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных понятий и определений, используемых при описании моделей безопасности компьютерных систем; отдельных типов и структуры моделей управления информационными потоками в компьютерных системах; знакомство с классификацией угроз безопасности для компьютерных систем; ***умение*** строить отдельные модели управления доступом; отдельные модели изолированной программной среды; отдельные модели безопасности информационных потоков; ***Владение практическими навыками*** разработки отдельных аспектов политики безопасности и построения соответствующих моделей управления информационными потоками в компьютерных системах.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** понятий и определений, используемых при описании моделей безопасности компьютерных систем; типов и структуры моделей управления информационными потоками в компьютерных системах; классификации угроз безопасности для компьютерных систем; ***неумение*** строить модели компьютерных систем с различными типами управления доступом; строить модели изолированной программной среды; строить модели безопасности информационных потоков; ***отсутствие практических навыков*** разработки политики безопасности и построения соответствующих моделей управления информационными потоками в компьютерных системах.	< 50%	
ПК-3 Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и	Начальный этап	***знать*:** отечественные и зарубежные стандарты в области компьютерной безопасности; основные положения законов и иных правовых актов РФ, регулирующих взаимоотношения	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** отечественных и зарубежных стандартов в области компьютерной безопасности; основных положений законов и иных правовых актов РФ, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; ***умение*** проводить анализ и оценку уровней защищённости компьютерных систем;	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет

зарубежным стандартам в области компьютерной безопасности.		между субъектами в сфере информационной безопасности; ***уметь*:** проводить анализ и оценку уровней защищённости компьютерных систем; ***владеть*:** методикой анализа и оценки уровней защищённости компьютерных систем с использованием стандартов; навыками подготовки отчётов и представления результатов оценки уровней защищённости компьютерных систем.	***владение практическими навыками*** анализа и оценки уровней защищённости компьютерных систем с использованием стандартов; навыками подготовки отчётов и представления результатов оценки уровней защищённости компьютерных систем.		
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** основных отечественных стандартов в области компьютерной безопасности; ряда положений законов и иных правовых актов РФ, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; ***умение*** проводить анализ и оценку уровней защищённости компьютерных систем; ***владение практическими навыками*** анализа и оценки уровней защищённости компьютерных систем с использованием стандартов.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных отечественных стандартов в области компьютерной безопасности; отдельных положений законов и иных правовых актов РФ, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; ***умение*** проводить анализ уровней защищённости компьютерных систем; ***владение практическими навыками*** анализа уровней защищённости компьютерных систем с использованием стандартов.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** отечественных и зарубежных стандартов в области компьютерной безопасности; положений законов и иных правовых актов РФ, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; ***неумение*** проводить анализ и оценку уровней защищённости компьютерных систем; ***отсутствие практических навыков*** анализа и оценки уровней защищённости компьютерных систем с использованием стандартов; навыков подготовки отчётов и представления результатов оценки уровней защищённости компьютерных систем.	< 50%	
ПК-4 Способность проводить анализ и участвовать в разработке математических моделей	Промежуточный этап	***знать*:** типы и структуру моделей управления информационными потоками в компьютерных системах; классификацию угроз безопасности	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** типов и структуры моделей управления информационными потоками в компьютерных системах; классификации угроз безопасности для компьютерных систем; проблем и задач в сфере обеспечения информационной безопасности компьютерных систем;	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференциро-

безопасности компьютерных систем.		для компьютерных систем; проблемы и задачи в сфере обеспечения информационной безопасности компьютерных систем; ***уметь*:** строить модели управления информационными потоками в компьютерных системах; проводить анализ и оценку уровней защищённости компьютерных систем; ***владеть*:** 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.	***умение*** строить модели управления информационными потоками в компьютерных системах; проводить анализ и оценку уровней защищённости компьютерных систем; ***владение практическими навыками*** разработки моделей безопасности компьютерных систем; навыками анализа свойств моделей и получения оценок защищённости компьютерных систем на основе названных моделей; навыками подготовки отчётов и наглядного представления моделей безопасности компьютерных систем.		ванный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** основных типов и структуры моделей управления информационными потоками в компьютерных системах; примерной классификации угроз безопасности для компьютерных систем; основных проблем и задач в сфере обеспечения информационной безопасности компьютерных систем; ***умение*** строить типовые модели управления информационными потоками в компьютерных системах; проводить анализ и оценку уровней защищённости компьютерных систем на основе типовых моделей; ***владение практическими навыками*** разработки типовых моделей безопасности компьютерных систем; навыками анализа свойств типовых моделей и получения оценок защищённости компьютерных систем на основе названных моделей; навыками подготовки отчётов по анализу и оценке защищённости компьютерных систем.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных типов и структуры моделей управления информационными потоками в компьютерных системах; примерной классификации угроз безопасности для компьютерных систем; ***умение*** строить отдельные модели управления информационными потоками в компьютерных системах; проводить анализ и оценку уровней защищённости компьютерных систем на основе названных моделей; ***владение практическими навыками*** разработки отдельных моделей безопасности компьютерных систем; навыками анализа свойств отдельных моделей и получения оценок защищённости компьютерных систем на основе названных моделей.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** типов и структуры моделей управления информационными потоками в компьютерных системах; классификации угроз безопасности для	< 50%	

			компьютерных систем; проблем и задач в сфере обеспечения информационной безопасности компьютерных систем; ***неумение*** строить модели управления информационными потоками в компьютерных системах; проводить анализ и оценку уровней защищённости компьютерных систем; ***отсутствие практических навыков*** разработки моделей безопасности компьютерных систем; навыков анализа свойств моделей и получения оценок защищённости компьютерных систем на основе названных моделей; навыков подготовки отчётов и наглядного представления моделей безопасности компьютерных систем.		
ПК-8 Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы.	Промежуточный этап	***знать*:** 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; ***уметь*:** 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; ***владеть*:** навыками проектирования подсистем защиты	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** современных информационных методик и технологий, методов математической обработки информации, методов теоретического и экспериментального исследования, стандартов и нормативов в области информационной безопасности; типовой структуры и методов создания подсистем информационной безопасности компьютерных систем различного профиля; ***умение*** 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; ***владение практическими 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.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** основных информационных методик и технологий, методов математической обработки информации, основных методов теоретического и экспериментального исследования, ряда стандартов и нормативов в области информационной безопасности; типовой структуры и методов создания подсистем информационной безопасности компьютерных систем различного профиля; ***умение*** применять математические методы и математические пакеты для обработки, анализа и систематизации информации в компьютерных системах, строить схемы и модели подсистем информационной безопасности компьютерной системы;	от 70% до 85%	

		информации с применением современных компьютерных технологий, навыками построения математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, навыками оценки эффективности их применения.	***владение практическими навыками*** проектирования подсистем защиты информации, навыками построения математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры.		
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных информационных методик и технологий, отдельных методов математической обработки информации, отдельных методов теоретического и экспериментального исследования, типовой структуры и методов создания подсистем информационной безопасности компьютерных систем; ***умение*** применять отдельные математические методы и математические пакеты для обработки, анализа и систематизации информации в компьютерных системах, строить схемы и модели отдельных подсистем информационной безопасности компьютерной системы; ***владение практическими навыками*** проектирования отдельных подсистем защиты информации, навыками построения математических моделей информационных потоков, возникающих при построении типовой криптографической инфраструктуры.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** информационных методик и технологий, методов математической обработки информации, методов теоретического и экспериментального исследования, стандартов и нормативов в области информационной безопасности; типовой структуры и методов создания подсистем информационной безопасности компьютерных систем различного профиля; ***неумение*** применять математические методы и математические пакеты для обработки, анализа и систематизации информации в компьютерных системах, строить схемы и модели подсистем информационной безопасности компьютерной системы; ***отсутствие практических навыков*** проектирования подсистем защиты информации, навыков построения математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, навыков оценки эффективности их применения.	< 50%	
ПСК-2.2 Способность на основе анализа применяемых	Промежуточный этап	***знать*:** типовые математические методы и алгоритмы, применяемые в системах защиты	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** математических методов и алгоритмов, применяемых в системах защиты информации в компьютерных системах; типовых и стандарти-	от 85% до 100%	Отчет по практике Отзыв руководителя практики

математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах.		информации в компьютерных системах; типовые и стандартизованные оценки эффективности средств и методов защиты информации; ***уметь*:** оценивать стойкость различных типов криптосистем; оценивать быстродействие вычислительных алгоритмов; ***владеть*:** методикой доказательства стойкости криптосистем; навыками подсчёта числа арифметических операций для математических моделей в области компьютерной безопасности.	зованных оценок эффективности средств и методов защиты информации; ***умение*** оценивать стойкость различных типов криптосистем; оценивать быстродействие вычислительных алгоритмов; ***владение практическими навыками*** доказательства стойкости криптосистем; навыками подсчёта числа арифметических операций для математических моделей в области компьютерной безопасности.		Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** основных математических методов и алгоритмов, применяемых в системах защиты информации в компьютерных системах; основных типовых и стандартизованных оценок эффективности средств и методов защиты информации; ***умение*** оценивать стойкость различных типов криптосистем; ***владение практическими навыками*** доказательства стойкости криптосистем.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных математических методов и алгоритмов, применяемых в системах защиты информации в компьютерных системах; отдельных типовых и стандартизованных оценок эффективности средств и методов защиты информации; ***умение*** оценивать стойкость отдельных типов криптосистем; ***владение практическими навыками*** доказательства стойкости отдельных типов криптосистем.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** математических методов и алгоритмов, применяемых в системах защиты информации в компьютерных системах; типовых и стандартизованных оценок эффективности средств и методов защиты информации; ***неумение*** оценивать стойкость различных типов криптосистем; оценивать быстродействие вычислительных алгоритмов; ***отсутствие практических навыков*** доказательства стойкости криптосистем; навыков подсчёта числа арифметических операций для математических моделей в области компьютерной безопасности.	< 50%	
ПСК-2.5 Способность проводить	Промежуточный	***знать*:** номенклатуру и основные характеристики	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** номенклатуры и характеристик сертифи-	от 85% до 100%	Отчет по практике Отзыв

сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации.	этап	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*:** осуществлять самостоятельную проектно-аналитическую работу; проводить сравнительный анализ эффективности математических методов и алгоритмов; ***владеть*:** навыками сравнительного анализа эффективности различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.	цированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; математических методов и алгоритмов, применяемых в программно-аппаратных средствах защиты информации; перспективных математических методов защиты информации; ***умение*** осуществлять самостоятельную проектно-аналитическую работу; проводить сравнительный анализ эффективности математических методов и алгоритмов; ***владение практическими навыками*** сравнительного анализа эффективности различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.		руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** основной номенклатуры и основных характеристик сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; распространённых математических методов и алгоритмов, применяемых в программно-аппаратных средствах защиты информации; ***умение*** осуществлять проектно-аналитическую работу; проводить анализ эффективности математических методов и алгоритмов; ***владение практическими навыками*** анализа эффективности различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** некоторых сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью и их основных характеристик; отдельных математических методов и алгоритмов, применяемых в программно-аппаратных средствах защиты информации; ***умение*** осуществлять проектно-аналитическую работу; проводить анализ эффективности вычислительных алгоритмов; ***владение практическими навыками*** анализа эффективности алгоритмов, реализованных в средствах защиты информации.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** номенклатуры и характеристик сертифицированных программно-аппаратных средств	< 50%	

			защиты информации, выпускаемых российской промышленностью; математических методов и алгоритмов, применяемых в программно-аппаратных средствах защиты информации; ***неумение*** осуществлять проектно-аналитическую работу; проводить анализ эффективности математических методов и алгоритмов; ***отсутствие практических навыков*** анализа эффективности различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.		

Указанные компетенции формируются у студентов в процессе прохождения преддипломной практики. Формой текущего контроля за сформированностью компетенций является написание отчета по преддипломной практике.

7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкалы оценивания

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания приведены в п. 7.1.

Для оценивания уровня сформированности компетенций используется следующая шкала, где оценки определяются по результатам (R), полученным во время аттестации, для каждой из компетенций исходя из следующих условий:

- «отлично»: $R \geq 85$ %;
- «хорошо»: $70 \leq R < 85$ %;
- «удовлетворительно»: $50\ \% \leq R < 70$ %;
- «неудовлетворительно»: $R < 50$ %.

Далее рассчитывается итоговая оценка (S) по следующей формуле:

$$S = \frac{\sum_{k=0}^{n} R_k}{n},$$

где: R_k – оценка по k-ой компетенции, n – общее количество оцениваемых компетенций.

В качестве оценки за зачет с оценкой выставляется следующая, в зависимости от полученного значения S:

- «отлично»: $S \geq 85$ %;
- «хорошо»: $70\ \% \leq S < 85$ %;
- «удовлетворительно»: $50\ \% \leq S < 70$ %;
- «неудовлетворительно»: $S < 50$ %.

7.3. Комплект оценочных средств по всем заявленным в рабочей программе видам занятий и самостоятельной работы обучающихся

В комплект оценочных средств входят оценочные средства по контролю промежуточной аттестации обучающихся по всем заявленным в рабочей программе видам работ обучающихся:

- индивидуальные задания для прохождения практики;
- контрольные вопросы к дифференцируемому зачету;
- отзыв руководителя практики от предприятия;
- отчет студента о прохождении практики.

Примерные контрольные вопросы к дифференцированному зачету по преддипломной практике:

1. Какие нормативные документы по охране труда, технике безопасности и пожарной безопасности вам были предоставлены для изучения?
2. В чем заключались Ваши права и обязанности в соответствии с должностной инструкцией?
3. Какие нормативные документы для составления отчетности используются на предприятии?
4. Суть порученных Вам производственных задач.
5. Какие методы, технологии были предложены вами для решения поставленных производственных задач?
6. Какие информационные системы/технологии используются на предприятии?
7. Описать административную и информационную структуру предприятия.
8. Описать цели и задачи, решаемые предприятием, направление деятельности предприятия.
9. Описать используемые на предприятии технические и программные средства вычислительной техники.
10. Описать организацию информационных систем с точки зрения информационной защищенности и защиты государственной тайны.
11. Описать технические устройства хранения, обработки и передачи информации, используемые на предприятии.
12. Представить анализ потенциальных каналов утечки информации и уязвимостей информационных процессов.
13. Описать схему инженерно-технической защиты информации.
14. Описать используемые методы и средства противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
15. Представить перечень правовых положений в области информационной безопасности и защиты информации, регламентирующих уровень защищённости базового предприятия.
16. Описать проведённые экспериментально-исследовательские работы по сертификации средств защиты информации и анализ их результатов.
17. Представить и обосновать рекомендации по совершенствованию системы информационной безопасности предприятия или его компьютерной системы.
18. Представить эскизный проект модификации системы информационной безопасности предприятия или его компьютерной системы.
19. Описать структуру и функции разработанного программного обеспечения для модифицированной системы информационной безопасности предприятия или его компьютерной системы.

20. Каковы выводы и предложения по внедрению рекомендаций по совершенствованию системы информационной безопасности на предприятии?
21. Какие работы проводились в рамках подготовки ВКР?
22. Какие математические модели были исследованы с целью подготовки ВКР? Каковы результаты исследований?
23. Какие материалы для прикладной части ВКР удалось собрать? Какие – не удалось?
24. Как соотносятся работы, выполненные на предприятии, с ВКР?

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка сформировавшихся компетенций по преддипломной практике проводится в форме текущей и промежуточной аттестации.

Текущий контроль осуществляется руководителем практики от базовой организации. Руководитель практики от организации контролирует выполнение индивидуального задания согласно плану-графику, оценивает каждый этап выполнения в дневнике практики.

Промежуточный контроль осуществляется на дифференцированном зачете.

На зачет студенты предоставляют следующие документы, заверенные подписью и печатью руководителя базы практики и / или руководителя практики от института:

- индивидуальное задание на практику, заверенное руководителями практики от института и организации;
- совместный рабочий график (план) на практику, заверенный руководителями практики от института и организации;
- дневник практики, заверенный руководителем практики от организации;
- отчет о результатах прохождения практики.

Защита отчета осуществляется перед комиссией, которая состоит из преподавателей и руководителей преддипломной практики.

Критерии выставления итоговой оценки- см. п . 7.2.

8. Перечень учебной литературы и ресурсов сети Интернет, необходимых для проведения практики

8.1. Основная литература

1. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. - Ч. 4: Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых on-line, 60 с.. - Библиогр.: с. 58-59. - ISBN 978-5-9971-0389-7: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)
2. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. Ч. 5: Методы алгебраических кривых. - 156, [1] с.. - Библиогр. в конце кн.. - ISBN 978-5-9971-0390-3: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)

3. Защита информации [Электронный ресурс]: учеб. пособие для вузов/ А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 2-е изд.. - Москва: РИОР; Москва: ИНФРА-М, 2015. - 1 эл. опт. диск (CD-ROM), 391, [1]: ил. - (Высшее образование - бакалавриат). - Библиогр.: с. 386-389 (55 назв.). - Соответствует ФГОС (третьего поколения). - ISBN 978-5-369-01378-6. - ISBN 978-5-16-010188-0: 15100.00 р. Имеются экземпляры в отделах /There are copies in departments: всего /all 2: ЭБС Кантиана(1), ч.з.N1(1)
4. Физические основы защиты информации, обрабатываемой средствами вычислительной техники [Электронный ресурс]/ М-во образования и науки РФ, Балт. федер. ун-т им. И. Канта, Ин-т приклад. математики и информац. технологий; М-во образования и науки РФ, Балт. федер. ун-т им. И. Канта, Ин-т приклад. математики и информац. технологий. - Калининград: БФУ им. И. Канта, 2015. - 1 on-line, 283 с.. - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)

8.2. Дополнительная литература

1. Абрамов, С. А. Лекции о сложности алгоритмов: учеб. пособие для вузов/ С. А. Абрамов. - 2-е изд., перераб.. - Москва: МЦНМО, 2012. - 245 с. - (Современные лекционные курсы). - Библиогр.: с. 236-240 (68 назв.). - Предм. указ.: с. 241-242. - ISBN 978-5-4439-0204-3: 266.00, 266.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 12: УБ(11), ч.з.N3(1)
2. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. Ч. 3: Вычислительный практикум по числовым полям и криптографии в квадратичных полях on-line, 93 с.. - Библиогр. в конце кн.. - ISBN 978-5-9971-0388-0: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)
3. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых/ А. А. Болотов, С. Б. Гашков, А. Б. Фролов. - 2-е изд.. - М.: КомКнига, 2012. - 303 с. - (Защита информации). - Вариант загл.: Протоколы криптографии на эллиптических кривых. - Библиогр.: с. 264-268 (97 назв.). - Предм. указ.: с. 269-274. - ISBN 978-5-484-01291-6: 401.00, 401.00, 367.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 27: УБ(26), ч.з.N3(1)
4. Запечников, С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие для вузов/ С.В. Запечников. - М.: Горячая линия-Телеком, 2007. - 319 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 296-305 (171 назв.). - ISBN 978-5-93517-318-2: 237.60, 237.60, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 15: УБ(15)
5. Защита информации [Электронный ресурс]: учеб. пособие для вузов/ А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 2-е изд.. - Москва: РИОР; Москва: ИНФРА-М, 2015. - 1 эл. опт. диск (CD-ROM), 391, [1]: ил. - (Высшее образование - бакалавриат). - Библиогр.: с. 386-389 (55 назв.). - Соответствует ФГОС (третьего поколения). - ISBN 978-5-369-01378-6. - ISBN 978-5-16-010188-0: 15100.00 р. Имеются экземпляры в отделах /There are copies in departments: всего /all 2: ЭБС Кантиана(1), ч.з.N1(1)
6. Колесниченко, О. В. Аппаратные средства PC/ Олег Колесниченко, Игорь Шишигин, Валентин Соломенчук. - 6-е изд., [перераб. и доп.]. - СПб.: БХВ-Петербург, 2010. - 782 с.: ил., табл.. - (В подлиннике). - Предм. указ.: с. 772-782. - ISBN 978-5-9775-0432-4: 449.00, 449.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 12: УБ(12)
7. Нестеренко, Ю. В. Теория чисел: учеб. для вузов/ Ю. В. Нестеренко. - М.: Академия, 2008. - 264, [1] с. - (Высшее профессиональное образование. Физико-математические науки). - (Учебник). - Библиогр.: с. 262 (17 назв.). - ISBN 978-5-7695-4646-4 : 354.53, 354.53, 514.80, р. Имеются экземпляры в отделах /There are copies in departments: всего /all

16: ч.з.N3(1), УБ(15)
8. Основы информационной безопасности: учеб. пособие/ Е. Б. Белов [и др.]. - М.: Горячая линия-Телеком, 2006. - 544 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр. в конце частей. - ISBN 5-93517-292-5: 316.25, 351.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 16: УБ(14), ч.з.N3(1), НА(1)
9. Проскурин, В. Г. Защита в операционных системах: учеб. пособие для вузов/ В. Г. Проскурин. - Москва: Горячая линия-Телеком, 2014. - 192 с.. - Библиогр.: с. 189-190. - ISBN 978-5-9912-0379-1: 392.15, 392.15, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 10: УБ(9), ч.з.N3(1)
10. Проскурин, В. Г. Защита программ и данных: учеб. пособие для вузов/ В. Г. Проскурин. - 2-е изд., стер.. - М.: Академия, 2012. - 198, [1] с.: ил. - (Высшее профессиональное образование. Информационная безопасность). - (Бакалавриат). - Библиогр.: с. 195-196 (31 назв.). - ISBN 978-5-7695-9288-1: 540.10, 540.10, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 15: УБ(14), ч.з.N3(1)
11. Платонов, В. В. Программно-аппаратные средства защиты информации: учеб. для вузов/ В. В. Платонов. - 2-е изд., стер.. - Москва: Академия, 2014. - 330, [1] с.: табл.. - (Высшее образование. Информационная безопасность). - (Бакалавриат). - Библиогр.: с. 326-327. - ISBN 978-5-4468-1302-5: 880.03, 888.03, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 10: УБ(9), ч.з.N3(1)
12. Смарт, Н. Криптография/ Н. Смарт ; пер. с англ. С. А. Кулешов под ред. С. К. Ландо. - Москва: Техносфера, 2006. - 525 с. - (Мир программирования). - Предм. указ.: с. 524-525. - ISBN 5-94836-043-1: 314.05, 370.00, 314.05, 454.96, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 17: УБ(15), НА(2)
13. Технические средства и методы защиты информации: учеб. пособие для вузов/ А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - [4-е изд., испр. и доп.]. - М.: Горячая линия-Телеком, 2012. - 615 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 608-609 (34 назв.). - ISBN 978-5-9912-0084-4: 699.60, 699.60, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 15: УБ(14), ч.з.N3(1)
14. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие / П. Б. Хорев. - 2-е изд., стер.. - М.: Академия, 2006. - 255 с.: ил., табл.. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 251-252 (28 назв.). - ISBN 5-7695-3288-2 : 197.60, 197.60, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 18: УБ(16), ч.з.N3(1), НА(1)
15. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы/ А. А. Болотов [и др.]. - 2-е изд., доп.. - М.: КомКнига, 2012. - 355 с.: граф., табл.. - (Защита информации). - Вариант загл.: Алгебраические и алгоритмические основы. - Библиогр.: с. 312-320 (187 назв.) - Предм. указ.: с. 321-324. - ISBN 978-5-484-01290-9: 401.00, 401.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 12: УБ(11), ч.з.N3(1)

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для выполнения преддипломной практики

1. http://xn--90ax2c.xn--p1ai/ – «Национальная электронная библиотека».
2. http://lib.kantiana.ru/irbis/standart/ELIB – ЭБС Кантиана.
3. http://elibrary.ru/defaultx.asp – Научная электронная библиотека eLIBRARY.RU.
4. **https://www.garant.ru/products/ipo/prime/doc/71456224/** - Доктрина информационной безопасности Российской Федерации.

5. **https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html** - Стратегия национальной безопасности Российской Федерации до конца 2020 года.
6. **http://iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii** - ГОСТ Р – Национальные стандарты Российской федерации в области защиты информации.
7. **http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=172255** - ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
8. **http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=172313** - ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
9. **http://protect.gost.ru/document.aspx?control=7&id=200990** - ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Функция хэширования.
10. **http://protect.gost.ru/document.aspx?control=7&id=200971** - ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
11. **http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf** - FIPS PUB 46-3 Data Encryption Standard (DES) 1999.
12. **http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf** - FIPS PUB 140-2 Security Requirements for Cryptographic Modules 3001, defines four increasing security levels.
13. **http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf** - FIPS PUB 180-4 Secure Hash Standard (SHS) 2012 defines the SHA family/
14. **http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf** - FIPS PUB 186-2 Digital Signature Standard (DSS) 2000.
15. **http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf** - FIPS PUB 197 Advanced Encryption Standard (AES) 2001
16. http://www.iacr.org – Международная ассоциация криптологических исследований (International Association for Cryptologic Research - IACR).
17. http://www.ifca.ai – Международная ассоциация финансовой криптографии (International Financial Cryptography Association – IFCA).
18. http://csrc.nist.gov – Национальный институт стандартов и технологий США (National Institute of Standards and Technology NIST).
19. http://dorlov.blogspot.ru/p/blog-page_3151.html - Перечень сайтов по информационной безопасности.
20. http://www.kaspersky.ru/protect-my-business/?cid=ru_RU:SEM:kl_google_business_nb&gclid=CJKilc2bqsoCFQISGwodvSUL_A – Лаборатория Касперского.
21. http://www.itsec.ru/main.php - Форум по информационной безопасности.
22. http://www.securitylab.ru – Информационный сайт по компьютерной безопасности.

23. http://lib.mexmat.ru/catalogue.php?dir=02_06 - Электронная библиотека механико-математического факультета Московского государственного университета. Раздел Криптография
24. MathWorld. – математический сайт, созданный *Weisstein, Eric W.* (англ.).
25. http://mathworld.wolfram.com/ - сайт по эллиптическим кривым.

9. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

9.1. Перечень информационных технологий, используемых при проведении практики

Для подготовки, прохождения практики и составления отчета используются следующие информационные технологии:

- технические средства: компьютерная техника и средства связи (персональные компьютеры, проектор, интерактивная доска, видеокамеры и пр.);
- методы обучения с использованием информационных технологий (компьютерное тестирование, демонстрация мультимедийных материалов и пр.);
- перечень интернет-сервисов и электронных ресурсов (поисковые системы, электронная почта, профессиональные, тематические чаты и форумы, системы видео- и аудиоконференций, он-лайн энциклопедии и справочники). Институт обеспечен лицензионным программным обеспечением.

9.2. Перечень программного обеспечения (используемое при необходимости)

Windows 7 Pro 32-bit SP1 –договор №1980/12 14.12.2012 ООО "ЭСЭМДЖИ", акт АА-118 от 21.12.2012
Entity Framework 6.1.3 Tools for Visual Studio 2015- договор № 494/12 от 4.04.12 ЗАО "СофтЛайн Трейд"
LibreOffice 5.0.2.2 общественная лицензия MPL 2.0
Microsoft Visual Studio Professional 2015- договор № 494/12 от 4.04.12 ЗАО "СофтЛайн Трейд"

9.3. Информационные справочные системы

1. http://xn--90ax2c.xn--p1ai/ – «Национальная электронная библиотека».
2. http://lib.kantiana.ru/irbis/standart/ELIB – ЭБС Кантиана.
3. http://elibrary.ru/defaultx.asp – Научная электронная библиотека eLIBRARY.RU.
4. http://infomag.biz/index.php – Служба ИНФОМАГ - Библиографическая и другая научная информация, в первую очередь оглавления научных и технических журналов, а также зарубежных научных электронных бюллетеней.
5. http://window.edu.ru/ – Информационная система «Единое окно доступа к образовательным ресурсам».
6. http://www.rsl.ru/ – Российская государственная библиотека.

7. http://www.biblioclub.ru/ – Университетская библиотека онлайн.

10. Описание материально-технической базы, необходимой для проведения практики

Материально-техническим обеспечением преддипломной практики служат базовые предприятия и организации, с которыми заключены договоры на места прохождения практик.

1.	ООО «Центр Защиты Информации»
2.	ГАУ КО «КГНИЦ»
3.	АО «Янтарьэнерго»
4.	ООО «Алгоритм»
5.	АО “ЦентрИнформ»
6.	ООО «СКА и К»
7.	ООО «Сократ»
8.	АО «33 судоремонтный завод»
9.	“Elite Games Limited”
10.	ООО «Альпея»
11.	ООО «Е-Легион»
12.	ФГБК «Федеральный центр высоких медицинских технологий» Министерства здравоохранения Российской Федерации
13.	ООО «Хирокрафт»

11. Приложения

Приложение 1

Титульный лист отчета по преддипломной практике

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

Отчёт
о прохождении производственной преддипломной практики

Тема ВКР _____
_____

Обучающийся _____
(*Ф.И.О. подпись*)

Направление подготовки 10.05.01 Компьютерная безопасность
(*шифр, название*)

Профиль Математические методы защиты информации
(*название*)

Место прохождения практики _____
_____
_____
_____
(*указывается полное наименование структурного подразделения Института / профильной организации и её структурного подразделения, а также их фактический адрес*)

Срок прохождения практики: с «___» 2019 г. по «___» 2019 г.

Руководитель практики от института:

_____
(*Ф.И.О., должность, подпись*)

Руководитель практики от организации:

_____
(*Ф.И.О., должность, подпись*)

Отчет подготовлен _____ _____
(*подпись обучающегося*) (*И.О. Фамилия*)

Калининград, 2019

Структура отчёта по преддипломной практике

Титульный лист
Оглавление
ВВЕДЕНИЕ. *Во введении ставятся цель и задачи НИР, обосновывается выбор научной тематики. Цель практики (формулируется на основе темы конкретного студента). Цель практики только одна! Задачи практики (формулируются исходя из цели). Обязательно указывается, что был пройден инструктаж по технике безопасности и прочие виды инструктажа, предусмотренные программой НИР.*

ОСНОВНАЯ ЧАСТЬ
В основной части содержится перечень информации, предусмотренный Программой соответствующей практики и обозначенный в индивидуальном задании.

ЗАКЛЮЧЕНИЕ
В заключении формулируются основные результаты проделанной работе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ
Список использованных источников может содержать перечень нормативных правовых источников, учебных, научных и периодических изданий, используемых обучающимся для выполнения программы практики.

ПРИЛОЖЕНИЯ К ОТЧЕТУ ПО ПРАКТИКЕ:

Приложение 1 – Индивидуальное задание на практику
Приложение 2 – Совместный рабочий график (план) на практику
Приложение 3 – Отзыв руководителя практики от организации
Приложение 4 – Дневник о прохождении практики
Приложение 5 – Дополнительная информация

В приложение 5 *могут включаться копии документов* (*нормативных актов, отчетов и др.*), *изученных и использованных обучающимся в период прохождения практики, могут быть отражены и указаны реальные процессы, происходящие на предприятии* (*в организации*) *и дополняющие изложенный в Отчете материал* (*например, копии заполненных документов, расчетные материалы и другие материалы*).

Структура оглавления отчёта по преддипломной практике

Оглавление

Приложение 2

Форма дневника прохождения преддипломной практики

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

ДНЕВНИК
прохождения преддипломной практики

Обучающийся _____, студент 6 курса
(*Ф.И.О. полностью*)

Направление подготовки 10.05.01 Компьютерная безопасность
(*шифр, название*)

Профиль Математические методы защиты информации
(*название*)

Место прохождения практики _____
_____
_____
_____.

Срок прохождения практики: с «__ » _____ 2019 г. по «___ » _____ 2019 г.

Руководитель практики от Института _____«___»_____ 2019 г.
(*Ф.И.О. подпись*)

Руководитель практики от предприятия _____«___»_____ 2019 г.
(*Ф.И.О. подпись*)

Дневник подготовлен _____
(*Ф.И.О. подпись*)

Калининград, 2019

Дневник

День	Дата	Содержание выполненного задания	Применяемое оборудование, литература (с указанием прорабатываемой темы), компьютерные программы, инструмент, материалы, и пр.	Отметка руководителя о качестве выполненного задания	Подпись руководителя НИР
1.		Инструктаж по технике безопасности, пожарной безопасности, ознакомление с правилами внутреннего трудового распорядка и с требованиями охраны труда.			
1.		Ознакомление с индивидуальным планом НИР.			
2.					
3.					
4.					
5.					
6.					

Приложение 3

Форма индивидуального задания на преддипломную практику

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

«УТВЕРЖДАЮ»
Руководитель практики от БФУ им. И. Канта
_____ / _____ /
«_____»_____ 20__ г.

«СОГЛАСОВАНО»
Руководитель практики
от профильной организации
_____ / _____ /
«_____»_____ 20__ г.

для _____,
(ФИО студента)

Место прохождения: _____

Срок прохождения: с «___» _____ 20___ г. по «___» _____ 20___ г.

Цель прохождения: _____
_____
_____
_____

Задачи: _____
_____
_____
_____
_____
_____

Содержание: _____
_____
_____
_____
_____
_____

Планируемые результаты:

1	
2	
3	
4	
5	
…	

Форма отчетности: _____

Форма контроля: _____

Ознакомлен(а) _____ «____» _____ 20___ г.
(подпись студента)

Цель прохождения практики:

- углубление профессиональных знаний и адаптация их к условиям конкретного производства;
- закрепление профессиональных компетенций, приобретение дополнительного опыта практической работы;
- сбор и обработка материала для написания ВКР.

Задачи практики:

Изучить:

- административную и информационную структуру предприятия;
- основные нормативно-правовые положения в области информационной безопасности и защиты информации, на основании которых обеспечивается информационная безопасность предприятия;
- должностные инструкции сотрудников организации, отвечающих за безопасность;
- применяемые аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, используемых на предприятии;
- потенциальные каналы утечки информации, способы их выявления и методы оценки опасности, современную технологию анализа потенциальных каналов утечки информации;
- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия, современную технологию противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
- криптографические средства, стандарты в области криптографической защиты информации и криптографическую инфраструктуру, используемые на предприятии;
- математические модели и алгоритмы, используемые в современных криптографических системах и системах помехоустойчивого кодирования
- структуру и методы построения современных моделей безопасности компьютерных систем;
- передовой опыт лучших специалистов подразделения;
- менеджмент в области программно-аппаратных и технических средств защиты информации.

Исследовать:

- методы организации и управления деятельности служб защиты информации на предприятии;
- технологию проектирования, построения и эксплуатации систем и подсистем компьютерной безопасности;

- методы анализа уязвимости и защищенности информационных процессов;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- методы и схемы управления информационной безопасностью;
- системы и алгоритмы шифрования информации, их свойства, оценки эффективности и их компьютерные модели;
- математические методы, модели и алгоритмы, используемые при разработке инфраструктуры современных криптосистем с открытым ключом, и их компьютерные модели;
- математические и компьютерные модели псевдослучайных генераторов, их свойства и методы статистического тестирования;
- системы и алгоритмы помехоустойчивого кодирования информации, их свойства, оценки эффективности и их компьютерные модели;
- структуру, принципы функционирования и управления современными системами защиты информации в компьютерных системах
- методы оценки экономической эффективности применения программно-аппаратных и технических средств защиты информации.

Содержание практики, вопросы, подлежащие изучению:

- На основе стандартов в области информационной безопасности, нормативных документов и с помощью программно-аппаратных средств контроля вторжений произвести анализ и оценку уровня информационной защищённости предприятия или его компьютерной системы.
- Разработать математические модели защищаемых информационных процессов, исследовать их свойства и приложения для создания средств защиты информации и систем, обеспечивающих информационную безопасность объектов.
- Обосновать и выбрать рациональное решение по уровню обеспечения информационной безопасности предприятия с учетом заданных требований и стандартов информационной безопасности; разработать и обосновать рекомендации по совершенствованию существующей системы информационной безопасности предприятия или его компьютерной системы.
- Разработать модификацию системы информационной безопасности предприятия или его компьютерной системы, или адаптировать существующую для обеспечения требуемого уровня безопасности; разработать необходимое программное обеспечение для модифицированной системы информационной безопасности предприятия или его компьютерной системы.
- Принять участие в разработке технических заданий на проектирование, разработку эскизных, технических и рабочих проектов систем и подсистем защиты информации, с учетом действующих нормативных и методических документов; подробно описать методику и этапы разработки технического задания.
- Принять участие в разработке проектов систем и подсистем управления информационной безопасностью предприятия в соответствии с техническим заданием; подробно описать методику и этапы проектирования.
- Принять участие в экспериментально-исследовательских работах по сертификации средств защиты информации и анализу результатов; подробно описать методику сертификации и порядок проведения соответствующих работ.

- Осуществить сбор и первичную обработку материала для подготовки к написанию выпускной квалификационной работы; разработать и исследовать математические модели, провести компьютерные эксперименты по теме ВКР.

Планируемые результаты практики:

- Перечень рекомендаций по совершенствованию системы информационной безопасности предприятия или его компьютерной системы (рекомендации должны быть обоснованными, т.е. сопровождаться ссылками на соответствующие нормативно-правовые документы в области информационной безопасности или авторитетное мнение специалистов по безопасности).
- Эскизный проект подсистемы информационной безопасности предприятия или его компьютерной системы или системы правления информационной безопасностью (проект опирается на анализ информационной защищенности, нормативно-правовую документацию в области информационной безопасности).
- Научная и практическая части выпускной квалификационной работы, включающие разработанные математические модели, алгоритмы, схемы, описания, методики, компьютерные программы и результаты компьютерных экспериментов по теме ВКР.

Приложение 4

Форма совместного рабочего графика (плана) на преддипломную практику

СОВМЕСТНЫЙ РАБОЧИЙ ГРАФИК (ПЛАН) НА ПРАКТИКУ

«УТВЕРЖДАЮ»
Руководитель практики от БФУ им. И. Канта

_____ / _____ /
«_____»_____ 20__ г.

«СОГЛАСОВАНО»
Руководитель практики
от профильной организации

_____ / _____ /
«_____»_____ 20__ г.

для _____,
(ФИО студента)

Срок прохождения: с «___» _____ 20___ г. по «___» _____ 20___ г.
Место прохождения: _____

№ п/п	Наименование этапа практики	Виды работ (ПРИМЕР формулировок)	Сроки выполнения	Отметка о выполнении
1	**Организационно – подготовительный этап**	- ознакомление с индивидуальным заданием; - прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также действующими в организации правилами внутреннего трудового распорядка организации; - ознакомление с отчетной документацией о прохождении практики	«___» _____ 20___ г.	
2	**Основной этап**	- выполнение индивидуального задания; - ежедневное выполнение установленных программой практики видов работ; - сбор, обработка и систематизация материала по конкретному этапу прохождения практики; - заполнение отчета о прохождении практики	с «___» _____ 20___ г. по «___» _____ 20___ г.	
3	**Заключительный этап**	- прохождение промежуточной аттестации по результатам прохождения практики	«___» _____ 20___ г.	

Приложение 5

Рекомендации по техническому оформлению отчета о результатах прохождения преддипломной практики

Оформление отчета о результатах прохождения преддипломной практики необходимо выполнять в соответствии со следующими правилами.

Объем работы: до 35 страниц формата А4 (210 х 297), но не менее 25 страниц, набранных через полтора интервала на одной стороне листа белой бумаги в текстовом процессоре Word, 2/3 из которых должна занимать практическая часть. Допускается представлять иллюстрации и таблицы на листах формата А3.

Поля: левое - 3 см, правое – 1,5 см, верхнее – 2 см, нижнее – 2 см.

Шрифт: TimesNewRoman, размер шрифта – 14 пунктов.

Титульный лист оформляется по образцу.

Все страницы отчета, включая иллюстрации и приложения, нумеруются по порядку от титульного листа до последней страницы без пропусков и повторений.

Первой страницей является титульный лист, оформленный в соответствующем порядке, номер страницы на нем не ставится. Далее, после титульного листа, вшивается рецензия руководителя практики от предприятия, которая не нумеруется. После вшивается индивидуальное задание на практику, совместный рабочий график (план) на практику и дневник практики, которые не нумеруются. Затем вшивается содержание работы, совпадающее с утвержденным заданием, номер страницы на нем не ставится. Элементы: введение, заключение, список использованной литературы, приложение в содержании и плане не нумеруются.

Далее вшивается первый лист введения, номер страницы на нем не ставится. На последующих страницах порядковый номер печатается в правом верхнем углу без точки в конце, начиная с четвертой страницы, которая является второй страницей введения.

Заголовки основных и дополнительных разделов отчета следует располагать на расстоянии не менее трех интервалов от текста в середине строки без точки в конце и печатать жирным шрифтом, прописными буквами, не подчеркивая.

Заголовки подразделов и пунктов следует начинать с абзацного отступа и печатать жирным шрифтом с прописной буквы, не подчеркивая, без точки в конце.

Если заголовок включает несколько предложений, их разделяют точками. Переносы слов в заголовках не допускаются.

Иллюстрации должны иметь названия. Иллюстрации обозначаются словом "Рисунок", которое помещают под иллюстрацией, и нумеруются последовательно арабскими цифрами в пределах всего отчета. Иллюстрации и таблицы, расположенные на отдельных листах, включают в общую нумерацию страниц. На все иллюстрации должны быть ссылки в отчете. Например,

На рис. 1 представлен...

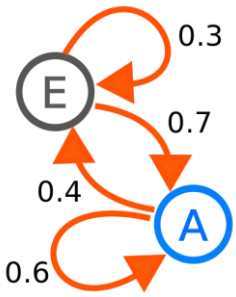

Рис. 1. Название.

Таблицы нумеруют последовательно арабскими цифрами в пределах всего отчёта. В левом верхнем углу таблицы помещают слово "Таблица" с указанием номера этой таблицы и соответствующим заголовком. На все таблицы должны быть ссылки в отчете. Например,… также по итогам работы за первые 3 месяца с заполнением формы (смотри табл. 1).

Таблица 1. Оценка поставщика по критериям.

Показатель	Критерий	Важность	Коэффициент	Балл	Результат	Цель	Оценка прошлого периода
а) Закупка		0,4				2	

(если текста в таблице много, то кегль можно уменьшить до 12, если таблица занимает более 1 страницы, то она убирается в приложения).

Если в отчёте одна таблица, ее не нумеруют и слово "Таблица" не пишут.

Таблицу размещают непосредственно после первого упоминания о ней в тексте на этой же или следующей странице таким образом, чтобы читать ее можно было без поворота или с поворотом по часовой стрелке. Ссылка на таблицу по ходу текста выполняется так: "в таблице 2 приводятся данные о ... ".

Примечания к таблицам, иллюстрациям или пунктам и подпунктам текста размещают непосредственно после пункта, подпункта, таблицы, иллюстрации, к которым они относятся, и печатают с прописной буквы с абзацного отступа. Слово "Примечание" следует печатать с абзацного отступа жирным шрифтом.

Ссылки на разделы, подразделы, пункты, подпункты, иллюстрации, таблицы, формулы, уравнения, перечисления, приложения, следуют указывать порядковым номером, например: "... в разделе 4", "... по пункту 3.3.4", "... в подпункте 2.3.41, перечисление 3", "...по формуле (3)", "... в уравнении (2)",-"... на рисунке 8", "... в приложении 6".

Формулы могут быть вписаны в текст от руки тщательно и разборчиво или напечатаны на компьютере. Не разрешается одну часть формулы вписывать от руки, а другую впечатывать. Выше и ниже каждой формулы должно быть оставлено не менее одной свободной строки. Размеры знаков для формулы рекомендуются следующие: прописные буквы и цифры – 7-8 мм, строчные – 4 мм, показатели степени и индексы – не менее 2 мм.

Формулы обычно располагают отдельными строками посередине листа или внутри текстовых строк. В тексте рекомендуется помещать формулы короткие, простые, не имеющие

самостоятельного значения и не пронумерованные. Наиболее важные формулы, а также длинные и громоздкие формулы, содержащие знаки суммирования, произведения, дифференцирования, интегрирования, располагают на отдельных строках. Для экономии места несколько коротких однотипных формул, выделенных из текста, можно помещать на одной строке, а не одну под другой.

Нумеровать следует наиболее важные формулы, на которые имеются ссылки в последующем тексте. Порядковые номера формул обозначают арабскими цифрами в круглых скобках у правого края страницы, например,

$$(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k} \qquad (1)$$

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой даны в формуле. Значение каждого символа и числового коэффициента следует давать с новой строки. Первую строку пояснения начинают со слова "где" без двоеточия.

Формулы в отчёте следует нумеровать порядковой нумерацией в пределах всего отчета арабскими цифрами в круглых скобках в крайнем правом положении на строке. Если в отчете только одна формула или уравнение, их не нумеруют.

Список использованной литературы должен быть выполнен в соответствии с ГОСТ Р 7.0.5 – 2008 «Библиографическая ссылка».

Рекомендуется представлять единый список литературы к работе в целом. Список обязательно должен быть пронумерован. Каждый источник упоминается в списке один раз, вне зависимости от того, как часто на него делается ссылка в тексте работы. Например,

1. Белл Р.Т. Социолингвистика. Цели, методы, проблемы / пер. с англ. — М.: Международные отношения, 1980. — 318 с.
2. Барт Р. Лингвистика текста // Новое в зарубежной лингвистике. — М.: Прогресс, 1978. — Вып. VIII: Лингвистика текста. — С. 442-449.
3. Войскунский А.Е. Метафоры Интернета // Вопросы философии. — 2001. — № 11. — С. 64-79.
4. Школовая М.С. Лингвистические и семиотические аспекты конструирования идентичности в электронной коммуникации: дис. канд. филол. наук. — Тверь, 2005. — 174 с.
5. Сиротинина О.Б. Структурно-функциональные изменения в современном русском литературном языке: проблема соотношения языка и его реального функционирования // Русская словесность в контексте современных интеграционных процессов: материалы междунар. науч. конф. — Волгоград: Изд-во ВолГУ, 2007. — Т. 1. — С. 14-19.
6. Бахтин М.М. Творчество Франсуа Рабле и народная культура средневековья и Ренессанса. — 2-е изд. — М.: Худож. лит., 1990. — 543 с. [Электронный ресурс]. URL: http://www.philosophy.ru/library/bahtin/rable.html#_ftn1 (дата обращения: 05.10.2008).
7. Белоус Н.А. Прагматическая реализация коммуникативных стратегий в конфликтном дискурсе // Мир лингвистики и коммуникации: электронный научный журнал. — 2006. — № 4 [Электронный ресурс]. URL: http://www.tverlingua.by.ru/archive/005/5_3_1.htm (дата обращения: 15.12.2007).
8. Новикова С.С. Социология: история, основы, институционализация в России. — М.: Московский психолого-социальный институт; Воронеж: Изд-во НПО «МОДЭК», 2000.

— 464 с. [Электронный ресурс]. Систем. требования: Архиватор RAR. — URL: http://ihtik.lib.ru/edu_21sept2007/edu_21sept2007_685.rar (дата обращения: 17.05.2007).
9. Парпалк Р. Общение в Интернете // Персональный сайт Романа Парпалака. — 2006. — 10 декабря [Электронный ресурс]. URL: http://written.ru (дата обращения: 26.07.2006).

На всю использованную литературу должны быть ссылки в тексте работы.

Приложения оформляются следующим образом:

Приложения

(при их наличии)

Приложение 1

Название приложения 1

На каждое приложение должна быть ссылка в тексте.

Отчет о результатах прохождения преддипломной практики вшивается в папку-скоросшиватель с прозрачной верхней обложкой.

Приложение 6

Форма отзыва руководителя практики от организации

ОТЗЫВ
о работе обучающегося в период прохождения практики

Обучающийся _____
(Ф.И.О.)
Института физико-математических наук и информационных технологий проходил производственную преддипломную практику _____
(вид и тип практики)
в период с с «___»_____2019 г. по «___»_____2019 г.
в _____
(*наименование профильной организации с указанием структурного подразделения*)
в качестве _____
(*должность*)

На время прохождения практики _____
(*Фамилия, И.О. обучающегося*)
поручалось решение следующих задач: _____
_____

За время прохождения практики обучающийся проявил _____
_____
_____
_____
_____
(*навыки, активность, дисциплина, помощь организации, качество и достаточность собранного материала для отчета и выполненных работ, поощрения и т.п.*)

Результаты работы обучающегося:
_____
_____
_____
_____
(*Индивидуальное задание выполнено, решения по порученным задачам предложены, материал собран полностью, иное*.)

Считаю, что по итогам практики обучающийся может (не может) быть допущен к защите отчета по преддипломной практике.

_____ _____ _____
(*Должность руководителя практики от профильной организации)* (*подпись*) (*И.О. Фамилия*)

«____»_____2019 г.

М.П.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. Иммануила Канта

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ Е.П.Ставицкая
«20» марта 2020 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«20» марта 2020 г.

Программа производственной практики
по получению профессиональных умений и опыта профессиональной деятельности

для студентов 4 и 5 курсов
очной формы обучения
специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации
квалификация (степень) выпускника: *специалист*

Калининград
2020

Лист согласования

Составитель: к.т.н., доцент Института физико-математических наук и информационных технологий АЛЕШНИКОВ СЕРГЕЙ ИВАНОВИЧ.

Рабочая программа обсуждена и утверждена на заседании Учебно-методического совета ИФМНиИТ.

Протокол №____от «____»_____ 201__ г.

Председатель Совета _____ доцент, к.ф.-м.н. А.А.Шпилевой
Менеджер ООП_____Е.П.Ставицкая

Рабочая программа пересмотрена на заседании Учебно-методического совета ИФМНиИТ

Внесены следующие изменения (или изменений не внесено):

1. _____
2. _____
3. _____

Протокол №____от «____»_____ 20__ г.

Председатель Совета _____ доцент, к.ф.-м.н. А.А.Шпилевой
Менеджер ООП_____Е.П.Ставицкая

Содержание

1. Вид практики, способ и формы ее проведения

Вид практики: Производственная практика по получению профессиональных умений и опыта профессиональной деятельности (далее **производственная практика** или **практика**).

Производственная практика проводится в следующих **формах**:

- непрерывная – в период учебного времени для проведения практики, указанного в календарном учебном графике.

Способы проведения производственной практики:

- стационарная на рабочем месте (в компании, с которой заключен договор на прохождение производственной практики).

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

Целью производственной практики является получение профессиональных умений и опыта профессиональной деятельности.

Задачи производственной практики:

- 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.

В результате освоения ООП обучающийся должен овладеть следующими результатами обучения при прохождении практики:

Код компетенции	**Результаты освоения ООП Содержание компетенций**	**Перечень планируемых результатов обучения при прохождении практики**
ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности.	В результате прохождения практики 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; • ***уметь*:** правильно толковать законы и иные правовые акты, особенно в сфере профессиональной деятельности, связанной с защитой информации; • ***владеть практическими навыками*:** применения законов и иных правовых актов в задачах анализа правовых норм и положений в области информационной безопасности.
ОК-6	Способность работать в коллективе, толерантно воспринимая социаль-	В результате прохождения практики обучающийся должен: • ***знать*:** нормы корректного поведения в обществе; социально-культурные характеристики основных этносов;

	ные, культурные и иные различия	• ***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; • ***владеть практическими навыками*:** урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий при планировании и реализации производственной деятельности трудового коллектива.
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.	В результате прохождения практики обучающийся должен: • ***знать*:** нормы русского языка и одного из иностранных языков; правила построения докладов и презентаций в профессиональной области защиты информации; • ***уметь*:** использовать средства Microsoft Office и/или иные компьютерные программы для создания текстов и презентаций; • ***владеть практическими навыками*:** применения компьютерных средствам создания текстов и презентаций; навыками выступления с докладами и ведения научных дискуссий в профессиональной сфере защиты информации.
ОПК-5	Способность использовать нормативные правовые акты в своей профессиональной деятельности	В результате прохождения практики обучающийся должен: • ***знать*:** 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; • ***уметь*:** правильно толковать законы и иные правовые акты в области защиты информации; • ***владеть практическими навыками*:** применения законов и иных правовых актов в задачах анализа правовых норм и положений, регламентирующих функционирование комплексных систем защиты информации.
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.	В результате прохождения практики обучающийся должен: • ***знать:*** методы и сертифицированные программно-аппа-ратные 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; • ***уметь*:** 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; • ***владеть практическими навыками*:** 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.
ПК-6	Способность участво-	В результате прохождения практики обучающийся должен:

	вать в разработке проектной и технической документации	• ***знать*:** 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; • ***уметь*:** выполнять расчётные работы и подготовку текстовых и графических документов средствами Microsoft Office и/или иными средствами; • ***владеть практическими навыками*:** проектирования подсистем информационной безопасности; навыками организации работы по проектированию систем информационной безопасности.
ПК-8	Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы	В результате прохождения практики обучающийся должен: • ***Знать*:** современные информационные методики и технологии, методы математической обработки информации, методы теоретического и экспериментального исследования, стандарты и нормативы в области информационной безопасности. • ***Уметь*:** грамотно применять изученные математические методы, математические пакеты для обработки, детального анализа и систематизации криптографической информации, строить схемы и модели подсистем информационной безопасности компьютерной системы. • ***Владеть практическими навыками*:** проектирования систем защиты информации, навыками применения современных компьютерных технологий, построения математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, навыками оценки эффективности их применения.

3. Место производственной практики в структуре ООП

Производственная практика относится к базовой части блока 2 «Практики, в том числе научно-исследовательская работа (НИР)» ООП подготовки специалистов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

Логическая и содержательная связь дисциплин и практик, участвующих в формировании представленных в п.2 компетенций, содержится в ниже представленной таблице:

Компетенция	Предшествующие дисциплины	Данная дисциплина	Последующие дисциплины
ОК-4	− Основы предпринимательской деятельности.	Производственная практика	− Подготовка к процедуре защиты ВКР.
ОК-6	− Основы деловых коммуникаций. − Учебная практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности. − Управление командой.		− Подготовка к процедуре защиты ВКР.
ОК-7	− Иностранный язык. − Основы деловых коммуникаций.		− Процедура защиты ВКР.
ОПК-5	− Безопасность жизнедеятельности. − Основы информационной безопасности.		− Подготовка к процедуре защиты ВКР.

	− Организационное и правовое обеспечение информационной безопасности.		
ПК-5	− Криптографические методы защиты информации. − Криптографические протоколы. − Основы построения защищённых компьютерных сетей. − Защита в операционных системах. − Защита программ и данных. − Основы построения защищённых баз данных. − Методы и алгоритмы генерации гиперэллиптических кривых для криптографии. − Методы и алгоритмы генерации эллиптических кривых для криптографии. − Спаривания на эллиптических кривых.		− Подготовка к процедуре защиты ВКР.
ПК-6	− Организационное и правовое обеспечение информационной безопасности. − Элективные курсы по физической культуре и спорту. − Основы HTML-5. − Управление командой.		− Подготовка к процедуре защиты ВКР.
ПК-8	- Модели безопасности компьютерных систем. - Организационное и правовое обеспечение информационной безопасности. - Компьютерный практикум по криптографии на эллиптических кривых. - Компьютерный практикум по криптографии на гиперэллиптических кривых. - Криптографические протоколы для защиты банковской информации. - Анализ стойкости финансовых протоколов. - Функциональные поля и их приложения. - Локальные поля и их приложения. - Методы и алгоритмы генерации эллиптических кривых для криптографии. - Спаривания на эллиптических кривых.		− Производственная преддипломная практика. − Подготовка к процедуре защиты выпускной квалификационной работы.

4. Объем практики в зачетных единицах и ее продолжительность в неделях либо в академических или астрономических часах

Производственная практика для обучающихся по специальности 10.05.01 – «Компьютерная безопасность», специализация: «Математические методы защиты информации» проводится в 8 семестре в течение 2 недель и в 10 семестре в течение 2 недель, трудоемкость производственной практики – 6 зачетных единиц.

Объём учебной практики	**Всего часов**	
	Контактные часы	**Самостоятельная работа**
Контактная работа обучающихся с препода-	2,0	

вателем (самостоятельная работа студента под руководством преподавателя).		
Самостоятельная работа обучающихся		212
Промежуточная аттестация – зачет с оценкой	0,5	1,5
Итого	2,5	213,5
Общая трудоемкость практики	216 часов (6 ЗЕ)	

5. Содержание практики

Студенты-практиканты выполняют программу практики в соответствии с планом-графиком практики, утверждаемым руководством базового предприятия и представителями института физико-математических наук и информационных технологий БФУ им. И. Канта.

Ведется дневник практики и составляется заключительный отчет, который защищается после окончания практики и утверждается руководителями практики со стороны базового предприятия и института. В зависимости от специализации базового подразделения, в котором студент проходит практику, осуществляется корректировка направления его деятельности.

Студентам-практикантам должна быть предоставлена возможность ознакомиться с научно-технической документацией и научной литературой, которая касается предмета его исследований. В процессе прохождения практики студенты прослушивают лекции ведущих специалистов базовых предприятий, участвуют в научно-технических семинарах и конференциях при их наличии.

Студенты-практиканты проходят практику в отделах компьютерной безопасности, информационной и технической безопасности, компьютерных лабораториях, в которых работают их руководители и сотрудники подразделений. Они должны иметь доступ к программно-техническим комплексам, программным комплексам, математическому обеспечению и техническим средствам, необходимым для исследований, иметь возможность непосредственных консультаций во время работы со специалистами подразделений. Практиканты ежедневно работают в течение 3-4 часов в отделах предприятия. Объем теоретических занятий и семинаров определяется спецификой базового предприятия.

При прохождении производственной практики студенты изучают:

- административную и информационную структуру предприятия;
- основные нормативно-правовые положения в области информационной безопасности и защиты информации;
- должностные инструкции сотрудников организации, отвечающих за безопасность;
- применяемые технические и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации;
- потенциальные каналы утечки информации, способы их выявления и методы оценки опасности;

- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- принципы построения современных криптографических систем, стандарты в области криптографической защиты информации;
- передовой опыт лучших специалистов подразделения;
- менеджмент в области программно-аппаратных и технических средств защиты информации.

При прохождении производственной практики студенты разрабатывают и исследуют:

- методы организации и управления деятельности служб защиты информации на предприятии;
- технологию проектирования, построения и эксплуатации систем компьютерной безопасности;
- методы анализа уязвимости и защищенности информационных процессов;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- методы и схемы управления информационной безопасностью;
- методы оценки экономической эффективности применения программно-аппаратных и технических средств защиты информации.

При прохождении производственной практики возможен следующий перечень индивидуальных заданий:

- анализ и оценка уровня информационной защищённости предприятия или его компьютерной системы;
- разработка рекомендаций по совершенствованию системы информационной безопасности предприятия или его компьютерной системы;
- модификация / адаптация системы информационной безопасности предприятия или его компьютерной системы;
- разработка программного обеспечения для модифицированной системы информационной безопасности предприятия или его компьютерной системы.

Задание на практику определяется вместе со студентом руководителями практики со стороны института и предприятия в начале практики. В конце практики студент должен представить результаты практики в виде отчета и сдать его руководителю от института. Руководитель практики от института организует защиту отчетов, по результатам которой на основании решения комиссии выставляется промежуточный контроль в виде зачета с оценкой.

Кроме того, при прохождении производственной практики на предприятии, учреждении, организации, студент обязан:

- пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка;
- посещать все мероприятия по месту практики;
- подчиняться действующим на предприятии, в учреждении, организации правилам внутреннего трудового распорядка;

– изучить и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии.

Особое внимание следует уделить внедрению результатов, полученных практикантом, по месту практики, а также анализу возможности применения и / или внедрения в производство предполагаемых результатов исследований по теме ВКР.

Краткий план-график производственной практики

8 и 10 семестры

№ п/п	Этапы (периоды) практики	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
1	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 (программа практики и дневник практики с направлением на практику) в сроки, определенные программой. 8. Изучение правовых основ, базовых нормативных и локальных правовых актов, регулирующих деятельность базы практики.	12	Письменный отчёт. Индивидуальное задание на практику.
2	Основной этап	1. Ознакомление с конкретными видами деятельности в соответствии с положениями структурных подразделений и должностными инструкциями. 2. Ознакомление с задачами отдела/службы организации базы практики. 3. Выполнение заданий, поставленных руководителями практики. 4. Выполнение программы практики, индивидуального задания на практику. 5. Сбор информации и материалов практики. 6. Обработка, систематизация и анализ фактического и теоретического материала. 7. Введение дневника практики.	78	Письменный отчет. Дневник практики
3	Заключительный этап	1. Выявление возможных недостатков в работе подразделения – места прохождения практики, их оценка и разработка предложений по совершенствованию суще-	18	Зачет с оценкой.

№ п/п	Этапы (периоды) практики	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
		ствующего порядка работы, а также по внедрению новых методов работы. 2. Подготовка отчета о прохождении практики, представления отчета по практики и прилагаемых документов для защиты.		
	Итого часов		**108**	

6. Формы отчетности по практике

Формы отчетности студентов по производственной практике (заверенные подписью и печатью руководителя базы практики или руководителя практики от института):

- индивидуальное задание на практику, заверенное руководителями практики от института и организации;
- план-график прохождения практики, заверенный руководителями практики от института и организации;
- дневник практики, заверенный руководителем практики от организации;
- отчет о результатах прохождения практики.

Формы отчетности руководителей практики:

- руководитель практики от института не позднее 1 месяца после окончания практики предоставляет в институт отчет о проведенной производственной практике;
- руководитель практики от организации предоставляет Отзыв о работе каждого студента-практиканта на практике.

Оформление результатов практики (*отчетов, характеристик, дневников*)

По окончании производственной практики студент обязан составить письменный отчет и сдать его руководителю практики от института. Отчет о практике должен содержать сведения о конкретной выполненной студентом запланированной работе (в соответствии с индивидуальным заданием на практику) в период прохождения практики, а также краткое описание структуры, целей и задач предприятия, организации, выводы и предложения.

Для оформления отчета студенту выделяется в конце практики 2 дня.

Требования, предъявляемые к оформлению отчета по производственной практике

Отчет по производственной практике должен состоять из Оглавления, Введения, описание основной части отчета (содержания практики), Заключения, Списка цитированной литературы.

Описание основной части отчета по производственной практике должно содержать:

– задание на производственную практику, полученное от руководителя;

– описание выполнения заданий, а также текущих поручений руководителя практики.

Рекомендуемый объем отчета не менее 10 страниц. Образец титульного листа прилагается (Приложение 1). Переплет отчета может быть произвольным и исключать рассыпание листов. Оформление отчета – см. Приложение 5.

Представленный студентом отчет рецензируется руководителем практики от института. В случае положительной рецензии он выносится на защиту.

Защита отчета осуществляется перед комиссией, которая состоит из преподавателей и руководителей производственной практики.

Порядок аттестации студентов по результатам практики

По окончании производственной практики проводится ***дифференцированный зачет.*** При проведении зачета используются следующие критерии итоговой оценки за производственную практику:

- полный и аккуратно оформленный в соответствии с требованиями отчет;
- наличие разработанного и успешно протестированного программного продукта, реализующего безопасность отдельных компонент компьютерной системы предприятия, либо
- развёрнутые рекомендации по совершенствованию системы информационной безопасности предприятия или его компьютерной системы, либо
- наличие эскизного проекта модификации соответствующей системы информационной безопасности предприятия или его компьютерной системы;
- правильные ответы студента на вопросы преподавателя, касающиеся предмета практики.

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

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках производственной практики

Компетенция	Этапы формирования компетенции	Показатели оценивания компетенции	Критерии оценивания компетенций	Шкала оценивания	Виды аттестации и виды оценочных средств

ОК-4 Способность использовать основы правовых знаний в различных сферах деятельности.	Начальный этап	***знать*** проблемы и задачи, возникающие в сфере правового регулирования вопросов информационной безопасности; основные положения законов и иных правовых актов, регулирующих взаимоотношения между субъектами в области информационной безопасности; функции и сферы ответственности регулирующих органов; ***уметь*** правильно толковать законы и иные правовые акты в сфере профессиональной деятельности, связанной с защитой информации; ***владеть практическими навыками*** применения законов и иных правовых актов в задачах анализа правовых норм и положений в области информационной безопасности.	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание проблематики в сфере правового регулирования сферы информационной безопасности, правовых и нормативных актов, регулирующих данную сферу, функции и сферы ответственности регуляторов. Умение верно трактовать правовые и нормативные акты в сфере информационной безопасности. Владение практическими навыками применения правовых и нормативных актов в области информационной безопасности, навыками анализа правовых норм и положений.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных проблем в сфере правового регулирования сферы информационной безопасности, основных правовых и нормативных актов, регулирующих данную сферу, основные функции и сферы ответственности регуляторов. Умение в основном верно трактовать правовые и нормативные акты в сфере информационной безопасности. Владение некоторыми практическими навыками применения правовых и нормативных актов в области информационной безопасности, некоторыми навыками анализа правовых норм и положений.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знакомство с проблематикой в сфере правового регулирования сферы информационной безопасности, знакомство с правовыми и нормативными актами, регулирующими данную сферу, знание некоторых функций регуляторов. Умение в основном верно трактовать некоторые правовые и нормативные акты в сфере информационной безопасности. Владение некоторыми практическими навыками применения отдельных правовых и нормативных актов в области информационной безопасности, некоторыми навыками анализа правовых норм и положений.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: Незнание проблем в сфере правового регулирования сферы информационной безопасности, незнание правовых и нормативных актов, регулирующих данную сферу, незнание функций и сфер ответственности регуляторов. Неумение трактовать правовые и нормативные акты в сфере информационной безопасности. Отсутствие практических навыков применения	< 50%	

			правовых и нормативных актов в области информационной безопасности, навыков анализа правовых норм и положений.		
ОК-6 Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Начальный этап	***знать*:** нормы корректного поведения в обществе; социально-культурные характеристики основных этносов; ***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; ***владеть практическими навыками*:** урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий при планировании и реализации производственной деятельности трудового коллектива.	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание норм корректного поведения в обществе; социально-культурных характеристик основных этносов, принципов функционирования команд / коллективов работников; Умение 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; Владение практическими навыками урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий при планировании и реализации производственной деятельности трудового коллектива.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание норм корректного поведения в обществе; ряда социально-культурных характеристик основных этносов, некоторых принципов функционирования команд / коллективов работников; Умение толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей; планировать и осуществлять производственную деятельность в коллективе; Владение некоторыми практическими навыками урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знание основных норм корректного поведения в обществе; отдельных социально-культурных характеристик основных этносов, отдельных принципов функционирования команд / коллективов работников; Умение в основном толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей; осуществлять производственную деятельность в коллективе; Владение практическими навыками избегать возникающие противоречия между членами трудового коллектива; отдельными навыками применения методики учёта социально культурных различий.	от 50% до 70%	

			Обучающийся ***на низком уровне*** демонстрирует: Незнание социально-культурных характеристик основных этносов, принципов функционирования команд / коллективов работников; Неумение толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей; осуществлять производственную деятельность в коллективе; избегать возникающих противоречий между членами трудового коллектива.	< 50%	
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.	Начальный этап	***знать*:** нормы русского языка и одного из иностранных языков; правила построения докладов и презентаций в профессиональной области защиты информации; ***уметь*:** использовать средства Microsoft Office и/или иные компьютерные программы для создания текстов и презентаций; ***владеть практическими навыками*:** применения компьютерных средств создания текстов и презентаций; навыками выступления с докладами и ведения научных дискуссий в профессиональной сфере защиты информации.	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание норм и правил русского языка и одного из иностранных языков; правил построения докладов и презентаций в профессиональной области защиты информации; Умение использовать средства Microsoft Office и/или иных компьютерных программ для создания текстов и презентаций; Владение практическими навыками применения компьютерных средств создания текстов и презентаций; навыками выступления с докладами и ведения научных дискуссий в профессиональной сфере защиты информации.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных норм и правил русского языка и одного из иностранных языков; основных правил построения докладов и презентаций в профессиональной области защиты информации; Умение использовать основные средства Microsoft Office и/или иных компьютерных программ для создания текстов и презентаций; Владение практическими навыками применения основных компьютерных средств создания текстов и презентаций; некоторыми навыками выступления с докладами и ведения научных дискуссий в профессиональной сфере защиты информации.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знание ряда норм и правил русского языка и одного из иностранных языков; ряда правил построения докладов и презентаций в профессиональной области защиты информации; Умение использовать отдельные средства Microsoft Office и/или иных компьютерных программ для создания текстов и презентаций; Владение практическими навыками применения ряда компьютерных средств создания текстов и презентаций; некоторыми навыками выступления с докладами и ведения научных дискуссий в профессиональной сфере защиты информации.	от 50% до 70%	

			Обучающийся ***на низком уровне*** демонстрирует: Незнание норм и правил русского языка и одного из иностранных языков; правил построения докладов и презентаций в профессиональной области защиты информации; Неумение использовать средства Microsoft Office и/или иных компьютерных программ для создания текстов и презентаций; применять компьютерные средства создания текстов и презентаций; выступать с докладами и вести научные дискуссии в профессиональной сфере защиты информации.	< 50%	
ОПК-5 Способность использовать нормативные правовые акты в своей профессиональной деятельности	Промежуточный этап	***знать*:** 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; ***уметь*:** правильно толковать законы и иные правовые акты в области защиты информации; ***владеть практическими навыками*:** применения законов и иных правовых актов в задачах анализа правовых норм и положений, регламентирующих функционирование комплексных систем защиты информации.	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание проблем и задач, возникающих в сфере правового регулирования информационной безопасности; положений законов и иных правовых актов, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; функций и сфер ответственности регулирующих органов в области информационной безопасности; Умение правильно толковать законы и иные правовые акты в области защиты информации; Владение практическими навыками применения законов и иных правовых актов в задачах анализа правовых норм и положений, регламентирующих функционирование комплексных систем защиты информации.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных проблем и задач, возникающих в сфере правового регулирования информационной безопасности; основных положений законов и иных правовых актов, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; основных функций и сфер ответственности регулирующих органов в области информационной безопасности; Умение правильно толковать ряд законов и иных правовых актов в области защиты информации; Владение практическими навыками применения ряда законов и иных правовых актов в задачах анализа правовых норм и положений, регламентирующих функционирование комплексных систем защиты информации.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знание некоторых проблем и задач, возникающих в сфере правового регулирования информационной безопасности; некоторых положений законов и иных правовых актов, регулирующих взаимоотношения между субъектами в сфере	от 50% до 70%	

			информационной безопасности; отдельных функций и сфер ответственности регулирующих органов в области информационной безопасности; Умение правильно толковать отдельные законы и иные правовые акты в области защиты информации; Владение практическими навыками применения отдельных законов и иных правовых актов в задачах анализа правовых норм и положений, регламентирующих функционирование комплексных систем защиты информации.		
			Обучающийся ***на низком уровне*** демонстрирует: Незнание проблем и задач, возникающих в сфере правового регулирования информационной безопасности; положений законов и иных правовых актов, регулирующих взаимоотношения между субъектами в сфере информационной безопасности; функций и сфер ответственности регулирующих органов в области информационной безопасности; Неумение правильно толковать законы и иные правовые акты в области защиты информации; применять законы и иные правовые акты в задачах анализа правовых норм и положений.	< 50%	
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.	Промежуточный этап	***знать:*** методы и сертифицированные программно-аппа-ратные 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;	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание методов и сертифицированных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем; способов и средств антивирусной защиты; принципов построения и оценки эффективности криптографических алгоритмов, а также разрешённых к применению средств криптографической защиты; процедур распределения и сертификации криптографических ключей; типовых схем обеспечения информационной безопасности компьютерных систем; Умение 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; Владение практическими навыками 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.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет

		***уметь*:** 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; ***владеть практическими навыками*:** 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.	Обучающийся ***на высоком уровне*** демонстрирует: Знание основных методов и сертифицированных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем; основных способов и средств антивирусной защиты; основных принципов построения и оценки эффективности криптографических алгоритмов, а также разрешённых к применению средств криптографической защиты; основных процедур распределения и сертификации криптографических ключей; типовых схем обеспечения информационной безопасности компьютерных систем; Умение осуществлять анализ уровней информационной защищённости компьютерных систем; разрабатывать проекты подсистем обеспечения информационной безопасности компьютерных систем; готовить научно-техническую документацию, презентации; Владение практическими навыками решения основных задач обеспечения информационной безопасности компьютерных систем с использованием основных программно-аппаратных средств на конкретном рабочем месте в качестве исполнителя или стажера; основными навыками проектирования систем защиты информации и подготовки соответствующей научно-технической документации.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знание ряда методов и сертифицированных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем; отдельных способов и средств антивирусной защиты; ряда принципов построения и оценки эффективности криптографических алгоритмов, а также разрешённых к применению средств криптографической защиты; отдельных процедур распределения и сертификации криптографических ключей; Умение, в основном, осуществлять анализ уровней информационной защищённости компьютерных систем; разрабатывать проекты отдельных блоков подсистем обеспечения информационной безопасности компьютерных систем; готовить презентации; Владение практическими навыками решения отдельных задач обеспечения информационной безопасности компьютерных систем с использованием ряда программно-аппаратных средств; отдельными навыками проектирования блоков подсистем защиты информации.	от 50% до 70%	
			Обучающийся ***на низком уровне***	< 50%	

			демонстрирует: Незнание методов и сертифицированных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем; способов и средств антивирусной защиты; принципов построения и оценки эффективности криптографических алгоритмов, а также разрешённых к применению средств криптографической защиты; процедур распределения и сертификации криптографических ключей; Неумение осуществлять анализ уровней информационной защищённости компьютерных систем; разрабатывать проекты отдельных блоков подсистем обеспечения информационной безопасности компьютерных систем; готовить презентации; решать задачи обеспечения информационной безопасности компьютерных систем с использованием программно-аппаратных средств; проектировать подсистемы защиты информации.		
ПК-6 Способность участвовать в разработке проектной и технической документации.	Промежуточный этап	***знать*:** 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; ***уметь*:** выполнять расчётные работы и подготовку текстовых и графических документов средствами Microsoft Office и/или иными средствами; ***владеть практическими навыками*:** проектирования подсистем информационной безопасности; навыками организации работы по проектированию систем	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание перечня необходимой проектной и технической документации, регламентирующей построение эффективных систем защиты информации; правил и этапов разработки проектной и технической документации в области обеспечения информационной безопасности компьютерных систем; Умение выполнять расчётные работы и подготовку текстовых и графических документов средствами Microsoft Office и/или иными средствами; Владение практическими навыками проектирования подсистем информационной безопасности; навыками организации работы по проектированию систем информационной безопасности.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных пунктов перечня проектной и технической документации, регламентирующей построение эффективных систем защиты информации; основных правил и этапов разработки проектной и технической документации в области обеспечения информационной безопасности компьютерных систем; Умение выполнять основные расчёты и готовить текстовые и графические документы средствами Microsoft Office и/или иными средствами; Владение практическими навыками проектирования отдельных подсистем информационной безопасности; навыками организации работы по проектированию отдельных подсистем информационной безопасности.	от 70% до 85%	

		информационной безопасности.	Обучающийся ***на среднем уровне*** демонстрирует: Знакомство с перечнем проектной и технической документации, регламентирующей построение эффективных систем защиты информации; с основными правилами и этапами разработки проектной и технической документации в области обеспечения информационной безопасности компьютерных систем; Умение выполнять некоторые расчёты и готовить текстовые и графические документы средствами Microsoft Office и/или иными средствами; Владение практическими навыками проектирования отдельных блоков подсистем информационной безопасности; навыками организации работы по проектированию отдельных блоков подсистем информационной безопасности.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: Незнание перечня проектной и технической документации, регламентирующей построение эффективных систем защиты информации; правил и этапов разработки проектной и технической документации в области обеспечения информационной безопасности компьютерных систем; Неумение выполнять расчёты и готовить текстовые и графические документы средствами Microsoft Office и/или иными средствами; проектировать отдельные блоки подсистем информационной безопасности; организовывать работы по проектированию подсистем информационной безопасности.	< 50%	
ПК-8 Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы	Промежуточный этап	***Знать*:** современные информационные методики и технологии, методы математической обработки информации, методы теоретического и экспериментального исследования, стандарты и нормативы в области информационной безопасности. ***Уметь*:** грамотно применять изученные математические методы, математические пакеты для обработки, детального анализа и систематизации	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание современных информационных методик и технологий, методов математической обработки информации, методов теоретического и экспериментального исследования, стандартов и нормативов в области информационной безопасности. Умение грамотно применять изученные математические методы, математические пакеты для обработки, детального анализа и систематизации криптографической информации, строить схемы и модели подсистем информационной безопасности компьютерной системы. Владение практическими навыками проектирования систем защиты информации, навыками применения современных компьютерных технологий, построения математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, навыками оценки эффективности их применения.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет

		криптографической информации, строить схемы и модели подсистем информационной безопасности компьютерной системы. ***Владеть практическими навыками*:** проектирования систем защиты информации, навыками применения современных компьютерных технологий, построения математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, навыками оценки эффективности их применения.	Обучающийся ***на высоком уровне*** демонстрирует: Знание основных информационных методик и технологий, основных методов математической обработки информации, основных методов теоретического и экспериментального исследования, основных стандартов и нормативов в области информационной безопасности. Умение применять изученные математические методы, математические пакеты для обработки, анализа и систематизации криптографической информации, строить схемы и модели основных подсистем информационной безопасности компьютерной системы. Владение практическими навыками проектирования основных систем защиты информации, навыками применения основных компьютерных технологий, построения математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, навыками оценки эффективности их применения.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знание отдельных информационных методик и технологий, основных методов математической обработки информации, отдельных методов теоретического и экспериментального исследования, основных стандартов и нормативов в области информационной безопасности. Умение применять отдельные математические методы, математические пакеты для обработки, анализа и систематизации криптографической информации, строить схемы и модели отдельных подсистем информационной безопасности компьютерной системы. Владение практическими навыками проектирования отдельных подсистем защиты информации, навыками применения отдельных компьютерных технологий, построения простых математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, навыками упрощённой оценки эффективности их применения.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: Незнание информационных методик и технологий, методов математической обработки информации, методов теоретического и экспериментального исследования, стандартов и нормативов в области информационной безопасности. Неумение применять математические методы, математические пакеты для обработки, анализа и систематизации криптографической информа-	< 50%	

			ции, строить схемы и модели подсистем информационной безопасности компьютерной системы; проектировать подсистемы защиты информации, применять компьютерные технологии, строить математические модели информационных потоков, возникающих при построении криптографической инфраструктуры, оценивать эффективность их применения.		

Указанные компетенции формируются у студентов в процессе прохождения производственной практики. Формой текущего контроля за сформированностью компетенций является написание отчета по производственной практике.

7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкалы оценивания

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания приведены в п. 7.1.

Для оценивания уровня сформированности компетенций используется следующая шкала, где оценки определяются по результатам (R), полученным во время аттестации, для каждой из компетенций исходя из следующих условий:

- «отлично»: $R \geq 85$ %;
- «хорошо»: $70 \leq R < 85$ %;
- «удовлетворительно»: $50\ \% \leq R < 70$ %;
- «неудовлетворительно»: $R < 50$ %.

Далее рассчитывается итоговая оценка (S) по следующей формуле:

$$S = \frac{\sum_{k=0}^{n} R_k}{n},$$

где: R_k – оценка по k-ой компетенции, n – общее количество оцениваемых компетенций.

В качестве оценки за зачет с оценкой выставляется следующая, в зависимости от полученного значения S:

- «отлично»: $S \geq 85$ %;
- «хорошо»: $70\ \% \leq S < 85$ %;
- «удовлетворительно»: $50\ \% \leq S < 70$ %;
- «неудовлетворительно»: $S < 50$ %.

7.3. Комплект оценочных средств по всем заявленным в рабочей программе видам занятий и самостоятельной работы обучающихся

В комплект оценочных средств входят оценочные средства по контролю промежуточной аттестации обучающихся по всем заявленным в рабочей программе видам работ обучающихся:

- индивидуальные задания для прохождения практики;
- контрольные вопросы к дифференцируемому зачету;
- отзыв руководителя практики от предприятия;

- отчет студента о прохождении практики.

Примерные контрольные вопросы к дифференцированному зачету по практике:

1. Какие нормативные документы по охране труда, технике безопасности и пожарной безопасности вам были предоставлены для изучения?
2. В чем заключались Ваши права и обязанности в соответствии с должностной инструкцией?
3. Какие нормативные документы для составления отчетности используются на предприятии?
4. Суть порученных Вам производственных задач.
5. Какие методы, технологии были предложены вами для решения поставленных производственных задач?
6. Какие информационные системы/технологии используются на предприятии?
7. Описать административную и информационную структуру предприятия.
8. Описать цели и задачи, решаемые предприятием, направление деятельности предприятия.
9. Описать используемые на предприятии технические и программные средства вычислительной техники.
10. Описать организацию информационных систем с точки зрения информационной защищенности и защиты государственной тайны.
11. Описать технические устройства хранения, обработки и передачи информации, используемые на предприятии.
12. Представить анализ потенциальных каналов утечки информации и уязвимостей информационных процессов.
13. Описать схему инженерно-технической защиты информации.
14. Описать используемые методы и средства противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
15. Представить перечень правовых положений в области информационной безопасности и защиты информации, регламентирующих уровень защищённости базового предприятия;
16. Представить и обосновать рекомендации по совершенствованию системы информационной безопасности предприятия или его компьютерной системы.
17. Представить эскизный проект модификации системы информационной безопасности предприятия или его компьютерной системы.
18. Описать структуру и функции разработанного программного обеспечения для модифицированной системы информационной безопасности предприятия или его компьютерной системы.
19. Каковы выводы и предложения по внедрению рекомендаций по совершенствованию системы информационной безопасности на предприятии?

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка сформировавшихся компетенций по производственной практике проводится в форме текущей и промежуточной аттестации.

Текущий контроль осуществляется руководителем практики от базовой организации. Руководитель практики от организации контролирует выполнение индивидуального задания согласно плану-графику, оценивает каждый этап выполнения в дневнике практики.

Промежуточный контроль осуществляется на дифференцированном зачете.

На зачет студенты предоставляют следующие документы, заверенные подписью и печатью руководителя базы практики или руководителя практики от института:

- индивидуальное задание на практику, заверенное руководителями практики от института и организации;
- план-график прохождения практики, заверенный руководителями практики от института и организации;
- дневник практики, заверенный руководителем практики от организации;
- отчет о результатах прохождения практики.

Защита отчета осуществляется перед комиссией, которая состоит из преподавателей и руководителей производственной практики.

Критерии выставления итоговой оценки- см. п . 7.2.

8. Перечень учебной литературы и ресурсов сети Интернет, необходимых для проведения практики

8.1. Основная литература

1. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета) №1512. утвержден 1 декабря 2016 г.
2. Приказ Минобрнауки России от 27.11.2015 №1383 «Об утверждении Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования» (зарегистрировано в Минюсте России 18.12.2015 №40168);
3. Положение о практике обучающихся, осваивающих основные профессиональные программы высшего образования БФУ им. И. Канта (принято решением ученого совета БФУ им. И. Канта 29 июня 2016 года, протокол №23).

8.2. Дополнительная литература

1. Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности [Текст] : учеб. пособие для вузов / С.В. Запечников, 2007. - 319 с. **(15 экз.)**
2. Защита информации **[Электронный ресурс]** : учеб. пособие для вузов / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин, 2015. - 1 эл. опт. диск (CD-ROM), 391, [1]
3. Колесниченко О. В. Аппаратные средства PC [Текст] / Олег Колесниченко, Игорь Шишигин, Валентин Соломенчук, 2010. - 782 с. **(12 экз.)**
4. Основы информационной безопасности [Текст] : учеб. пособие / Е. Б. Белов [и др.],

2006. - 544 с. **(16 экз.)**
5. Проскурин В. Г. Защита в операционных системах [Текст] : учеб. пособие для вузов / В. Г. Проскурин, 2014. - 192 с. **(10 экз.)**, 2000. – 166 с. **(1 экз.)**
6. Проскурин В. Г. Защита программ и данных [Текст] : учеб. пособие для вузов / В. Г. Проскурин, 2012. - 198, [1] с. **(15 экз.)**
7. Платонов В. В. Программно-аппаратные средства защиты информации [Текст] : учеб. для вузов / В. В. Платонов, 2014. - 330, [1] с. **(10 экз.)**
8. Смарт Н. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешов под ред. С. К. Ландо, 2006. - 525 с. **(17 экз.)**
9. Технические средства и методы защиты информации [Текст] : учеб. пособие для вузов / А. П. Зайцев [и др.], 2012. - 615 с. **(15 экз.)**
10. Физические основы защиты информации, обрабатываемой средствами вычислительной техники [Электронный ресурс] / сост. А. С. Горбачев, 2015 **on-line**, 283 с.
11. Хорев П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев, 2006. - 327 с. **(18 экз.)**

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для выполнения производственной практики

1. http://xn--90ax2c.xn--p1ai/ – «Национальная электронная библиотека».
2. http://lib.kantiana.ru/irbis/standart/ELIB – ЭБС Кантиана.
3. http://elibrary.ru/defaultx.asp – Научная электронная библиотека eLIBRARY.RU.
4. http://www.iacr.org – Международная ассоциация криптологических исследований (International Association for Cryptologic Research - IACR).
5. http://www.ifca.ai – Международная ассоциация финансовой криптографии (International Financial Cryptography Association – IFCA).
6. http://csrc.nist.gov – Национальный институт стандартов и технологий США (National Institute of Standards and Technology NIST).
7. http://dorlov.blogspot.ru/p/blog-page_3151.html - Перечень сайтов по информационной безопасности.
8. http://www.kaspersky.ru/protect-my-business/?cid=ru_RU:SEM:kl_google_business_nb&gclid=CJKilc2bqsoCFQISGwodvSULA – Лаборатория Касперского.
9. http://www.itsec.ru/main.php - Форум по информационной безопасности.
10. http://www.securitylab.ru – Информационный сайт по компьютерной безопасности.

9. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

9.1. Перечень информационных технологий, используемых при проведении практики

Для подготовки, прохождения практики и составления отчета используются следующие информационные технологии:

- технические средства: компьютерная техника и средства связи (персональные компьютеры, проектор, интерактивная доска, видеокамеры и пр.);

- методы обучения с использованием информационных технологий (компьютерное тестирование, демонстрация мультимедийных материалов и пр.);

- перечень интернет-сервисов и электронных ресурсов (поисковые системы, электронная почта, профессиональные, тематические чаты и форумы, системы видео- и аудиоконференций, он-лайн энциклопедии и справочники). Институт обеспечен лицензионным программным обеспечением.

9.2. Перечень программного обеспечения (используемое при необходимости)

- Программа для ЭВМ Wolfram Mathematica 10.2 Education Bundled Price (Количество лицензий – 3, Номер акта / накладной – Tr053766, Дата акта – 02.11.15);
- IBM SPSS Statistics Base Campus Edition (Количество лицензий – 25, Номер акта / накладной – Tr031923, Дата акта – 10.06.15);
- Intel Cluster Studio for Linux (Количество лицензий – 2, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Maple 11 (Количество лицензий – 30, Номер акта / накладной – Tr068983, Дата акта – 19.12.07);
- Mathematica (Количество лицензий – 15, Номер акта / накладной – Tr066706, Дата акта – 18.11.13);
- Mathworks Gauges Blockset Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Mathworks Simulink 3d animation Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Microsoft SQL Srv Standard Core 2014 (Количество лицензий – 4, Номер акта / накладной – Tr063168, Дата акта – 24.11.14);
- Microsoft Visio Professional 2010 (Количество лицензий – 25, Номер акта / накладной – Tr070182, Дата акта – 15.12.11);
- Microsoft Visual Studio 2005 (Количество лицензий – 30, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).
- Parallel Computing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Signal Processing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Statistica Base (Количество лицензий – 20, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).
- Statistics Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- System Identification Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11).

9.3. Информационные справочные системы

1. http://xn--90ax2c.xn--p1ai/ – «Национальная электронная библиотека».
2. http://lib.kantiana.ru/irbis/standart/ELIB – ЭБС Кантиана.
3. http://elibrary.ru/defaultx.asp – Научная электронная библиотека eLIBRARY.RU.
4. http://infomag.biz/index.php – Служба ИНФОМАГ - Библиографическая и другая научная информация, в первую очередь оглавления научных и технических журналов, а также зарубежных научных электронных бюллетеней.
5. http://window.edu.ru/ – Информационная система «Единое окно доступа к образовательным ресурсам».
6. http://www.rsl.ru/ – Российская государственная библиотека.
7. http://www.biblioclub.ru/ – Университетская библиотека онлайн.

10. Описание материально-технической базы, необходимой для проведения практики

Материально-техническим обеспечением производственной практики служат базовые предприятия и организации, с которыми заключены договоры на места прохождения практик.

1.	ООО «Центр Защиты Информации»
2.	ГАУ КО «КГНИЦ»
3.	АО «Янтарьэнерго»
4.	ООО «Алгоритм»
5.	АО “ЦентрИнформ»
6.	ООО «СКА и К»
7.	ООО «Сократ»
8.	АО «33 судоремонтный завод»
9.	“Elite Games Limited”
10.	ООО «Альпея»
11.	ООО «Е-Легион»
12.	ФГБК «Федеральный центр высоких медицинских технологий» Министерства здравоохранения Российской Федерации
13.	ООО «Хирокрафт»

11. Приложения

Приложение 1

Титульный лист отчета по производственной практике

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

Отчёт
о прохождении производственной практики

Обучающийся _____
(*Ф.И.О. подпись*)

Направление подготовки 10.05.01 Компьютерная безопасность
(*шифр, название*)

Профиль Математические методы защиты информации
(*название*)

Место прохождения практики _____

_____

_____

_____

(*указывается полное наименование структурного подразделения Института / профильной организации и её структурного подразделения, а также их фактический адрес*)

Срок прохождения практики: с « 17 » июня 2019 г. по « 30 » июня 2019 г.

Руководители практики:

Руководитель практики от института:

_____
(*Ф.И.О., должность, подпись*)

Руководитель практики от организации:

_____
(*Ф.И.О., должность, подпись*)

Отчет подготовлен _____ _____
(*подпись обучающегося*) (*И.О. Фамилия*)

Калининград, 2019

СТРУКТУРА ОТЧЕТА ПО ПРАКТИКЕ

Титульный лист
Оглавление
ВВЕДЕНИЕ
Во введении ставятся цель и задачи прохождения практики, обозначается место ее прохождения, а также раскрывается суть деятельности обучающегося во время практики. Обязательно указывается, что был пройден инструктаж по технике безопасности и прочие виды инструктажа, предусмотренные программой практики.

ОСНОВНАЯ ЧАСТЬ
В основной части содержится перечень информации, предусмотренный Программой соответствующей практики и обозначенный в индивидуальном задании.

ЗАКЛЮЧЕНИЕ
В заключении формулируются основные результаты проделанной работе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ
Список использованных источников может содержать перечень нормативных правовых источников, учебных, научных и периодических изданий, используемых обучающимся для выполнения программы практики.

ПРИЛОЖЕНИЯ К ОТЧЕТУ ПО ПРАКТИКЕ:

Приложение 1 – Индивидуальное задание руководителя практики
Приложение 2 – Рабочий план-график проведения практики
Приложение 3 – Отзыв руководителя практики от организации
Приложение 4 – Дневник о прохождении практики
Приложение 5 – Дополнительная информация

В приложение 5 *могут включаться копии документов* (*нормативных актов, отчетов и др.*), *изученных и использованных обучающимся в период прохождения практики, могут быть отражены и указаны реальные процессы, происходящие на предприятии* (*в организации*) *и дополняющие изложенный в Отчете материал* (*например, копии заполненных документов, расчетные материалы и другие материалы*).

Приложение 2

Форма дневника прохождения производственной практики

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

ДНЕВНИК

прохождения производственной практики

Обучающийся _____
(*Ф.И.О. подпись*)

Направление подготовки 10.05.01 Компьютерная безопасность
(*шифр, название*)

Профиль Математические методы защиты информации
(*название*)

Место прохождения практики _____

_____

Срок прохождения практики: с « 17 » июня 2019 г. по « 30 » июня 2019 г.

Руководитель от ИФМНиИТ _____ «___»_____ 2019 г.
(*Ф.И.О. подпись*)

Руководитель практики от организации _____ «___»_____ 2019 г.
(*Ф.И.О. подпись*)

Калининград, 2019

Дневник

День	Дата	Содержание выполненного задания	Применяемое оборудование, литература (с указанием прорабатываемой темы) инструмент, материалы, и пр.	Отметка руководителя о качестве выполненного задания	Подпись руководителя практики от предприятия
1		Инструктаж по технике безопасности, пожарной безопасности, ознакомление с правилами внутреннего трудового распорядка и с требованиями охраны труда.			
2		Ознакомление с индивидуальным заданием на производственную практику.			
3					
4					
5					
6					
7					

Обучающийся _____ _____ «___»_____ 2019 г.
(*Ф.И.О. подпись*)

_____ _____ _____
(*Должность руководителя практики от профильной организации)* (*подпись*) (*И.О. Фамилия*)

«___»_____ 2019 г.

М.П.

Приложение 3

Форма индивидуального задания на производственную практику

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на производственную практику (практику по получению профессиональных умений и опыта профессиональной деятельности)

для _____

(*ФИО обучающегося полностью*)

Обучающегося ____ курса

Направление подготовки 10.05.01 Компьютерная безопасность

Профиль Математические методы защиты информации

Место прохождения практики _____

_____

_____

Адрес организации: _____

(*указывается полное наименование структурного подразделения Института / профильной организации и ее структурного подразделения, а также их фактический адрес*)

Срок прохождения практики: с « 17 » июня 2019 г. по « 30 » июня 2019 г.

Цель прохождения практики:

- закрепление и углубление знаний, умений, навыков и компетенций, полученных обучающимися в процессе аудиторных занятий;
- изучение опыта работы в сфере деятельности, соответствующей направлению 10.05.01 «Компьютерная безопасность»;
- изучение конкретных методов и методик анализа проблем обеспечения информационной / компьютерной безопасности на предприятии / в организации, методов и средств и решения.

Задачи практики:

Изучить:

- административную и информационную структуру предприятия;
- основные нормативно-правовые положения в области информационной безопасности и защиты информации;
- должностные инструкции сотрудников организации, отвечающих за безопасность;
- применяемые технические и программные средства вычислительной техники;

- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации;
- потенциальные каналы утечки информации, способы их выявления и методы оценки опасности;
- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- принципы построения современных криптографических систем, стандарты в области криптографической защиты информации;
- передовой опыт лучших специалистов подразделения;
- менеджмент в области программно-аппаратных и технических средств защиты информации.

Исследовать:
- методы организации и управления деятельности служб защиты информации на предприятии;
- технологию проектирования, построения и эксплуатации систем компьютерной безопасности;
- методы анализа уязвимости и защищенности информационных процессов;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- методы и схемы управления информационной безопасностью;
- методы оценки экономической эффективности применения программно-аппаратных и технических средств защиты информации.

Содержание практики, вопросы, подлежащие изучению:
- На основе стандартов в области информационной безопасности, нормативных документов и с помощью программно-аппаратных средств контроля вторжений произвести анализ и оценку уровня информационной защищённости предприятия или его компьютерной системы.
- Разработать модификацию системы информационной безопасности предприятия или его компьютерной системы или адаптировать существующую для обеспечения требуемого уровня безопасности.
- Разработать необходимое программное обеспечение для модифицированной системы информационной безопасности предприятия или его компьютерной системы.
- Осуществить сбор и первичную обработку материала для подготовки к написанию курсовой работы и / или выпускной квалификационной работы.

Планируемые результаты практики:
- Подготовка рекомендаций по совершенствованию системы информационной безопасности предприятия или его компьютерной системы (рекомендации должны быть

обоснованными, т.е. сопровождаться ссылками на соответствующие нормативно-правовые документы в области информационной безопасности или авторитетное мнение специалистов по безопасности).

- подготовка общих выводов о состоянии системы информационной безопасности предприятия или его компьютерной системы предприятия или организации, а также практических рекомендаций по совершенствованию правовых, организационных, компьютерных и технических составляющих системы;
- Систематизация и обобщение материала для написания курсовой и / или выпускной квалификационной работы.

СОГЛАСОВАНО

_____

Руководитель практики от профильной организации

«___» _____2019 г.

УТВЕРЖДАЮ

_____

Руководитель практики от Института

«____» _____2019 г.

Задание принято к исполнению: _____ «___» _____2019 г.

(*подпись обучающегося*)

Приложение 4

Форма рабочего плана-графика

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

СОГЛАСОВАНО

_____

_____

(*И.О. Фамилия руководителя практики от профильной организации*)

«___»_____ 2019 *г.*

УТВЕРЖДАЮ

_____

_____

(*И.О. Фамилия руководителя практики от Института*)

«___»_____ 2019 г.

РАБОЧИЙ ПЛАН-ГРАФИК
проведения производственной практики (Практики по получению профессиональных умений и опыта профессиональной деятельности)

для _____

(*ФИО обучающегося полностью*)

Обучающегося ___ курса

Направление подготовки 10.05.01 Компьютерная безопасность

Профиль Математические методы защиты информации

№ п/п	Этапы (периоды) практики НИР	Вид работ	Срок прохождения этапа (периода) практики	Форма отчетности
1	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 (программа практики и дневник практики с направлением на практику) в сроки, опреде-		Письменный отчёт. Индивидуальное задание на практику.

№ п/п	Этапы (периоды) практики НИР	Вид работ	Срок прохождения этапа (периода) практики	Форма отчетности
		ленные программой; 8. Изучение правовых основ, базовых нормативных и локальных правовых актов, регулирующих деятельность базы практики		
2	Основной этап	1. Ознакомление с конкретными видами деятельности в соответствии с положениями структурных подразделений и должностными инструкциями 2. Ознакомление с задачами отдела/службы организации базы практики; 3. Выполнение заданий, поставленных руководителями практики; 4. Выполнение программы практики, индивидуального задания на практику; 5. Сбор информации и материалов практики 6. Обработка, систематизация и анализ фактического и теоретического материала. 7. Введение дневника практики		Письменный отчет. Дневник практики
3	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, представление отчета по практике и прилагаемых документов в Институт для защиты.		Зачет с оценкой.

Место прохождения практики: _____

_____

_____

адрес организации:

_____

(*указывается полное наименование структурного подразделения БФУ им. И. Канта или профильной организации и её структурного подразделения, а также их фактический адрес*)

Срок прохождения практики: с « 17 » июня 2019 г. по « 30 » июня 2019 г.

Обучающийся _____

(*Ф.И.О.*)

Приложение 5

Рекомендации по техническому оформлению отчета о результатах прохождения производственной практики

Оформление отчета о результатах прохождения производственной практики необходимо выполнять в соответствии со следующими правилами.

Объем работы: до 25 страниц формата А4 (210 х 297), но не менее 10 страниц, набранных через полтора интервала на одной стороне листа белой бумаги в текстовом процессоре Word, 2/3 из которых должна занимать практическая часть. Допускается представлять иллюстрации и таблицы на листах формата А3.

Поля: левое - 3 см, правое – 1,5 см, верхнее – 2 см, нижнее – 2 см.

Шрифт: TimesNewRoman, размер шрифта – 14 пунктов.

Титульный лист оформляется по образцу.

Все страницы отчета, включая иллюстрации и приложения, нумеруются по порядку от титульного листа до последней страницы без пропусков и повторений.

Первой страницей является титульный лист, оформленный в соответствующем порядке, номер страницы на нем не ставится. Далее, после титульного листа, вшивается чистый лист для написания рецензии, который не нумеруется. После вшивается план работы, подписанный руководителем производственной практики, который не нумеруется. Затем вшивается содержание работы, совпадающее с утвержденным планом, номер страницы на нем не ставится. Элементы: введение, заключение, список использованной литературы, приложение в содержании и плане не нумеруются.

Далее вшивается первый лист введения, номер страницы на нем не ставится. На последующих страницах порядковый номер печатается в правом верхнем углу без точки в конце, начиная с четвертой страницы, которая является второй страницей введения.

Заголовки основных и дополнительных разделов отчета следует располагать на расстоянии не менее трех интервалов от текста в середине строки без точки в конце и печатать жирным шрифтом, прописными буквами, не подчеркивая.

Заголовки подразделов и пунктов следует начинать с абзацного отступа и печатать жирным шрифтом с прописной буквы, не подчеркивая, без точки в конце.

Если заголовок включает несколько предложений, их разделяют точками. Переносы слов в заголовках не допускаются.

Иллюстрации должны иметь названия. Иллюстрации обозначаются словом "Рисунок", которое помещают под иллюстрацией, и нумеруются последовательно арабскими цифрами в пределах всего отчета. Иллюстрации и таблицы, расположенные на отдельных листах, включают в общую нумерацию страниц. На все иллюстрации должны быть ссылки в отчете.

Таблицы нумеруют последовательно арабскими цифрами в пределах всей работы. В левом верхнем углу таблицы помещают слово "Таблица" с указанием номера этой таблицы и соответствующим заголовком. На все таблицы должны быть ссылки в отчете.

Если в работе одна таблица, ее не нумеруют и слово "Таблица" не пишут.

Таблицу размещают непосредственно после первого упоминания о ней в тексте на этой же или следующей странице таким образом, чтобы читать ее можно было без поворота или с

поворотом по часовой стрелке. Ссылка на таблицу по ходу текста выполняется так: "в таблице 2 приводятся данные о ... ".

Примечания к таблицам, иллюстрациям или пунктам и подпунктам текста размещают непосредственно после пункта, подпункта, таблицы, иллюстрации, к которым они относятся, и печатают с прописной буквы с абзацного отступа. Слово "Примечание" следует печатать с абзацного отступа жирным шрифтом.

Ссылки на разделы, подразделы, пункты, подпункты, иллюстрации, таблицы, формулы, уравнения, перечисления, приложения, следуют указывать порядковым номером, например: "... в разделе 4", "... по пункту 3.3.4", "... в подпункте 2.3.41, перечисление 3", "...по формуле (3)", "... в уравнении (2)",-"... на рисунке 8", "... в приложении 6".

Формулы могут быть вписаны в текст от руки тщательно и разборчиво или напечатаны на компьютере. Не разрешается одну часть формулы вписывать от руки, а другую впечатывать. Выше и ниже каждой формулы должно быть оставлено не менее одной свободной строки. Размеры знаков для формулы рекомендуются следующие: прописные буквы и цифры – 7-8 мм, строчные – 4 мм, показатели степени и индексы – не менее 2 мм.

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой даны в формуле. Значение каждого символа и числового коэффициента следует давать с новой строки. Первую строку пояснения начинают со слова "где" без двоеточия.

Формулы в работе следует нумеровать порядковой нумерацией в пределах всего отчета арабскими цифрами в круглых скобках в крайнем правом положении на строке. Если в отчете только одна формула или уравнение, их не нумеруют.

Отчет о результатах прохождения производственной практики вшивается в папку-скоросшиватель с прозрачной верхней обложкой.

Приложение 6

Форма отзыва руководителя практики от организации

ОТЗЫВ
о работе обучающегося в период прохождения практики

Обучающийся _____
(Ф.И.О.)
Института физико-математических наук и информационных технологий проходил производственную практику по получению профессиональных умений и опыта профессиональной деятельности _____
(вид и тип практики)
в период с с « 17 » июня 2019 г. по « 30 » июня 2019 г.
в _____
(*наименование профильной организации с указанием структурного подразделения*)
в качестве _____
(*должность*)

На время прохождения практики _____
(*Фамилия, И.О. обучающегося*)
поручалось решение следующих задач: _____
_____

За время прохождения практики обучающийся проявил _____
_____
_____
_____
_____
(*навыки, активность, дисциплина, помощь организации, качество и достаточность собранного материала для отчета и выполненных работ, поощрения и т.п.*)

Результаты работы обучающегося:
_____
_____
_____
_____
(*Индивидуальное задание выполнено, решения по порученным задачам предложены, материал собран полностью, иное*.)

Считаю, что по итогам практики обучающийся может (не может) быть допущен к защите отчета по практике.

_____ _____ _____
(*Должность руководителя практики от профильной организации)* (*подпись*) (*И.О. Фамилия*)

«____»_____2019 г.

М.П.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. Иммануила Канта

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ Е.П.Ставицкая
«20» марта 2020 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«___» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕНОЙ ПРАКТИКИ

(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*

Калининград
2020 г.

Лист согласования

Составитель: к.т.н., доцент Института физико-математических наук и информационных технологий АЛЕШНИКОВ СЕРГЕЙ ИВАНОВИЧ.

Рабочая программа обсуждена и утверждена на заседании Учебно-методического совета ИФМНиИТ
Протокол №____от «____»_____ 201_ г.

Председатель Совета _____ доцент, к.ф.-м. н. А.А.Шпилевой
Менеджер ООП _____ Е.П. Новикова

Рабочая программа пересмотрена на заседании Учебно-методического совета ИФМНиИТ

Внесены следующие изменения (или изменений не внесено):

1. _____
2. _____
3. _____

Протокол №____от «____»_____ 20__ г.

Председатель Совета _____ доцент, к.ф.-м. н. А.А.Шпилевой
Менеджер ООП _____ (Е.П. Новикова)

СОДЕРЖАНИЕ

1. Способ и формы проведения научно-исследовательской работы

Вид практики: Производственная практика (научно-исследовательская работа) (далее **научно-исследовательская работа** или **НИР**).

НИР проводится в следующих **формах**:

- непрерывная – в период учебного времени для проведения НИР, указанного в календарном учебном графике.

Способы проведения НИР:

- стационарная на рабочем месте. Включает в себя самостоятельную работу студентов.

Итогом НИР является представление отчета по НИР об основных результатах проведенной научно-исследовательской работы.

2. Перечень планируемых результатов обучения при выполнении НИР

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.

В результате освоения ООП обучающийся должен овладеть следующими результатами обучения при выполнении НИР:

Код компетенции	**Результаты освоения ООП Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ОК-8	Способность к самоорганизации и самообразованию	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать*:** - правила и нормы здорового образа жизни; - основную профессиональную литературу и Интернет-ресурсы в области компьютерной безопасности и смежных областях, способные

		служить для самообразования; ***уметь*:** - ставить достижимые цели саморазвития и самообразования; - рационально планировать свою деятельность в течения дня, недели, месяца, года, соотнося цели с возможностями; - пользоваться электронными устройствами для доступа к Интернет-ресурсам и электронным библиотекам, для чтения литературы; ***владеть:*** - навыками организации жизни в соответствии с принятыми личными планами; - навыками систематического чтения профессиональной литературы согласно плану самообразования.
ОК-9	Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать*:** - факторы здорового образа жизни; - методы оценки физического развития, телосложения, двигательной и функциональной подготовленности средствами физической культуры и спорта в студенческом возрасте; ***уметь*:** - использовать средства физической культуры в регулировании своего психофизиологического состояния методами психофизической тренировки; - воспроизводить основные двигательные действия и использовать их в своей профессиональной деятельности; ***владеть*:** - основными двигательными действиями в избранном виде спорта, а также методами тренировки в избранном виде двигательной активности; - навыками оптимизации своего физического состояния в условиях профессиональной деятельности;
ОПК-1	Способность анализировать физические явления и процессы при решении профессиональных задач	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать*:** - основные физические законы и их приложения в профессиональной сфере; - основные математические модели информационных процессов в компьютерных системах и методы их исследования; - основные математические модели структур, возникающие при описании компьютерных систем; - методы алгебры, теории чисел, математического анализа, теории вероятностей и математической статистики для исследования математических моделей процессов и структур в компьютерных системах; ***уметь*:** - математически формализовать задачи физического и информационного характера, возникающие при моделировании компьютерных систем; - подбирать подходящие методы из различных областей математики для исследования свойств построенных математических моделей и решения поставленных математических задач; - проводить компьютерные эксперименты с целью моделирования физических явлений и процессов; ***владеть:*** - профессиональным математическим языком для описания физиче-

		ских явлений и процессов; - навыками построения математических моделей и исследования их свойств, методами решения математических задач.
ОПК-4	Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать*:** - основные этапы научного исследования и методологию реализации этапов; - научную и инженерную проблематику в области компьютерной безопасности; - взаимосвязи между различными аспектами моделирования компьютерных систем – математическими, информационными, техническими, организационно-правовыми; ***уметь*:** - корректно формулировать научные задачи в области компьютерной безопасности; - разрабатывать комплексные (междисциплинарные и инновационные) проекты создания и исследования компьютерных систем и их подсистем; - интегрировать отдельные задачи в рамках комплексного проекта; - анализировать и оптимизировать информационные потоки в рамках комплексного проекта; ***владеть:*** - навыками реализации комплексных проектов в области компьютерной безопасности; - навыками разработки проектной и технической документации; - навыками представления проектов в форме презентаций.
ОПК-10	Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать*:** - 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; ***уметь*:** - 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; ***владеть:*** - 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.
ПК-1	Способность осуществлять подбор,	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен:

	изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности	***знать*:** - основные источники печатной информации в области компьютерной безопасности: научные и научно-технические журналы, библиотеки, архивы; - основные электронные источники, российские и зарубежные, в области компьютерной безопасности: Интернет-ресурсы, электронные библиотеки, базы данных, Интернет-форумы, профессиональные сайты; - правила оформления списков и обзоров литературы; ***уметь*:** - осуществлять поиск информации в печатных изданиях; - пользоваться поисковыми системами и осуществлять поиск информации в электронных источниках; - сортировать и классифицировать найденную информацию, составлять списки и обзоры литературы; ***владеть:*** - навыками поиска, анализа и составления списков источников и обзоров литературы в области компьютерной безопасности.
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.	В ходе защиты выпускной квалификационной работы студент должен: • ***знать*:** технические нормативы и правовые нормы обеспечения информационной безопасности; сертифицированные технические, программные и аппаратные средства определения уровней защищённости компьютерных систем; порядок и процедуру проведения экспериментальных научных исследований по оценке информационной безопасности в компьютерных системах; формы отчётности по результатам исследований; • ***уметь*:** пользоваться сертифицированными техническими, программными и аппаратными средствами определения уровней защищённости компьютерных систем; проводить замеры параметров, определяющих информационную безопасность; уметь составлять отчёты по результатам замеров параметров; • ***владеть*:** методикой планирования и практическими навыками проведения экспериментальных научно-исследовательских работ по оценке защищённости компьютерных систем; навыками использования сертифицированных технических, программных и аппаратных средств определения уровней защищённости.
ПК-7	Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** основные методы и средства обеспечения информационной безопасности компьютерных систем; типовые проектные решения по обеспечению информационной безопасности компьютерных систем; стандарты по информационной защищённости компьютерных систем; • ***уметь*:** строить и анализировать математические модели безопасности компьютерных систем; ориентироваться в нормативно-правовой базе по информационной безопасности; интегрировать показатели информационной защищённости компьютерной системы в единый комплекс; • ***владеть*:** методикой анализа и оценки уровней информационной защищённости компьютерных систем; практическими навыками разработки нормативной и технической документации по проектированию, разработке и управлению системами безопасности компьютерных систем.

ПСК-2.3	Способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать:*** - типовые алгоритмы преобразования информации в компьютерных системах и оценки их эффективности; - перспективные методы и алгоритмы преобразования информации в компьютерных системах и методику оценки их эффективности; - российские и иностранные стандарты безопасности компьютерных систем; ***уметь:*** - строить математические модели информационных процессов в компьютерных системах и алгоритмизировать вычислительные процедуры в этих моделях; - поводить аналитическую работу по сравнительной оценке эффективности применения различных математических моделей; - оценивать быстродействие и объём необходимой памяти для заданного алгоритма; ***владеть:*** - навыками построения математических моделей информационных процессов в компьютерных системах и навыками их алгоритмизации; - методикой анализа эффективности алгоритмов.
ПСК-2.4	Способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен: ***знать*:** - 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 методы обработки информации в компьютерных системах; - методы алгебры, теории чисел, алгебраической геометрии и дискретной математики и их применение в моделях информационных процессов; ***уметь*:** - строить математические модели информационных процессов, возникающих при работе программно-аппаратных средств; - проводить анализ адекватности существующих математических моделей на основе сравнения их показателей эффективности с перспективными моделями; - проводить анализ адекватности существующих математических моделей на основе компьютерного моделирования и получения статистических оценок эффективности; ***владеть*:** - методикой разработки математических моделей информационных процессов в компьютерных системах, используя методы алгебры, теории чисел, алгебраической геометрии и дискретной математики; - навыками оценки адекватности моделей информационных процессов в программно-аппаратных средствах.

3. Место НИР в структуре ООП

Научно-исследовательская работа относится к базовой части блока 2 «Практики, в том числе научно-исследовательская работа (НИР)» ООП подготовки специалистов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

Логическая и содержательная связь дисциплин и практик, участвующих в формировании представленных в п.2 компетенций, содержится в ниже представленной таблице:

Компетенция	Предшествующие дисциплины	Данная дисциплина	Последующие дисциплины
ОК-8	− Иностранный язык.	Производственная практика (научно-исследовательская работа)	− Процедура защиты ВКР.
ОК-9	− Физическая культура и спорт. − Элективные курсы по физической культуре и спорту.		− Подготовка к процедуре защиты выпускной квалификационной работы.
ОПК-1	− Физика. − Техническая защита информации. − Электроника и схемотехника. − Основы технической физики		− Подготовка к процедуре защиты выпускной квалификационной работы.
ОПК-4	− Философия. − Дискретная математика. − Математическая логика и теория алгоритмов. − Теория информации. − Методы алгебраической геометрии в криптографии. − Методы и алгоритмы генерации гиперэллиптических кривых для криптографии. − Теория чисел. − Теория автоматов. − Формальные языки.		− Подготовка к процедуре защиты выпускной квалификационной работы.
ОПК-10	− Алгебра. − Информатика. − Математическая логика и теория алгоритмов. − Быстрые мультипликаторы. − Криптографические методы защиты информации. − Криптографические протоколы. − Методы алгебраической геометрии в криптографии. − Системы компьютерной алгебры и реализация криптографических алгоритмов. − Аналитические методы в задачах защиты информации. − Прикладная алгебра. − Вычислительная алгебра. − Учебная практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности.		− Подготовка к процедуре защиты выпускной квалификационной работы.
ПК-1	− Основы информационной безопасности. − Теоретико-числовые методы в криптографии. − Криптографические методы защиты информации.		− Подготовка к процедуре защиты выпускной квалификационной работы. − Процедура защиты вы-

	− Введение в специальность. − Основы технической физики. − Квантовая защита и обработка информации. − Прикладная алгебра. − Вычислительная алгебра.		пускной квалификационной работы.
ПК-2	− Защита данных в государственных информационных системах − Модуль 6. Дискретная математика − Теория псевдослучайных генераторов − Модуль 7. Компьютерные технологии − Системы управления базами данных − Модуль 12. Техническая защита информации − Техническая защита информации − Модуль 14. Криптография − Криптографические методы защиты информации − Криптографические протоколы − Модуль 15. Программно-аппаратные средства обеспечения информационной безопасности − Основы построения защищенных компьютерных сетей − Защита программ и данных − Защита в операционных системах − Основы построения защищенных баз данных − Модуль 4. Фундаментальная математика − История криптографии − Внешний аудит безопасности корпоративных сетей − Системы тестового вторжения		− Процедура защиты выпускной квалификационной работы
ПК-7	− Модуль 5. Теория чисел и прикладная алгебра − Основы информационной безопасности − Модуль 11. Дополнительные разделы дискретной математики − Теория кодирования, сжатия и восстановления информации − Модуль 13. Теоретико-числовые методы криптографии − Теоретико-числовые методы в криптографии − Модуль 14. Криптография − Криптографические протоколы − Модуль 18. Криптография на алгебраических кривых − Модуль 5. Теория чисел и прикладная алгебра − Теория чисел − Программирование микроконтроллеров − Технология инфраструктуры открытых ключей − Методы и алгоритмы генерации эллиптических кривых для криптографии − Спаривание на эллиптических кривых		− Подготовка к процедуре защиты выпускной квалификационной работы
ПСК-2.3	− Теория псевдослучайных генераторов. − Теория кодирования, сжатия и восстановления информации. − Модели безопасности компьютерных систем.		− Подготовка к процедуре защиты выпускной квалификационной работы.

	− Криптографические методы защиты информации. − Методы алгебраической геометрии в криптографии. − Криптографические протоколы для защиты банковской информации. − Анализ стойкости финансовых протоколов. − Компьютерный практикум по методам вычисления дискретного логарифма. − Технология инфраструктуры открытых ключей.		
ПСК-2.4	− Теория псевдослучайных генераторов. − Компьютерный практикум по криптографии на эллиптических кривых. − Компьютерный практикум по криптографии на гиперэллиптических кривых. − Системы компьютерной алгебры и реализация криптографических алгоритмов. − Методы алгебраической теории чисел в криптографии. − Компьютерный практикум по методам вычисления дискретного логарифма. − Технология инфраструктуры открытых ключей.		− Подготовка к процедуре защиты выпускной квалификационной работы.

4. <u>Объем НИР в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся</u>

Научно-исследовательская работа для обучающихся по специальности 10.05.01 – «Компьютерная безопасность», специализация: «Математические методы защиты информации» проводится в 11 семестре в течение 4 недель, трудоемкость НИР – 6 зачетных единиц, 216 академических часов.

Объём НИР	**Всего часов**	
	Контактные часы	**Самостоятельная работа**
Контактная работа обучающихся с преподавателем (самостоятельная работа студента под руководством преподавателя).	2,0	
Самостоятельная работа обучающихся		212
Промежуточная аттестация – зачет с оценкой	0,5	1,5
Итого:	2,5	213,5
Общая трудоемкость НИР	216 часов (6 ЗЕ)	

5. <u>Содержание НИР</u>

Студенты выполняют программу НИР в соответствии с индивидуальным планом проведения НИР, утверждаемым руководителем НИР.

Ведется дневник НИР и составляется заключительный отчет, который защищается после окончания практики и утверждается руководителем НИР.

Студентам должна быть предоставлена возможность ознакомиться с научно-технической документацией и научной литературой, которая касается предмета его исследований. В процессе выполнения НИР студенты прослушивают лекции ведущих специалистов, участвуют в научно-технических семинарах и конференциях при их наличии.

Студенты проходят НИР в лабораториях Института физико-математических наук и информационных технологий, относящихся к специальности «Компьютерная безопасность» и компьютерных классах. Они должны иметь доступ к программно-техническим комплексам, программным комплексам, математическому обеспечению и техническим средствам, необходимым для исследований, иметь возможность непосредственных консультаций во время проведения НИР с руководителями ВКР.

В результате выполнения НИР студент готовит материалы для написания ВКР в рамках ее предполагаемой тематики и в соответствии со специализацией «Математические методы защиты информации».

При проведении НИР студенты **изучают**:

- научную литературу по теме ВКР (монографии, статьи, патентные материалы, научные отчёты, техническую документацию, авторефераты и диссертации);
- современную технологию анализа потенциальных каналов утечки информации;
- структуру и методы построения современных моделей безопасности компьютерных систем;
- современную технологию защиты информации в компьютерных системах;
- современную технологию противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- математические модели и алгоритмы, используемые в современных криптографических системах и системах помехоустойчивого кодирования.

При проведении НИР студенты разрабатывают и **исследуют**:

- алгоритмы быстрых вычислений в алгебраических структурах, их компьютерную реализацию;
- системы и алгоритмы помехоустойчивого кодирования информации, их свойства, оценки эффективности и их компьютерные модели;
- системы и алгоритмы шифрования информации, их свойства, оценки эффективности и их компьютерные модели;
- математические методы, модели и алгоритмы, используемые при разработке инфраструктуры современных криптосистем с открытым ключом, и их компьютерные модели;
- математические и компьютерные модели псевдослучайных генераторов, их свойства и методы статистического тестирования;
- структуру, принципы функционирования и управления современными системами защиты информации в компьютерных системах;

При выполнении НИР возможен следующий перечень **индивидуальных заданий**:

- Разработка методик анализа и оценки уровней защищённости компьютерных систем.

- Проектирование защищённых компьютерных систем, в частности систем автоматизированной обработки персональных данных.
- Разработка систем защиты информации и систем управления информационной безопасностью, основанных на новых логических и математических принципах;
- Разработка методов контроля эффективности защиты информации, основанных на новых математических моделях и методах;
- Анализ эффективности, модификация и построение криптографических алгоритмов, основанных на новых математических принципах.
- Разработка и анализ систем помехоустойчивого кодирования на алгебраических кривых над конечными полями с большим числом точек.
- Проектирование и статистический анализ качества потоковых шифров и генераторов псевдослучайных чисел.
- Компьютерное моделирование эффективных алгоритмов: вычислительных, криптографических, кодирования, сжатия и восстановления информации при её передаче и хранении.
- Анализ и разработка криптографической инфраструктуры для конкретных систем защиты информации; алгоритмическое обеспечение инфраструктуры.
- Анализ стойкости и разработка схем и защищённых протоколов обмена информацией в компьютерных системах и сетях общего назначения.
- Анализ стойкости и разработка защищённых протоколов обмена информацией в специализированных компьютерных системах и сетях: банковских, корпоративных, системах электронного голосования и т.д.

Задание на НИР определяется вместе со студентом руководителями НИР в начале работы. В конце выполнения НИР студент должен представить результаты НИР в виде отчета и сдать его руководителю от института. Руководитель НИР организует защиту отчетов, по результатам которой на основании решения комиссии выставляется промежуточный контроль в виде зачета с оценкой.

Кроме того, при прохождении НИР в лабораториях и компьютерных классах студент обязан:

- пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка, принятого в лабораториях ИФМНиИТ;
- посещать все мероприятия научного характера по теме НИР, проводимые в ИФМНиИТ;
- подчиняться действующим в лабораториях правилам внутреннего трудового распорядка;
- изучить и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии.

Особое внимание следует уделить анализу возможности публичного представления результатов НИР, возможности внедрения результатов исследования в проектную деятельность, инженерную практику и в производство.

Краткий план-график НИР

№ п/п	Этапы (периоды) НИР	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
1	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.	12	Письменный отчёт. Индивидуальное задание на НИР.
2	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.	180	Письменный отчет. Дневник НИР
3	Заключительный этап	1. Подготовка отчета о НИР, представления отчета по НИР и прилагаемых документов для защиты.	24	Зачет с оценкой.

№ п/п	Этапы (периоды) НИР	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
	Итого часов		**216**	

6. Формы отчетности по НИР

Формы отчетности студентов по НИР:

- задание на НИР, заверенное подписями руководителя НИР и руководителя ВКР;
- индивидуальный план НИР, заверенный подписями руководителя НИР и руководителя ВКР;
- дневник НИР, заверенный подписью руководителя НИР.
- отчет по научно-исследовательской работе, заверенный подписями руководителя НИР и руководителя ВКР.

Формы отчетности руководителей НИР:

- не позднее 1 месяца после окончания НИР предоставляет в институт отчет о проведенной НИР;
- предоставляет Отзыв о научно-исследовательской работе каждого студента, заверенный также подписью руководителя ВКР.

Оформление результатов НИР

По окончании НИР студент обязан составить письменный отчет и сдать его руководителю НИР. Отчет по НИР должен содержать сведения о конкретной выполненной студентом запланированной работе в период прохождения НИР. В отчет по НИР входит также краткое описание результатов, полученных студентом по теме ВКР.

Для оформления отчета студенту выделяется в конце периода НИР 3 дня.

Требования, предъявляемые к оформлению отчета по НИР

Отчет по НИР должен состоять из Оглавления, Введения, описания Основной части, Заключения, Списка использованной литературы.

Описание основной части отчета по НИР должно содержать

- задание на НИР, полученное от руководителей НИР и ВКР;
- описание процесса выполнения студентом запланированной работы.

Рекомендуемый объем отчета не менее 15 страниц. Образец титульного листа прилагается (Приложение 1). Переплет отчета может быть произвольным и исключать рассыпание листов. Оформление отчета – см. Приложение 5.

Представленный студентом отчет рецензируется руководителями НИР и ВКР. В случае положительной рецензии он выносится на защиту.

Защита отчета осуществляется перед комиссией, которая состоит из руководителя НИР и сотрудников ИФМНиИТ.

Порядок аттестации студентов по результатам НИР

По окончании НИР проводится ***дифференцированный зачет.*** При проведении зачета используются следующие критерии итоговой оценки за НИР:

- грамотный обзор и анализ литературы по теме исследования;
- наличие постановок конкретных задач исследования;
- наличие планов и результатов предварительного компьютерного моделирования, результаты статистического анализа его итогов;
- ясное и логичное описание рабочих гипотез, структурных схем, математических моделей, протоколов обмена информацией, вычислительных алгоритмов;
- обоснованные результаты исследования и анализа свойств математических моделей;
- обоснованные результаты анализа эффективности разработанных алгоритмов;
- достаточно полное описание разработанного комплекса программ;
- наличие планов и результатов компьютерного моделирования в соответствии с разработанными моделями и алгоритмами, результаты анализа адекватности разработанных математических моделей, корректности алгоритмов, работоспособности комплекса программ;
- правильные ответы студента на вопросы преподавателя, касающиеся предмета НИР.

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

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках НИР

Компетенция	**Этапы формирования компетенции**	**Показатели оценивания компетенции**	**Критерии оценивания компетенций**	**Шкала оценивания**	**Виды аттестации и виды оценочных средств**
ОК-8 Способность к самоорганизации и самообразованию	Начальный этап	***знать*:** правила и нормы здорового образа жизни; основную профессиональную литературу и Интернет-ресурсы в области компьютерной безопасности и смежных областях, спо-	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание правил и норм здорового образа жизни, подтверждаемых хорошей физической формой; хорошее знание профессиональной литературы и Интернет-ресурсов в области компьютерной безопасности и смежных областях, способных служить для самообразования Умение ставить достижимые цели саморазвития и самообразования; рационально планировать	от 85% до 100%	Отчет по НИР, Отзыв руководителя НИР Дифференцированный зачет

		собные служить для самообразования; ***уметь*:** ставить достижимые цели саморазвития и самообразования; рационально планировать свою деятельность в течения дня, недели, месяца, года, соотнося цели с возможностями; пользоваться электронными устройствами для доступа к Интернет-ресурсам и электронным библиотекам, для чтения литературы; ***владеть*:** навыками организации жизни в соответствии с принятыми личными планами; навыками систематического чтения профессиональной литературы согласно плану самообразования.	свою деятельность в течения дня, недели, месяца, года, соотнося цели с возможностями; пользоваться электронными устройствами для доступа к Интернет-ресурсам и электронным библиотекам, для чтения литературы. Владение практическими навыками организации жизни в соответствии с принятыми личными планами; навыками систематического чтения профессиональной литературы согласно плану самообразования.		
			Обучающийся ***на высоком уровне*** демонстрирует: Знание правил и норм здорового образа жизни, знание основной профессиональной литературы и Интернет-ресурсов в области компьютерной безопасности и смежных областях, способных служить для самообразования Умение ставить достижимые цели саморазвития и самообразования; рационально планировать свою деятельность в течения дня, недели, месяца, года; пользоваться электронными устройствами для доступа к Интернет-ресурсам и электронным библиотекам, для чтения литературы. Владение основными практическими навыками организации жизни в соответствии с принятыми личными планами; навыками чтения профессиональной литературы согласно плану самообразования.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знакомство с правилами и нормами здорового образа жизни; знакомство с профессиональной литературой и Интернет-ресурсами в области компьютерной безопасности и смежных областях, способных служить для самообразования Умение ставить определённые цели саморазвития и самообразования; планировать свою деятельность в течения дня, недели, месяца, года; пользоваться электронными устройствами для доступа к Интернет-ресурсам и электронным библиотекам, для чтения литературы. Владение некоторыми практическими навыками организации жизни в соответствии с принятыми личными планами.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: Незнание правил и норм здорового образа жизни; незнание профессиональной литературы и Интернет-ресурсов в области компьютерной безопасности и смежных областях, способных служить для самообразования. Неумение ставить достижимые цели саморазвития и самообразования; рационально планировать свою деятельность в течения дня, недели,	< 50%	

			месяца, года; пользоваться электронными устройствами для доступа к Интернет-ресурсам и электронным библиотекам, для чтения литературы. Отсутствие практических навыков организации жизни в соответствии с принятыми личными планами; навыков чтения профессиональной литературы.		
ОК-9 Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	Начальный этап	***знать*:** факторы здорового образа жизни; методы оценки физического развития, телосложения, двигательной и функциональной подготовленности средствами физической культуры и спорта в студенческом возрасте; ***уметь*:** использовать средства физической культуры в регулировании своего психофизиологического состояния методами психофизической тренировки; воспроизводить основные двигательные действия и использовать их в своей профессиональной деятельности; ***владеть*:** основными двигательными действиями в избранном виде спорта, а также методами тренировки в избранном виде двигательной активности; навыками оптимизации своего физического состояния в условиях профессиональной деятельности;	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание факторов здорового образа жизни; методов оценки физического развития, телосложения, двигательной и функциональной подготовленности средствами физической культуры и спорта в студенческом возрасте. Умение использовать средства физической культуры в регулировании своего психофизиологического состояния методами психофизической тренировки; воспроизводить двигательные действия и использовать их в своей профессиональной деятельности. Владение практическими навыками основных двигательных действий в избранном виде спорта, а также методами тренировки в избранном виде двигательной активности; навыками оптимизации своего физического состояния в условиях профессиональной деятельности.	от 85% до 100%	Отчет по НИР, Отзыв руководителя НИР Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных факторов здорового образа жизни; основных методов оценки физического развития, телосложения, двигательной и функциональной подготовленности средствами физической культуры и спорта в студенческом возрасте. Умение использовать некоторые средства физической культуры в регулировании своего психофизиологического состояния методами психофизической тренировки; воспроизводить основные двигательные действия и использовать их в своей профессиональной деятельности. Владение некоторыми практическими навыками ряда двигательных действий в избранном виде спорта, а также некоторыми методами тренировки в избранном виде двигательной активности; некоторыми навыками оптимизации своего физического состояния в условиях профессиональной деятельности.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знание некоторых факторов здорового образа жизни; некоторых методов оценки физического развития, телосложения, двигательной и функциональной подготовленности.	от 50% до 70%	

			Умение использовать отдельные средства физической культуры в регулировании своего психофизиологического состояния методами психофизической тренировки; воспроизводить отдельные двигательные действия и использовать их в своей профессиональной деятельности. Владение отдельными практическими навыками двигательных действий в избранном виде спорта, а также отдельными методами тренировки в избранном виде двигательной активности.		
			Обучающийся ***на низком уровне*** демонстрирует: Незнание факторов здорового образа жизни; методов оценки физического развития, телосложения, двигательной и функциональной подготовленности средствами физической культуры и спорта в студенческом возрасте. Неумение использовать средства физической культуры в регулировании своего психофизиологического состояния методами психофизической тренировки; воспроизводить двигательные действия и использовать их в своей профессиональной деятельности. Отсутствие практических навыков двигательных действий в любом виде спорта, отсутствие тренированности в любом виде двигательной активности; отсутствие навыков оптимизации своего физического состояния в условиях профессиональной деятельности.	< 50%	
ОПК-1 Способность анализировать физические явления и процессы при решении профессиональных задач	Начальный этап	***знать*:** основные физические законы и их приложения в профессиональной сфере; основные математические модели информационных процессов в компьютерных системах и методы их исследования; основные математические модели структур, возникающие при описании компьютерных систем; методы алгебры, теории чисел, математического анализа, теории вероятностей и математической статистики для исследования математических моделей	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание физических законов и их приложений в профессиональной сфере; математических моделей информационных процессов в компьютерных системах и методов их исследования; математических моделей структур, возникающих при описании компьютерных систем; методов алгебры, теории чисел, математического анализа, теории вероятностей и математической статистики для исследования математических моделей процессов и структур в компьютерных системах. Умение математически корректно формализовать задачи физического и информационного характера, возникающие при моделировании компьютерных систем; подбирать подходящие методы из различных областей математики для исследования свойств построенных математических моделей и решения поставленных математических задач; проводить компьютерные эксперименты с целью моделирования физических явлений и процессов. Владение практическими навыками описания на профессиональном языке физических явлений и процессов; навыками построения математиче-	от 85% до 100%	Отчет по НИР, Отзыв руководителя НИР Дифференцированный зачет

		процессов и структур в компьютерных системах; ***уметь*:** математически формализовать задачи физического и информационного характера, возникающие при моделировании компьютерных систем; подбирать подходящие методы из различных областей математики для исследования свойств построенных математических моделей и решения поставленных математических задач; проводить компьютерные эксперименты с целью моделирования физических явлений и процессов; ***владеть:*** профессиональным математическим языком для описания физических явлений и процессов; навыками построения математических моделей и исследования их свойств, методами решения математических задач.	ских моделей и исследования их свойств, методами решения математических задач.		
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных физических законов и их приложений в профессиональной сфере; основных типов математических моделей информационных процессов в компьютерных системах и основных методов их исследования; основных математических моделей структур, возникающих при описании компьютерных систем; основных методов алгебры, теории чисел, математического анализа, теории вероятностей и математической статистики для исследования математических моделей процессов и структур в компьютерных системах. Умение математически формализовать задачи физического и информационного характера, возникающие при моделировании компьютерных систем; использовать указанные методы из различных областей математики для исследования свойств построенных математических моделей и решения поставленных математических задач; проводить компьютерные эксперименты с целью моделирования физических явлений и процессов. Владение некоторыми практическими навыками описания на профессиональном языке физических явлений и процессов; отдельными навыками построения математических моделей и исследования их свойств, некоторыми методами решения математических задач.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знакомство с основными физическими законами и их приложениями в профессиональной сфере; с основными типами математических моделей информационных процессов в компьютерных системах и основными методами их исследования; с основными математическими моделями структур, возникающих при описании компьютерных систем; с основными методами алгебры, теории чисел, математического анализа, теории вероятностей и математической статистики для исследования математических моделей процессов и структур в компьютерных системах. Умение использовать некоторые из указанных методов из различных областей математики для исследования свойств математических моделей и решения поставленных математических задач; проводить ряд компьютерных экспериментов с целью моделирования физических явлений и процессов. Владение отдельными практическими навыками описания на профессиональном языке физиче-	от 50% до 70%	

			ских явлений и процессов; отдельными навыками исследования свойств математических моделей, отдельными методами решения математических задач.		
			Обучающийся ***на низком уровне*** демонстрирует: Незнание физических законов и их приложений в профессиональной сфере; математических моделей информационных процессов в компьютерных системах и методов их исследования; математических моделей структур, возникающих при описании компьютерных систем; методов алгебры, теории чисел, математического анализа, теории вероятностей и математической статистики для исследования математических моделей процессов и структур в компьютерных системах. Неумение использовать указанные методы из различных областей математики для исследования свойств математических моделей и решения поставленных математических задач; неумение проводить компьютерные эксперименты с целью моделирования физических явлений и процессов. Отсутствие практических навыков описания на профессиональном языке физических явлений и процессов; навыков исследования свойств математических моделей, навыков решения математических задач.	< 50%	
ОПК-4 Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Промежуточный этап	***знать*:** основные этапы научного исследования и методологию реализации этапов; научную и инженерную проблематику в области компьютерной безопасности; взаимосвязи между различными аспектами моделирования компьютерных систем – математическими, информационными, техническими, организационно-правовыми; ***уметь*:** корректно формулировать научные задачи в области компьютерной безопасности; разрабатывать комплексные (междисциплинарные и	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание этапов научного исследования и методологии реализации этапов; научной и инженерной проблематики в области компьютерной безопасности; взаимосвязей между различными аспектами моделирования компьютерных систем – математическими, информационными, техническими, организационно-правовыми. Умение корректно формулировать научные задачи в области компьютерной безопасности; разрабатывать комплексные (междисциплинарные и инновационные) проекты создания и исследования компьютерных систем и их подсистем; интегрировать отдельные задачи в рамках комплексного проекта; анализировать и оптимизировать информационные потоки в рамках комплексного проекта. Владение практическими навыками реализации комплексных проектов в области компьютерной безопасности; навыками разработки проектной и технической документации; навыками представления проектов в форме презентаций.	от 85% до 100%	Отчет по НИР, Отзыв руководителя НИР Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных этапов научного исследования и методологии реализации этих этапов; основной	от 70% до 85%	

		инновационные) проекты создания и исследования компьютерных систем и их подсистем; интегрировать отдельные задачи в рамках комплексного проекта; анализировать и оптимизировать информационные потоки в рамках комплексного проекта; ***владеть:*** навыками реализации комплексных проектов в области компьютерной безопасности; навыками разработки проектной и технической документации; навыками представления проектов в форме презентаций.	научной и инженерной проблематики в области компьютерной безопасности; основных взаимосвязей между различными аспектами моделирования компьютерных систем – математическими, информационными, техническими, организационно-правовыми. Умение формулировать типовые научные задачи в области компьютерной безопасности; участвовать в разработке комплексных (междисциплинарных и инновационных) проектов создания и исследования компьютерных систем и их подсистем; интегрировать отдельные задачи в рамках комплексного проекта; анализировать и оптимизировать информационные потоки в рамках комплексного проекта. Владение некоторыми практическими навыками реализации комплексных проектов в области компьютерной безопасности; некоторыми навыками разработки проектной и технической документации; некоторыми навыками представления проектов в форме презентаций.		
			Обучающийся ***на среднем уровне*** демонстрирует: Знание отдельных этапов научного исследования и методологии реализации этих этапов; основной инженерной проблематики в области компьютерной безопасности; отдельных взаимосвязей между различными аспектами моделирования компьютерных систем – математическими, информационными, техническими, организационно-правовыми. Умение участвовать в разработке комплексных (междисциплинарных и инновационных) проектов создания и исследования компьютерных систем и их подсистем; интегрировать отдельные задачи в рамках комплексного проекта; анализировать информационные потоки в рамках комплексного проекта. Владение отдельными практическими навыками реализации комплексных проектов в области компьютерной безопасности; отдельными навыками разработки проектной и технической документации; отдельными навыками представления проектов в форме презентаций.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: Незнание этапов научного исследования и методологии реализации этапов; научной и инженерной проблематики в области компьютерной безопасности; взаимосвязей между различными аспектами моделирования компьютерных систем. Неумение участвовать в разработке комплексных (междисциплинарных и инновационных) проектов создания и исследования компьютерных си-	< 50%	

			стем и их подсистем; неумение интегрировать отдельные задачи в рамках комплексного проекта; анализировать и оптимизировать информационные потоки в рамках комплексного проекта. Отсутствие практических навыков реализации комплексных проектов в области компьютерной безопасности; навыков разработки проектной и технической документации; навыков представления проектов в форме презентаций.		
ОПК-10 Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Промежуточный этап	***знать*:** 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; ***уметь*:** 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; ***владеть:*** навыками написания алгоритмов на языках программирования	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание математических моделей преобразования информации в компьютерных системах; алгоритмов обработки информации в её представлении на языках программирования высокого уровня; блоков и структуры алгоритмов, реализуемых на языках программирования высокого уровня. Умение 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; Владение практическими 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.	от 85% до 100%	Отчет по НИР, Отзыв руководителя НИР Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных математических моделей преобразования информации в компьютерных системах; основных алгоритмов обработки информации в её представлении на языках программирования высокого уровня; основных блоков и структуры алгоритмов, реализуемых на языках программирования высокого уровня. Умение строить вычислительные алгоритмы, используя основные численные методы моделирования физических явлений и процессов; строить типовые вычислительные алгоритмы на алгебраических структурах с помощью математических пакетов, в частности, с помощью систем компьютерной алгебры; проводить общий анализ вычислительной эффективности алгоритма, включая анализ быстродействия и объём необходимой памяти; Владение практическими навыками написания	от 70% до 85%	

		высокого уровня; навыками реализации алгоритмов с помощью математических пакетов, в частности, с помощью систем компьютерной алгебры; навыками анализа вычислительной эффективности алгоритмов.	типовых алгоритмов на языках программирования высокого уровня; основными навыками реализации алгоритмов с помощью математических пакетов, в частности, с помощью систем компьютерной алгебры; основными навыками анализа вычислительной эффективности алгоритмов.		
			Обучающийся ***на среднем уровне*** демонстрирует: Знание ряда математических моделей преобразования информации в компьютерных системах; ряда алгоритмов обработки информации в её представлении на языках программирования высокого уровня; отдельных блоков и структуры алгоритмов, реализуемых хотя бы на одном языке программирования высокого уровня. Умение строить отдельные вычислительные алгоритмы, используя численные методы моделирования физических явлений и процессов; строить отдельные типовые вычислительные алгоритмы на алгебраических структурах с помощью хотя бы одного из математических пакетов, в частности, с помощью систем компьютерной алгебры. Владение некоторыми практическими навыками написания отдельных типовых алгоритмов хотя бы на одном языке программирования высокого уровня; некоторыми навыками реализации алгоритмов с помощью хотя бы одного из математических пакетов, в частности, с помощью систем компьютерной алгебры.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: Незнание математических моделей преобразования информации в компьютерных системах; алгоритмов обработки информации в её представлении на языках программирования высокого уровня; незнание блоков и структуры алгоритмов. Неумение строить вычислительные алгоритмы, используя численные методы моделирования физических явлений и процессов; строить вычислительные алгоритмы на алгебраических структурах. Отсутствие практических навыков написания алгоритмов; навыков реализации алгоритмов с помощью систем компьютерной алгебры.	< 50%	
ПК-1 Способность осуществлять подбор, изучение и обобщение научно-технической	Промежуточный этап	***знать*:** основные источники печатной информации в области компьютерной безопасности: научные и научно-технические жур-	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание источников печатной информации в области компьютерной безопасности: научных и научно-технических журналов, библиотек, архивов; электронных источников, российских и зарубежных, в области компьютерной безопасности: Интернет-ресурсов, электронных библиотек,	от 85% до 100%	Отчет по НИР, Отзыв руководителя НИР Дифференциро-

информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности		налы, библиотеки, архивы; основные электронные источники, российские и зарубежные, в области компьютерной безопасности: Интернет-ресурсы, электронные библиотеки, базы данных, Интернет-форумы, профессиональные сайты; правила оформления списков и обзоров литературы; ***уметь:*** осуществлять поиск информации в печатных изданиях; - пользоваться поисковыми системами и осуществлять поиск информации в электронных источниках; сортировать и классифицировать найденную информацию, составлять списки и обзоры литературы; ***владеть:*** навыками поиска, анализа и составления списков источников и обзоров литературы в области компьютерной безопасности.	баз данных, Интернет-форумов, профессиональных сайтов; правил оформления списков и обзоров литературы. Умение осуществлять эффективный поиск информации в печатных изданиях; пользоваться поисковыми системами и осуществлять поиск информации в электронных источниках; сортировать и классифицировать найденную информацию, составлять списки и обзоры литературы в соответствии с ГОСТами. Владение практическими навыками поиска, анализа и составления списков источников и обзоров литературы в области компьютерной безопасности в соответствии с ГОСТами.		ванный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных источников печатной информации в области компьютерной безопасности: основных научных и научно-технических журналов, библиотек, архивов; основных электронных источников, российских и зарубежных, в области компьютерной безопасности: Интернет-ресурсов, электронных библиотек, баз данных, Интернет-форумов, профессиональных сайтов; основных правил оформления списков и обзоров литературы. Умение осуществлять поиск информации в печатных изданиях; пользоваться основными поисковыми системами и осуществлять поиск информации в электронных источниках; сортировать и классифицировать найденную информацию, составлять списки и обзоры литературы. Владение основными практическими навыками поиска, анализа и составления списков источников и обзоров литературы в области компьютерной безопасности.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знание отдельных источников печатной информации в области компьютерной безопасности: отдельных научных и научно-технических журналов, библиотек, архивов; отдельных электронных источников, российских и зарубежных, в области компьютерной безопасности: Интернет-ресурсов, электронных библиотек, баз данных, Интернет-форумов, профессиональных сайтов. Умение осуществлять поиск информации в печатных изданиях; пользоваться отдельными поисковыми системами и осуществлять поиск информации в электронных источниках; сортировать и классифицировать найденную информацию. Владение отдельными практическими навыками поиска и анализа источников и составления об-	от 50% до 70%	

			зоров литературы в области компьютерной безопасности.		
			Обучающийся ***на низком уровне*** демонстрирует: Незнание источников печатной информации в области компьютерной безопасности: научных и научно-технических журналов, библиотек, архивов; электронных источников, российских и зарубежных, в области компьютерной безопасности: Интернет-ресурсов, электронных библиотек, баз данных, Интернет-форумов, профессиональных сайтов. Неумение осуществлять поиск информации в печатных изданиях; пользоваться поисковыми системами и осуществлять поиск информации в электронных источниках; сортировать и классифицировать найденную информацию, составлять списки литературы. Отсутствие практических навыков поиска и анализа источников и составления обзоров и списков литературы в области компьютерной безопасности.	< 50%	
ПСК-2.3 Способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	Промежуточный этап	***знать:*** типовые алгоритмы преобразования информации в компьютерных системах и оценки их эффективности; перспективные методы и алгоритмы преобразования информации в компьютерных системах и методику оценки их эффективности; российские и иностранные стандарты безопасности компьютерных систем; ***уметь:*** строить математические модели информационных процессов в компьютерных системах и алгоритмизировать вычислительные процедуры в этих моделях; поводить аналитическую работу по сравнительной оценке	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание алгоритмов преобразования информации в компьютерных системах и оценок их эффективности; перспективных методов и алгоритмов преобразования информации в компьютерных системах и методики оценки их эффективности; российских и иностранных стандартов безопасности компьютерных систем Умение строить корректные математические модели информационных процессов в компьютерных системах и алгоритмизировать вычислительные процедуры в этих моделях; проводить аналитическую работу по сравнительной оценке эффективности применения различных математических моделей; оценивать быстродействие и объём необходимой памяти для заданного алгоритма. Владение практическими навыками построения математических моделей информационных процессов в компьютерных системах и навыками их алгоритмизации; методикой анализа эффективности алгоритмов.	от 85% до 100%	Отчет по НИР, Отзыв руководителя НИР Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: Знание основных алгоритмов преобразования информации в компьютерных системах и оценок их эффективности; отдельных перспективных методов и алгоритмов преобразования информации в компьютерных системах и методики оценки их эффективности; основных российских и иностранных стандартов безопасности компью-	от 70% до 85%	

		эффективности применения различных математических моделей; оценивать быстродействие и объём необходимой памяти для заданного алгоритма; ***владеть:*** навыками построения математических моделей информационных процессов в компьютерных системах и навыками их алгоритмизации; методикой анализа эффективности алгоритмов.	терных систем Умение строить математические модели основных информационных процессов в компьютерных системах и алгоритмизировать вычислительные процедуры в этих моделях; оценивать быстродействие и объём необходимой памяти для заданного алгоритма. Владение практическими навыками построения основных математических моделей информационных процессов в компьютерных системах и навыками их алгоритмизации; методикой анализа эффективности алгоритмов.		
			Обучающийся ***на среднем уровне*** демонстрирует: Знание отдельных алгоритмов преобразования информации в компьютерных системах; отдельных российских и иностранных стандартов безопасности компьютерных систем Умение строить математические модели отдельных информационных процессов в компьютерных системах и алгоритмизировать вычислительные процедуры в этих моделях. Владение практическими навыками построения отдельных математических моделей информационных процессов в компьютерных системах и навыками их алгоритмизации.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: Незнание алгоритмов преобразования информации в компьютерных системах и оценок их эффективности; перспективных методов и алгоритмов преобразования информации в компьютерных системах и методики оценки их эффективности; российских и иностранных стандартов безопасности компьютерных систем. Неумение строить математические модели информационных процессов в компьютерных системах и алгоритмизировать вычислительные процедуры в этих моделях; оценивать быстродействие и объём необходимой памяти для заданного алгоритма. Отсутствие навыков построения математических моделей информационных процессов в компьютерных системах и навыков их алгоритмизации; владения методикой анализа эффективности алгоритмов.	< 50%	
ПСК-2.4 Способность разрабатывать, анализировать и обосновывать адекватность ма-	Промежуточный этап	***знать*:** номенклатуру и основные характеристики сертифицированных программно-аппаратных средств защиты информации, выпускаемых	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание номенклатуры и характеристик сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; математических методов и алгоритмов, применяемых в программно-аппаратных средствах защиты информации; пер-	от 85% до 100%	Отчет по НИР, Отзыв руководителя НИР Диффе-ренциро-

тематических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации		российской промышленностью; математические методы и алгоритмы, применяемые в программно-аппаратных средствах защиты информации; перспективные методы обработки информации в компьютерных системах; методы алгебры, теории чисел, алгебраической геометрии и дискретной математики и их применение в моделях информационных процессов;	спективных методов обработки информации в компьютерных системах; методов алгебры, теории чисел, алгебраической геометрии и дискретной математики и их применения в моделях информационных процессов. Умение строить математические модели информационных процессов, возникающих при работе программно-аппаратных средств; проводить анализ адекватности существующих математических моделей на основе сравнения их показателей эффективности с перспективными моделями; проводить анализ адекватности существующих математических моделей на основе компьютерного моделирования и получения статистических оценок эффективности. Владение практическими навыками разработки математических моделей информационных процессов в компьютерных системах, используя методы алгебры, теории чисел, алгебраической геометрии и дискретной математики; навыками оценки адекватности моделей информационных процессов в программно-аппаратных средствах.		ванный зачет
		***уметь*:** строить математические модели информационных процессов, возникающих при работе программно-аппаратных средств; проводить анализ адекватности существующих математических моделей на основе сравнения их показателей эффективности с перспективными моделями; проводить анализ адекватности существующих математических моделей на основе компьютерного моделирования и получения статистических оценок эффективности; ***владеть*:** методикой разработки математических моделей информационных процессов в	Обучающийся ***на высоком уровне*** демонстрирует: Знание основной номенклатуры и основных характеристик сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; основных математических методов и алгоритмов, применяемых в программно-аппаратных средствах защиты информации; отдельных перспективных методов обработки информации в компьютерных системах; основных методов алгебры, теории чисел, алгебраической геометрии и дискретной математики и их применения в моделях информационных процессов. Умение строить математические модели основных информационных процессов, возникающих при работе программно-аппаратных средств; проводить анализ адекватности основных существующих математических моделей; проводить анализ адекватности основных существующих математических моделей на основе компьютерного моделирования и получения статистических оценок эффективности. Владение практическими навыками разработки основных математических моделей информационных процессов в компьютерных системах, используя методы алгебры, теории чисел, алгебраической геометрии и дискретной математики; навыками оценки адекватности основных моделей информационных процессов в программно-аппаратных средствах.		
			Обучающийся ***на среднем уровне*** демонстриру-		

		компьютерных системах, используя методы алгебры, теории чисел, алгебраической геометрии и дискретной математики; навыками оценки адекватности моделей информационных процессов в программно-аппаратных средствах	ет: Знакомство с отдельными сертифицированными программно-аппаратными средствами защиты информации, выпускаемыми российской промышленностью и их основными характеристиками; с отдельными математическими методами и алгоритмами, применяемыми в программно-аппаратных средствах защиты информации; отдельными методами алгебры, теории чисел, алгебраической геометрии и дискретной математики. Умение строить математические модели отдельных информационных процессов, возникающих при работе программно-аппаратных средств; проводить анализ адекватности отдельных математических моделей основе компьютерного моделирования и получения статистических оценок эффективности. Владение практическими навыками разработки отдельных математических моделей информационных процессов в компьютерных системах, используя методы алгебры, теории чисел, алгебраической геометрии и дискретной математики; навыками оценки адекватности отдельных моделей информационных процессов в программно-аппаратных средствах.		
			Обучающийся ***на низком уровне*** демонстрирует: Незнание сертифицированных программно-аппаратных средств защиты информации, выпускаемыми российской промышленностью и их основных характеристик; математических методов и алгоритмов, применяемых в программно-аппаратных средствах защиты информации; методов алгебры, теории чисел, алгебраической геометрии и дискретной математики. Неумение строить математические модели информационных процессов, возникающих при работе программно-аппаратных средств; проводить анализ адекватности математических моделей. Отсутствие навыков разработки математических моделей информационных процессов в компьютерных системах; навыков оценки адекватности отдельных моделей информационных процессов в программно-аппаратных средствах.		

Указанные компетенции формируются у студентов в процессе выполнения НИР. Формой текущего контроля за сформированностью компетенций является написание отчета по НИР.

7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкалы оценивания

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания приведены в п. 7.1.

Для оценивания уровня сформированности компетенций используется следующая шкала, где оценки определяются по результатам (R), полученным во время аттестации, для каждой из компетенций исходя из следующих условий:

- «отлично»: $R \geq 85$ %;
- «хорошо»: $70 \leq R < 85$ %;
- «удовлетворительно»: $50\ \% \leq R < 70$ %;
- «неудовлетворительно»: $R < 50$ %.

Далее рассчитывается итоговая оценка (S) по следующей формуле:

$$S = \frac{\sum_{k=0}^{n} R_k}{n},$$

где: R_k – оценка по k-ой компетенции, n – общее количество оцениваемых компетенций.

В качестве оценки за зачет с оценкой выставляется следующая, в зависимости от полученного значения S:

- «отлично»: $S \geq 85$ %;
- «хорошо»: $70\ \% \leq S < 85$ %;
- «удовлетворительно»: $50\ \% \leq S < 70$ %;
- «неудовлетворительно»: $S < 50$ %.

7.3. Комплект оценочных средств по всем заявленным в рабочей программе видам занятий и самостоятельной работы обучающихся

В комплект оценочных средств входят оценочные средства по контролю промежуточной аттестации обучающихся по всем заявленным в рабочей программе видам работ обучающихся:

- индивидуальные задания на НИР;
- контрольные вопросы к дифференцируемому зачету;
- отзыв руководителя НИР;
- отчет студента о НИР.

Вопросы для дифференцированного зачёта:

1. Сформулировать научную задачу (проблему), решаемую в рамках НИР.
2. Описать актуальность и научную значимость решения поставленной задачи (проблемы).
3. Описать результаты анализа эффективности и защищённости исследуемой компьютерной системы (предприятия, организации).
4. Описать частичные задачи, к решению которых сводится главная задача (проблема).

5. По результатам обзора литературы описать состояние решения поставленной задачи (проблемы) на сегодняшний день.
6. Описать планы и результаты проведённых компьютерных экспериментов по определению эффективности и уровней защищённости исследуемой компьютерной системы (предприятия, организации).
7. Описать основные идеи и математические модели, лежащие в основе теоретического исследования.
8. Описать результаты исследования свойств разработанных (используемых) математических моделей.
9. Описать разработанные вычислительные алгоритмы и оценки их эффективности.
10. Описать структуру программного комплекса, реализующего разработанные алгоритмы.
11. Описать планы и результаты компьютерных экспериментов, подтверждающих работоспособность комплекса программ.
12. Произвести сравнительный анализ результатов вычислительных экспериментов.
13. Описать перспективы практического использования результатов решения поставленной задачи (проблемы).

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка сформировавшихся компетенций по НИР проводится в форме текущей и промежуточной аттестации.

Текущий контроль осуществляется руководителем НИР. Руководитель НИР контролирует выполнение задания на НИР согласно индивидуальному плану, оценивает каждый этап выполнения в дневнике НИР.

Промежуточный контроль осуществляется на дифференцированном зачете.

На зачет студенты предоставляют следующие документы:

- задание на НИР, заверенное подписями руководителей НИР и ВКР;
- индивидуальный план НИР, заверенный подписями руководителей НИР и ВКР;
- дневник НИР, заверенный подписью руководителя НИР;
- отчет о результатах НИР, заверенный подписями руководителей НИР и ВКР.

Защита отчета осуществляется перед комиссией, которая состоит из преподавателей и руководителя НИР.

Критерии выставления итоговой оценки- см. п . 7.2.

8. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

8.1. Основная литература

1. Федеральный государственный образовательный стандарт высшего образования по

специальности 10.05.01 Компьютерная безопасность (уровень специалитета) №1512. утвержден 1 декабря 2016 г.

2. Приказ Минобрнауки России от 27.11.2015 №1383 «Об утверждении Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования» (зарегистрировано в Минюсте России 18.12.2015 №40168);
3. Положение о практике обучающихся, осваивающих основные профессиональные программы высшего образования БФУ им. И. Канта (принято решением ученого совета БФУ им. И. Канта 29 июня 2016 года, протокол №23).
4. Алешников С. И. Математические методы защиты информации [Текст]. Ч. 1 : Алгебраические методы, 2015 - 113 с. **Электронная версия.**
5. Алешников С. И. Математические методы защиты информации [Текст] : учеб. пособие. Ч. 2 : Методы алгебраической теории чисел : учебное пособие, 2015 **on-line** - 119 с.
6. Алешников С. И. Математические методы защиты информации [Текст] : практ. пособие. Ч. 3 : Вычислительный практикум по числовым полям и криптографии в квадратичных полях, 2006 - 92 с. **(30 экз.)**
7. Алешников С. И. Математические методы защиты информации [Текст] : практ. пособие. Ч. 4 : Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых, 2015 **on-line**, - 59 с.
8. Алешников С. И. Математические методы защиты информации [Текст] : практ. пособие. Ч. 5 : Методы алгебраических кривых, 2015 - 156, [1] с. **Электронная версия.**
9. Болотов А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых [Текст] / А. А. Болотов, С. Б. Гашков, А. Б. Фролов, 2012. - 303 с. **(27 экз.)**
10. Методы алгебраической геометрии в криптографии [Электронный ресурс] / сост. С. И. Алешников, 2015 **on-line**, 118 с.
11. Нестеренко Ю. В. Теория чисел [Текст] : учеб. для вузов / Ю. В. Нестеренко, 2008. - 264, [1] с. **(16 экз.)**
12. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы [Текст] / А. А. Болотов [и др.], 2012. - 355 с. **(12 экз.)**

8.2. Дополнительная литература

1. Абрамов С. А. Лекции о сложности алгоритмов [Текст] : учеб. пособие для вузов / С. А. Абрамов, 2012. - 245 с. **(12 экз.)**
2. Быстрые мультипликаторы [Электронный ресурс] / сост. Е. С. Алексеенко, 2015 **on-line**, 95 с.
3. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие для вузов/ С.В. Запечников. - М.: Горячая линия-Телеком, 2007. - 319 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). **(15 экз.)**
4. Кайе Ф. Введение в квантовые вычисления [Текст] / Ф. Кайе, Р. Лафламм, М. Моска, 2009. - 346 с. **(16 экз.)**

5. Локальные поля и их приложения [Электронный ресурс] / сост. С. И. Алешников, 2015 **on-line**, 128 с.
6. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение [Текст] : учеб. пособие для вузов / Р. Морелос-Сарагоса ; пер. с англ. В. Б. Афанасьева, 2006. - 319 с. **(16 экз.)**
7. Платонов В. В. Программно-аппаратные средства защиты информации [Текст] : учеб. для вузов / В. В. Платонов, 2014. - 330, [1] с. **(10 экз.)**
8. Смарт Н. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешов под ред. С. К. Ландо, 2006. - 525 с. **(17 экз.)**
9. Технические средства и методы защиты информации [Текст] : учеб. пособие для вузов / А. П. Зайцев [и др.], 2012. - 615 с. **(15 экз.)**
10. Холево А. С. Квантовые системы, каналы, информация [Текст] / А. С. Холево, 2010. - 327 с. **(13 экз.)**

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для выполнения НИР

1. http://xn--90ax2c.xn--p1ai/ - «Национальная электронная библиотека».
2. http://lib.kantiana.ru/irbis/standart/ELIB - ЭБС Кантиана.
3. http://elibrary.ru/defaultx.asp - Научная электронная библиотека eLIBRARY.RU.
4. http://lib.mexmat.ru/catalogue.php?dir=02_06 - Электронная библиотека механико-математического факультета Московского государственного университета. Раздел Криптография
5. http://booklid.org/g/mt_number+theory - Библиотека научной литературы. Раздел «Теория чисел».
6. https://www.coursehero.com/file/p7t1rf7/External-links-Certicom-ECC-Tutorial-http-www-certicom-com-index-php-ecc/ - Online Elliptic Curve Cryptography Tutorial, Certicom Corp.
7. MathWorld. – математический сайт, созданный *Weisstein, Eric W.* (англ.). http://mathworld.wolfram.com/ - сайт по эллиптическим кривым.
8. http://mathemlib.ru/ - библиотека по математике.
9. http://www.math.uiuc.edu/~r-ash/ANT.html - курс по алгебраической теории чисел Robert B. Ash.
10. http://www1.spms.ntu.edu.sg/~frederique/Teaching.html - электронные курсы лекций: алгебра, алгебраическая теория чисел, дискретная математика, группы и симметрии.
11. http://www1.spms.ntu.edu.sg/~frederique/ANT10.pdf - Лекции по алгебраической теории чисел F.Oggier.
12. http://www.math.wisc.edu/~mmwood/748Fall2014/weston.pdf - лекции по алгебраической теории чисел Tom Weston.
13. http://www2.warwick.ac.uk/fac/sci/maths/undergrad/ughandbook/year3/ma3a6/ - электронные лекции по алгебраической теории чисел университета Warwick.

14. http://arxiv.org/list/math.AG/recent - архив новых публикаций по алгебраической геометрии.
15. http://www.jmilne.org/math/CourseNotes/ag.html - веб-сайт J.Miln'a с публикациями по алгебраической геометрии.
16. http://www.fen.bilkent.edu.tr/~franz/LN/LN-algeo.html - собрание лекций по алгебраической геометрии.
17. http://www.math.utah.edu/~yplee/teaching/LN_ag.html - собрание лекций по алгебраической геометрии.
18. http://www.math.byu.edu/~jarvis/alg-geom.html - информация о веб-сайтах по алгебраической геометрии.
19. http://ocw.mit.edu/courses/mathematics/18-726-algebraic-geometry-spring-2009/lecture-notes/ - открытый курс лекций по алгебраической геометрии.
20. http://www.freebookcentre.net/Mathematics/Algebraic-Geometry-Books.html - лекции по алгебраической геометрии в свободном доступе.

10. Методические указания для обучающихся по выполнению НИР

В качестве первого этапа выполнения НИР студенту необходимо ознакомится с программой научно-исследовательской работы. Конкретизировать тему, цель и задачи научно-исследовательской работы с руководителем НИР, а также получить рекомендации по сбору материалов необходимых для ведения НИР. На этом этапе формируется индивидуальный план НИР. Рекомендуется подбирать тему НИР таким образом, чтобы она соответствовала теме выпускной квалификационной работы и специализации «Математические методы защиты информации».

Второй этап выполнения НИР заключается в выполнении задания НИР, которое выражается в виде написания отчета по НИР. Студент осуществляет теоретическое исследование по теме НИР, при необходимости осуществляет практическое исследование. В случае получения глубоких и оригинальных результатов студент готовит тезисы статьи по результатам НИР.

По окончании НИР каждый студент в назначенные сроки, должен предоставить следующие материалы:

1. Отзыв (характеристика), в которой должны быть отражены, оценка умения студента применять профессиональные знания на практике, его деловые качества, коммуникабельность в коллективе и др. Заверяется подписью руководителя НИР.

2. Отчет по НИР и представление результатов исследования: текста статьи (в случаи наличия), практических материалов и др. После ознакомления руководителя НИР с отчетом он допускается или не допускается к защите.

По результатам защиты выставляется итоговая оценка за НИР.

Примеры тематик НИР с кратким содержанием

1. *Анализ стойкости и реализация криптосистемы, основанной на евклидовой решётке.*

Тема квантовых компьютеров — машин, которые используют квантово-механические явления для решения сложных или неразрешимых для современных компьютеров задач, была значительно изучена. Если крупномасштабные квантовые компьютеры когда-либо будут построены, то вопрос взлома большинства используемых сегодня криптосистем с открытым ключом будет решён. Существующие инфраструктуры открытых ключей в значительной степени зависят от криптографических примитивов, таких как криптография на эллиптических кривых, RSA и т.д. Безопасность этих примитивов основывается на сложности решения задачи дискретного логарифма эллиптической кривой и факторизации целого числа. Для обычных компьютеров эти задачи остаются вычислительно неразрешимыми при использовании больших размеров ключей. Однако использование алгоритма Шора (для RSA) и Залки (для ECDLP (Elliptic Curve Discrete Logarithm Problem)) на квантовом компьютере позволяет решить эти задачи за полиномиальное время. Это подрывает конфиденциальность и целостность цифровых коммуникаций в Интернете и во многих других областях. Поэтому национальный институт стандартов и технологий NIST рекомендует постепенный переход к постквантовой криптографии, а также призвал к процессу стандартизации данных схем на конференции PQcrypto в 2016 году. Целью постквантовой криптографии является разработка криптографических систем, которые защищены от атак как квантовых, так и стандартных компьютеров, и могут взаимодействовать с существующими алгоритмами и протоколами. Все вышесказанное и делает данную область актуальной на сегодняшний день.

Целью НИР является анализ структуры и безопасности криптосистемы «ThreeBears», безопасность которой основывается на I-RLWE задаче (Integer-ring Learning with errors). На сегодняшний день уже существует оценка стойкости данной криптосистемы, но решетка, с помощью которой оценивается сложность решения задачи I-RLWE отличается от той, которая используется в данной системе.

Для достижения поставленной цели следует решить следующие задачи:

- описать и проанализировать концепции обучения с ошибками;
- проанализировать взаимосвязи задач RLWE (Ring Learning with errors) и I-RLWE;
- построить решетку, адаптированную к параметрам рассматриваемой криптосистемы;
- оценить параметры BKZ-редукции (*Block Korkine* Zolotarev) для выбранной решетки;
- реализовать основных криптопримитивы в одной из систем компьютерной алгебры.

Литература:

a. M. Roetteler, M. Naehrig, K.M. Svore, K. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In: Takagi, T., Peyrin, T. (eds.), Asiacrypt 2017 (2), Springer LNCS 10625, 2017. - С. 241–270.
b. Gu Chunsheng. Integer version of ring-LWE and its applications. Cryptology ePrint Archive, Report 2017/641, 2017. - 15 с.
c. M. Hamburg. Module-LWE key exchange and encryption: The three bears. Technical report, National Institute of Standards and Technology, 2017.- 28 с.
d. M.R. Albrecht, et al. Estimate all the {{LWE, NTRU}} schemes! IACR Cryptology ePrint Archive, 2018. - 54 с.

2. *Редукция дискретного логарифма на гиперэллиптических рода 2 к конечному полю с помощью билинейных спариваний.*

Многие криптографические протоколы для безопасного обмена ключами и цифровых подписей основаны на вычислительной сложности решения задачи дискретного логарифма в некоторой группе. Наиболее распространёнными группами являются мультипликативные группы конечных полей и группы точек на эллиптических кривых над конечными полями. В качестве альтернативы группам точек эллиптических кривых Н.Коблиц предложил использовать для криптографии якобианы гиперэллиптических кривых. Требования к размеру группы в них меньше и, как следствие, криптосистемы на гиперэллиптических кривых будут работать быстрее. Гиперэллиптические кривые позволяют в перспективе уменьшить требуемый размер ключа в два раза, что, учитывая увеличение вычислительных мощностей с каждым годом (а, следовательно, и требования к размерам ключей), является серьезным преимуществом. Отметим, что гиперэллиптические кривые малого рода (g = 2, 3) являются наиболее оптимальным выбором, так как для них не существует эффективного алгоритма вычисления дискретного логарифма, за исключением общего ρ-метода Полларда. Также из плюсов выбора малого рода можем отметить существование быстрого группового закона. Исходя из этого, можно сказать, что исследование безопасности криптосистем на гиперэллиптических кривых является важным вопросом.

Целью НИР является разработка и реализация специализированного алгоритма сведения задачи дискретного логарифма на гиперэллиптических кривых рода 2 к задаче дискретного логарифма в конечном поле с помощью билинейных спариваний, а также подбор и генерация оптимальных гиперэллиптических кривых рода 2 и практическая проверка их стойкости.

Для этого необходимо решить следующие задачи:

1. Проанализировать скорости существующих явных формул сложения и удвоения точек в якобиане гиперэллиптической кривой рода 2.
2. Подобрать подходящую кривую и ее параметры для реализации билинейных спариваний.
3. Исследовать границы применимости атаки Фрея – Рюка и выбрать оптимальные параметры для криптосистем на гиперэллиптических кривых рода 2.
4. Описать и проанализировать спаривание Тэйта в общем случае и для гиперэллиптических кривых рода 2.
5. Реализовать спаривание Тэйта в системе компьютерной алгебры.
6. Проанализировать алгоритм MOV-атаки и алгоритм атаки Фрея – Рюка и выполнить его реализацию.
7. Оптимизировать атаку Фрея – Рюка с помощью эйт-спаривания на гиперэллиптических кривых.

Литература:

a. Bos, Joppe W, Craig Costello, and Andrea Miele. 2014. “Elliptic and Hyperelliptic Curves: A Practical Security Analysis.” In *International Workshop on Public Key Cryptography*, 203–20. Springer.
b. Cohen, Henri, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. 2005. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC press.
c. Frey, Gerhard, and Tony Shaska. 2018. “Curves, Jacobians, and Cryptography.” *arXiv Preprint arXiv:1807.05270*.

d. Ishii, Masahiro. 2016. “Pairings on Hyperelliptic Curves of Genus 2 at High Security Levels.” PhD thesis, Ph. D. thesis, Nara Institute of Science; Technology.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

11.1. Программное обеспечение

- Программа для ЭВМ Wolfram Mathematica 10.2 Education Bundled Price (Количество лицензий – 3, Номер акта / накладной – Tr053766, Дата акта – 02.11.15);
- IBM SPSS Statistics Base Campus Edition (Количество лицензий – 25, Номер акта / накладной – Tr031923, Дата акта – 10.06.15);
- Intel Cluster Studio for Linux (Количество лицензий – 2, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Maple 11 (Количество лицензий – 30, Номер акта / накладной – Tr068983, Дата акта – 19.12.07);
- Mathematica (Количество лицензий – 15, Номер акта / накладной – Tr066706, Дата акта – 18.11.13);
- Mathworks Gauges Blockset Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Mathworks Simulink 3d animation Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Microsoft SQL Srv Standard Core 2014 (Количество лицензий – 4, Номер акта / накладной – Tr063168, Дата акта – 24.11.14);
- Microsoft Visio Professional 2010 (Количество лицензий – 25, Номер акта / накладной – Tr070182, Дата акта – 15.12.11);
- Microsoft Visual Studio 2005 (Количество лицензий – 30, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).
- Parallel Computing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Signal Processing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Statistica Base (Количество лицензий – 20, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).
- Statistics Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- System Identification Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11).

11.2. Информационные справочные системы

1. http://xn--90ax2c.xn--p1ai/ – «Национальная электронная библиотека».
2. http://lib.kantiana.ru/irbis/standart/ELIB – ЭБС Кантиана.
3. http://elibrary.ru/defaultx.asp – Научная электронная библиотека eLIBRARY.RU.
4. http://ibooks.ru/ – ЭБС «Айбукс.ру/ibooks.ru».
5. http://www.iprbookshop.ru/ – ЭБС «IPRbooks».
6. http://e.lanbook.com/ – Издательство «Лань», ЭБС.
7. http://infomag.biz/index.php – Служба ИНФОМАГ - Библиографическая и другая научная информация, в первую очередь оглавления научных и технических журналов, а также зарубежных научных электронных бюллетеней.
8. http://window.edu.ru/ – Информационная система «Единое окно доступа к образовательным ресурсам».
9. http://www.rsl.ru/ – Российская государственная библиотека
10. http://www.biblioclub.ru/ – Университетская библиотека онлайн

11.3. Электронные версии книг

1. *Болотов А.А*. Элементарное введение в эллиптическую криптографию. Том 1, 2 / А. А. Болотов, С. Б. Гашков, А. Б. Фролов, А.А. Часовских 2006. - 303 с. https://vk.com/wall-54530371_7165
2. *Городенцев А.Л*. Геометрическое введение в алгебраическую геометрию. – Екатеринбург: Рукопись 8 – 13 октября 2012. http://gorod.bogomolov-lab.ru/ps/stud/giag_ru/giag.pdf
3. *Кокс Д., Литтл Дж., О'Ши Д*. Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. – М.: Мир, 2000. http://inis.jinr.ru/sl/vol2/Mathematics/Алгебра/Кокс,Литтл,О'Ши,_Идеалы,многообразия_и_алгоритмы,2000.pdf
4. *Львовский С.М.* Лекции по алгебраической геометрии (Рукопись). – М.: НМУ, 1996/97. http://ium.mccme.ru/ancient/agf96.html
5. *Мао В*. Современная криптография. Теория и практика; [пер. с англ. и ред. Д. А. Клюшина]; Компания Hewlett-Packard. - М.; СПб.; Киев: Вильямс, 2005. http://booksshare.net/index.php?id1=4&category=cryptography&author=venbo-mao&book=2005
6. *Рид М.* Алгебраическая геометрия для всех. – М.: Мир, 1991. http://nashol.com/2013070372256/algebraicheskaya-geometriya-dlya-vseh-rid-m-1991.html
7. *Степанов С.А*. Арифметика алгебраических кривых. – М.: Наука, 1991. http://inis.jinr.ru/sl/vol2/Mathematics/Number%20Theory/Степанов%20С.А.,%20Арифметика%20алгебраических%20кривых,%201991.pdf

8. *Харрис Дж.* Алгебраическая геометрия. Начальный курс. – М.: МЦНМО, 2005. http://www.read.in.ua/book141763/?r=13&p=2&s=%D5
9. *Шафаревич И.Р.* Основы алгебраической геометрии. Том 1. Алгебраические многообразия в проективном пространстве – М.: МЦНМО, 2007. http://bookre.org/reader?file=440571
10. *Alaca S., Williams K.S.* Introductoty Algebraic Number Theory. – Cambridge University Press, 2004. - http://catdir.loc.gov/catdir/samples/cam041/2003051243.pdf
11. *Bump D.* Algebraic geometry. – World Scientific, 1998. http://bookre.org/reader?file=440227&pg=173
12. *Chambert-Loir A.* Algebre commutative et introduction a la geometrie algebrique (Manuscript). – Paris : Universite Paris-Sud, 2013. https://webusers.imj-prg.fr/~antoine.chambert-loir/enseignement/2013-14/aceiga/Dea.pdf
13. *Fulton W.* Algebraic Curves. An Introduction to Algebraic Geometry. – W. A. Benjamin Inc., 2008. http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf
14. *Frey G.* On the Relation between Brauer Groups and Discrete Logarithms. Tatra Mt. Math. Publ, 33: 199-227, 2006. http://www.iem.uni-due.de/preprints/frey_brauerpreprint1.pdf
15. *Frey G.* Duality Theorems in Arithmetic Geometry and Applications in Data Security (Manuscript). IEM. Universität of Duisburg-Essen. Essen, 2008. http://www.tau.ac.il/~jarden/Summer/block.pdf
16. *Frey G., Lange T.* Mathematical Background of Public Key Cryptography (Preprint № 10). IEM. Universität of Duisburg-Essen. Essen, 2003. http://www.emis.de/journals/SC/2005/11/pdf/smf_sem-cong_11_41-73.pdf
17. *Gathmann A.* Algebraic Geometry. Class Notes TU Kaiserslautern 2014, available at https://www.mathematik.uni-kl.de/~gathmann/class/alggeom-2014/alggeom-2014.pdf
18. *Gathmann A.* Algebraic Geometry. Notes for a class taught at the University of Kaiserslautern 2002/2003 (Manuscript). https://www.mathematik.uni-kl.de/~gathmann/class/alggeom-2002/alggeom-2002.pdf
19. *Handbook* of elliptic and hyperelliptic curve cryptography / Scientific editors, Henry Cohen &Gerhard Frey. – Chapman & Hall/CRC, 2006. https://www.pdfdrive.com/handbook-of-elliptic-and-hyperelliptic-curve-cryptography-d8067205.html
20. *Hassett B.* Introduction to Algebraic Geometry. – Cambridge University Press, 2007. http://ebooks.cambridge.org/chapter.jsf?bid=CBO9780511755224&cid=CBO9780511755224A045&tabName=Chapter&imageExtract=
21. *Hohold T,* et al. Algebraic geometry Codes. In the Handbook of Coding Theory, vol I, pp. 871-961. – Elsevier, Amsterdam. Corrected version 2011. http://www.win.tue.nl/~ruudp/paper/31.pdf*Hulek K.* Elementary Algebraic Geometry. – AMS, 2003. http://bookre.org/isearch?q=Hulek+Elementary+Algebraic+Geometry
22. *Li H.* An Introduction to Commutative Algebra. From the Viewpoint of Normalization. – World Scientific, 2004. http://booksee.org/md5/1f1bf965947161cc7f300d4475dd0c36

23. *Milne J.S.* Algebraic Number Theory, 2014. http://www.jmilne.org/math/CourseNotes/ANT.pdf
24. *Nguyen K.* Explicit Arithmetic of Brauer Groups. Ray Class Fields and Index Calculus. Diss. Zur Erlangung des Grades eines Doktors der Naturwissenschaften. Universitaet GEHE. Essen, 2001. http://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-10585/thesis.pdf
25. *Niederreiter H., Xing Ch.* Algebraic Geometry in Coding Theory and Cryptography. – Princeton University Press, 2009. http://booksee.org/md5/9ba70b303733e0b965bcc4968a13e169
26. *Perrin D.* Algebraic Geometry. An Introduction. – Springer-Verlag, 2008. http://booksee.org/md5/b2d586a1c5478d71e5a7c9e4c0634c18
27. *Stein William.* Algebraic Number Theory, a Computational Approach. http://wstein.org/books/ant/ant.pdf
28. *Stichtenoth H.* Algebraic Function Fields and Codes. – Springer-Verlag Berlin Heidelberg, 2009. http://booksee.org/g/%20Henning%20Stichtenoth
29. *Washington L.C.* Elliptic curves: number theory and cryptography. – Chapman & Hall/CRL, 2008. https://people.cs.nctu.edu.tw/~rjchen/ECC2012S/Elliptic%20Curves%20Number%20Theory%20And%20Cryptography%202n.pdf
30. *Weng A.* Constructing Hyperelliptic Curves of Genus 2 suitable for Cryptography. Math. of Comput. Vol 72, № 241, 2002. P. 435-458. http://www.ams.org/journals/mcom/2003-72-241/S0025-5718-02-01422-9/S0025-5718-02-01422-9.pdf
31. *Weng A.* Konstruktion kryptographisch geeigneter Kurven mit komplexen Multiplikation (Dissertation). Universität GH Essen, 2001. http://www.iem.uni-due.de/zahlentheorie/preprints/wengthesis.pdf

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по НИР

Класс персональных компьютеров, объединенных в локальную сеть с выходом в сеть Интернет. Стандартное программное обеспечение. Программные продукты, указанные в п.11.1.

1. Лекционная аудитория на 80 человек со средствами мультимедиа в составе: экран, проектор EPSON EB-450W, моноблок MSI AE 222 G.

2. Учебный дисплейный класс (аудитории №№ 214, 220, 230а и 235 Учебного корпуса №2 БФУ им.И.Канта), в которых установлены персональные компьютеры с параметрами - Intel Core I3-3220, 3.3 GHz, 4Gb RAM, 1 Tb HDD, 21,5", keyboard, Mouse, LAN, Internet access. Компьютеры включены в соответствующий домен компьютерной сети БФУ им.И.Канта.

На данных ПК установлено обычное ПО, а также указанное в разделе 9.2. специализированное ПО.

Программно-аппаратные средства лаборатории программно-аппаратных средств защиты информации согласно имеющемуся перечню.

1. Маршрутизатор Cisco 2821. Коммутатор switch d-link des-3526. Стойка серверная 1000 мм 42u с дополнительным пассивным и организующим оборудованием.
2. АПКШ «Континент» (криптошлюз) в корпусе промышленного PC (1U), ЦУС «Континент» (центр управления сетью) в корпусе промышленного PC (1U) с сервером доступа, Абонентский пункт «Континент-АП».
3. «Аккорд-NT/2000» v. 2.0.1 на базе комплекса СЗИ НСД «Аккорд-АМДЗ» v.3.1 (PCI).
4. Средство криптографической защиты информации, включающее библиотеки шифрования и электронную цифровую подпись Верба-W.
5. Средство криптографической защиты информации КРИПТО-ПРО УЦ.
6. Система обеспечения безопасности информации в корпоративной сети «Secret Net» версии 5.0. (обновление) в составе: - Сервер безопасности Secret Net 5.0 -C (до 50 защищаемых серверов и рабочих станций); - «Secret Net» для Windows 2000/XP/2003 (клиенты сервера безопасности); - Системы обеспечения безопасности информации автономных компьютеров «Secret Net» версии 5.0. (обновление); - «Secret Net 5.0 – C» для Windows 2000|XP/2003.
7. Система обнаружения атак Real Secure Network 10/100.
8. Программный продукт для обеспечения сетевой безопасности Internet Scanner.
9. Программный продукт для обеспечения сетевой безопасности X Spider 7.
10. Средство контроля защищенности от несанкционированного доступа “Ревизор сети” (версия 1.2.1.0).
11. Средство контроля защищенности от несанкционированного доступа “Ревизор системы” (версия 1.0).
12. Средство контроля защищенности от несанкционированного доступа “TERRIER (версия 3.0).
13. Средство контроля защищенности от несанкционированного доступа “Ревизор 1 XP”.
14. Средство контроля защищенности от несанкционированного доступа “Ревизор 2 XP”.
15. Средство контроля защищенности от несанкционированного доступа ФИКС 3.0.
16. Персональное средство криптографической защиты информации ПСКЗИ ШИПКА-1.5.
17. Межсетевой экран ССПТ-1М, исполнение 54323649.401350.003-03 (корпус Iwill G478_XG(19” 1U).
18. Программное средство для защиты от несанкционированного доступа к информации в персональном компьютере с возможностью подключения аппаратных идентификаторов Dallas Lock 7.0.

Технические средства лаборатории технических средств защиты информации согласно имеющемуся перечню

1. Программно-аппаратный комплекс автоматического обнаружения, идентификации и нейтрализации подслушивающих устройств типа «Крона плюс».

2. Анализатор спектра типа "СК-4 Белан - 32".
3. Комплекс для проведения исследований на ПЭМИН типа «НАВИГАТОР».
4. Универсальный поисковый прибор типа «СРМ-700 Advancer + ВМР 1200.
5. Анализатор проводных линий типа «Отклик».
6. Портативный металло-детектор типа «ВМ311».
7. Блокиратор сотовых телефонов типа «Завеса».
8. Прибор ночного видения типа «Эдельвейс - МП».
9. Устройство защиты аналоговых АТС «Гранит».
10. Устройство защиты цифровых АТС «МП-1Ц».
11. Генератор вибро-акустического шума типа «Соната-АВ-1М».
12. Ручной измеритель частоты и мощности типа «РИЧ-8».
13. Аудио-излучатель типа «Соната-АВ-АИ-65».
14. Вибро-излучатель типа «Соната-АВ-ВИ-45».
15. Универсальный генератор шума типа «Гром-ЗИ-4».
16. Подавитель диктофонов типа «ЛГШ-104».
17. Генератор вибро-акустического шума ЛГШ-401.
18. Генератор радиопомех типа «ЛГШ-501».
19. Пьезо-излучатель типа «Соната-АВ-ПИ-45».
20. Антенна логопериодическая типа «ЕЛВ-26».
21. Сканирующий приемник типа AR-8200.
22. Нелинейный локатор типа «Лорнет».

13. Приложения

Приложение 1

Титульный лист отчета по НИР

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

Отчёт
о научно-исследовательской работе

Обучающийся _____
(*Ф.И.О. подпись*)

Направление подготовки 10.05.01 Компьютерная безопасность
(*шифр, название*)

Профиль Математические методы защиты информации
(*название*)

Тема выпускной квалификационной работы _____
_____
_____
_____

Срок прохождения НИР: с « 1 » сентября 2019 г. по « 28 » сентября 2019 г.

Руководитель НИР:

_____
(*Ф.И.О., должность, подпись*)

Руководитель ВКР:

_____
(*Ф.И.О., должность, подпись*)

Отчет подготовлен _____ _____
(*подпись обучающегося*) (*И.О. Фамилия*)

Калининград, 2019

СТРУКТУРА ОТЧЕТА ПО НИР

Титульный лист

Оглавление

ВВЕДЕНИЕ. *Во введении ставятся цель и задачи НИР, обосновывается выбор научной тематики. Обязательно указывается, что был пройден инструктаж по технике безопасности и прочие виды инструктажа, предусмотренные программой НИР.*

ОСНОВНАЯ ЧАСТЬ. *В основной части содержится*

- *обзор и анализ литературы по теме исследования*;
- *постановки конкретных задач исследования*;
- *описание методики проведения теоретического исследования / практической работы*;
- *планы и результаты предварительного компьютерного моделирования, результаты статистического анализа его итогов*;
- *описание рабочих гипотез, структурных схем, математических моделей, протоколов обмена информацией, вычислительных алгоритмов*;
- *результаты исследования и анализа свойств математических моделей*;
- *результаты анализа эффективности разработанных алгоритмов*;
- *описание разработанного комплекса программ*;
- *планы и результаты компьютерного моделирования в соответствии с разработанными моделями и алгоритмами*;
- *результаты анализа адекватности разработанных математических моделей, корректности алгоритмов, работоспособности комплекса программ*;
- *предложения и рекомендации по внедрению результатов НИР в проектную деятельность, инженерную практику и производство*.

ЗАКЛЮЧЕНИЕ. *В заключении формулируются основные результаты проделанной работе.*

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ. *Список использованных источников может содержать перечень нормативных правовых источников, учебных, научных и периодических изданий, используемых обучающимся для выполнения программы НИР.*

ПРИЛОЖЕНИЯ К ОТЧЕТУ ПО НИР:

Приложение 1 – Задание на НИР.

Приложение 2 – Индивидуальный план НИР.

Приложение 3 – Дневник НИР.

Приложение 4 – Отзыв руководителя НИР.

Приложение 5 – Дополнительная информация.

В приложение 5 *могут включаться копии документов* (*статей, нормативных документов, отчетов и др.*), *изученных и использованных обучающимся в период проведения НИР, листинги компьютерных программ, таблицы с результатами компьютерных экспериментов, графики, статистические материалы и т.д.*

Приложение 2

Форма задания на НИР

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

Задание на
научно-исследовательскую работу

для _____

(*ФИО обучающегося полностью*)

Обучающегося 6 курса

Направление подготовки 10.05.01 Компьютерная безопасность

Профиль Математические методы защиты информации

Срок прохождения НИР: с « 1 » сентября 2019 г. по « 28 » сентября 2019 г.

№ п/п	Формулировка задания	Время выполнения
I.	Цель: *в соответствии с темой выпускной квалификационной работы*	
II.	**Содержание НИР:** *в соответствии с темой выпускной квалификационной работы* 1. Изучить:	
	2. Теоретически исследовать:	
	3. Провести компьютерное моделирование	
	4. Приобрести навыки:	
III.	**Дополнительное задание:** Подготовить и представить оформленный в соответствии с требованиями отчет по НИР и прилагаемые документы к защите.	
IV.	**Организационно-методические указания:**	

Цель НИР:

- 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.

Задачи НИР:

Изучить:

- научную литературу по теме ВКР (монографии, статьи, патентные материалы, научные отчёты, техническую документацию, авторефераты и диссертации);
- современную технологию анализа потенциальных каналов утечки информации;
- структуру и методы построения современных моделей безопасности компьютерных систем;
- современную технологию защиты информации в компьютерных системах;
- современную технологию противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- математические модели и алгоритмы, используемые в современных криптографических системах и системах помехоустойчивого кодирования.

Исследовать:

- алгоритмы быстрых вычислений в алгебраических структурах, их компьютерную реализацию;
- системы и алгоритмы помехоустойчивого кодирования информации, их свойства, оценки эффективности и их компьютерные модели;
- системы и алгоритмы шифрования информации, их свойства, оценки эффективности и их компьютерные модели;
- математические методы, модели и алгоритмы, используемые при разработке инфраструктуры современных криптосистем с открытым ключом, и их компьютерные модели;
- математические и компьютерные модели псевдослучайных генераторов, их свойства и методы статистического тестирования;
- структуру, принципы функционирования и управления современными системами защиты информации в компьютерных системах;

Содержание НИР, вопросы, подлежащие изучению:

- Разработка методик анализа и оценки уровней защищённости компьютерных систем.
- Проектирование защищённых компьютерных систем, в частности систем автоматизированной обработки персональных данных.
- Разработка систем защиты информации и систем управления информационной безопасностью, основанных на новых логических и математических принципах;

- Разработка методов контроля эффективности защиты информации, основанных на новых математических моделях и методах;
- Анализ эффективности, модификация и построение криптографических алгоритмов, основанных на новых математических принципах.
- Разработка и анализ систем помехоустойчивого кодирования на алгебраических кривых над конечными полями с большим числом точек.
- Проектирование и статистический анализ качества потоковых шифров и генераторов псевдослучайных чисел.
- Компьютерное моделирование эффективных алгоритмов: вычислительных, криптографических, кодирования, сжатия и восстановления информации при её передаче и хранении.
- Анализ и разработка криптографической инфраструктуры для конкретных систем защиты информации; алгоритмическое обеспечение инфраструктуры.
- Анализ стойкости и разработка схем и защищённых протоколов обмена информацией в компьютерных системах и сетях общего назначения.
- Анализ стойкости и разработка защищённых протоколов обмена информацией в специализированных компьютерных системах и сетях: банковских, корпоративных, системах электронного голосования и т.д.

Планируемые результаты НИР:

- подготовка основных результатов теоретического исследования (теоремы, свойства, доказательства, математические алгоритмы, описания, анализ и оценка результатов);
- подготовка основных результатов компьютерного моделирования (компьютерные алгоритмы, описания экспериментов, результаты экспериментов, анализ и оценка результатов);
- систематизация и обобщение материала для написания выпускной квалификационной работы.

Задание выдал руководитель ВКР_____

Ф.И.О., подпись, «___» _____2019 г.

Руководитель НИР:_____

Ф.И.О., подпись, «___» _____2019 г.

Задание получил _____

Ф.И.О., подпись, «____» _____2019 г.

Приложение 3

Форма индивидуального плана НИР

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

Индивидуальный план
проведения научно-исследовательской работы

для _____

(*ФИО обучающегося полностью*)

Обучающегося 6 курса

Направление подготовки 10.05.01 Компьютерная безопасность

Профиль Математические методы защиты информации

Срок прохождения НИР: с « 1 » сентября 2019 г. по « 28 » сентября 2019 г.

Руководитель НИР:

_____

(*Ф.И.О., должность, подпись*)

Руководитель ВКР:

_____

(*Ф.И.О., должность, подпись*)

№ п/п	Этапы (периоды) НИР	Вид работ	Срок прохождения этапа (периода) НИР	Форма отчетности
1	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. Выбор и обоснование текущей темы исследования. 5. Получение и согласование индивидуального задания на НИР; 6. Разработка и утверждение индивидуального плана НИР и графика проведения исследований; 7. Получение документации по НИР (программа НИР и дневник НИР) в сроки, определенные программой;		Письменный отчёт. Индивидуальное задание на НИР.
2	Основной	1. Подготовка к проведению научного исследования: ознаком-		Письмен-

№ п/п	Этапы (периоды) НИР	Вид работ	Срок прохождения этапа (периода) НИР	Форма отчетности
	этап	ление 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.		ный отчет. Дневник НИР
		2. Проведение предварительного 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. Проведение заключительного экспериментального исследования: экспериментальная проверка теоретических результатов, компьютерное моделирование разработанных алгоритмов, расчёт ключевых примеров.		
		5. Обработка и анализ полученных теоретических результатов и результатов компьютерного моделирования, проверка корректности разработанных алгоритмов; проверка работоспособности комплекса программ.		
		6. Анализ возможности публичного представления результатов НИР, возможности внедрения результатов исследования в проектную деятельность, инженерную практику, в производство.		
		7. Введение дневника НИР		
3	Заключительный этап	1. Подготовка отчета о прохождении НИР 2. Представление отчета по НИР и прилагаемых документов в Институт для защиты.		Зачет с оценкой.

Обучающийся _____

(*Ф.И.О.*)

Приложение 4

Форма дневника научно-исследовательской работы

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

ДНЕВНИК

научно-исследовательской работы

Обучающийся _____

(*Ф.И.О. полностью*)

Направление подготовки 10.05.01 Компьютерная безопасность

(*шифр, название*)

Профиль Математические методы защиты информации

(*название*)

Срок прохождения НИР: с « 1 » сентября 2019 г. по « 28 » сентября 2019 г.

Руководитель НИР _____ «___» _____ 2019 г.

(*Ф.И.О. подпись*)

Калининград, 2019

Дневник

День	Дата	Содержание выполненного задания	Применяемое оборудование, литература (с указанием прорабатываемой темы), компьютерные программы, инструмент, материалы, и пр.	Отметка руководителя о качестве выполненного задания	Подпись руководителя НИР
1.		Инструктаж по технике безопасности, пожарной безопасности, ознакомление с правилами внутреннего трудового распорядка и с требованиями охраны труда.			
1.		Ознакомление с индивидуальным планом НИР.			
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					

Обучающийся _____ _____ «___»_____ 2019 г.

(*Ф.И.О. подпись*)

Приложение 5

Рекомендации по техническому оформлению отчета о результатах научно-исследовательской работы

Оформление отчета о результатах прохождения НИР необходимо выполнять в соответствии со следующими правилами.

Объем работы: до 25 страниц формата А4 (210 х 297), но не менее 10 страниц, набранных через полтора интервала на одной стороне листа белой бумаги в текстовом процессоре Word, 2/3 из которых должна занимать практическая часть. Допускается представлять иллюстрации и таблицы на листах формата А3.

Поля: левое - 3 см, правое – 1,5 см, верхнее – 2 см, нижнее – 2 см.

Шрифт: TimesNewRoman, размер шрифта – 14 пунктов.

Титульный лист оформляется по образцу.

Все страницы отчета, включая иллюстрации и приложения, нумеруются по порядку от титульного листа до последней страницы без пропусков и повторений.

Первой страницей является титульный лист, оформленный в соответствующем порядке, номер страницы на нем не ставится. Далее, после титульного листа, вшивается чистый лист для написания рецензии, который не нумеруется. После вшивается задание на НИР и индивидуальный план НИР, подписанные руководителем НИР, которые не нумеруются. Затем формируется содержание отчёта, совпадающее с утвержденным планом. Элементы: введение, заключение, список использованной литературы, приложение в содержании и плане не нумеруются.

Далее вшивается первый лист введения, номер страницы на нем не ставится. На последующих страницах порядковый номер печатается в правом верхнем углу без точки в конце, начиная с четвертой страницы, которая является второй страницей введения.

Заголовки основных и дополнительных разделов отчета следует располагать на расстоянии не менее трех интервалов от текста в середине строки без точки в конце и печатать жирным шрифтом, прописными буквами, не подчеркивая.

Заголовки подразделов и пунктов следует начинать с абзацного отступа и печатать жирным шрифтом с прописной буквы, не подчеркивая, без точки в конце.

Если заголовок включает несколько предложений, их разделяют точками. Переносы слов в заголовках не допускаются.

Иллюстрации должны иметь названия. Иллюстрации обозначаются словом "Рисунок", которое помещают под иллюстрацией, и нумеруются последовательно арабскими цифрами в пределах всего отчета. Иллюстрации и таблицы, расположенные на отдельных листах, включают в общую нумерацию страниц. На все иллюстрации должны быть ссылки в отчете.

Таблицы нумеруют последовательно арабскими цифрами в пределах всего отчёта. В левом верхнем углу таблицы помещают слово "Таблица" с указанием номера этой таблицы и соответствующим заголовком. На все таблицы должны быть ссылки в отчете.

Если в отчёте одна таблица, ее не нумеруют и слово "Таблица" не пишут.

Таблицу размещают непосредственно после первого упоминания о ней в тексте на этой же или следующей странице таким образом, чтобы читать ее можно было без пово-

рота или с поворотом по часовой стрелке. Ссылка на таблицу по ходу текста выполняется так: "в таблице 2 приводятся данные о ... ".

Примечания к таблицам, иллюстрациям или пунктам и подпунктам текста размещают непосредственно после пункта, подпункта, таблицы, иллюстрации, к которым они относятся, и печатают с прописной буквы с абзацного отступа. Слово "Примечание" следует печатать с абзацного отступа жирным шрифтом.

Ссылки на разделы, подразделы, пункты, подпункты, иллюстрации, таблицы, формулы, уравнения, перечисления, приложения, следуют указывать порядковым номером, например: "... в разделе 4", "... по пункту 3.3.4", "... в подпункте 2.3.41, перечисление 3", "...по формуле (3)", "... в уравнении (2)",-"... на рисунке 8", "... в приложении 6".

Формулы могут быть вписаны в текст от руки тщательно и разборчиво или напечатаны на компьютере. Не разрешается одну часть формулы вписывать от руки, а другую впечатывать. Выше и ниже каждой формулы должно быть оставлено не менее одной свободной строки. Размеры знаков для формулы рекомендуются следующие: прописные буквы и цифры – 7-8 мм, строчные – 4 мм, показатели степени и индексы – не менее 2 мм.

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой даны в формуле. Значение каждого символа и числового коэффициента следует давать с новой строки. Первую строку пояснения начинают со слова "где" без двоеточия.

Формулы в отчёте следует нумеровать порядковой нумерацией в пределах всего отчета арабскими цифрами в круглых скобках в крайнем правом положении на строке. Если в отчете только одна формула или уравнение, их не нумеруют.

Отчет о результатах НИР вшивается в папку-скоросшиватель с прозрачной верхней обложкой.

Приложение 6

Форма отзыва руководителя НИР

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

ОТЗЫВ
руководителя о работе обучающегося в период прохождения НИР

Обучающийся _____
(Ф.И.О.)

Института физико-математических наук и информационных технологий проходил научно-исследовательскую работу _____
(вид и тип практики)

в период с « 1 » сентября 2019 г. по « 28 » сентября 2019 г.

На время НИР _____
(*Фамилия, И.О. обучающегося*)

поручалось решение следующих задач: _____

_____

_____

Результаты работы обучающегося:

Степень раскрытия темы _____

_____

Обоснованность выбранных методов исследования _____

_____

Достоверность результатов исследования _____

_____

Положительные стороны отчета _____

_____

Недостатки отчета _____

_____

Самостоятельность и инициативность студента _____

_____

Навыки, приобретенные за время НИР _____

_____

Отношения студента к работе _____

Считаю, что по итогам НИР обучающийся может (не может) быть допущен к защите отчета по НИР.

Рекомендуемая оценка за НИР_____
(дифференцированный зачет)

Руководитель НИР_____
(Ф.И.О. подпись)

«____»_____2019 г.

Руководитель ВКР:

_____
(Ф.И.О. подпись)

«____»_____2019 г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. Иммануила Канта

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ Е.П.Ставицкая
«20» марта 2020 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«20» марта 2020 г.

Программа учебной практики

по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности

для студентов 1, 2 и 3 курсов
очной формы обучения
специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации
квалификация (степень) выпускника: *специалист*

Калининград
2020

Лист согласования

Составитель: доцент Института физико-математических наук и информационных технологий БОЛТНЕВ ЮРИЙ ФЁДОРОВИЧ.

Рабочая программа обсуждена и утверждена на заседании Учебно-методического совета ИФМНиИТ.

Протокол №____от «____»_____ 201__ г.

Председатель Совета _____ доцент, к.ф.-м.н. А.А.Шпилевой
Менеджер ООП_____Е.П.Ставицкая

Рабочая программа пересмотрена на заседании Учебно-методического совета ИФМНиИТ

Внесены следующие изменения (или изменений не внесено):

1. _____
2. _____
3. _____

Протокол №____от «____»_____ 20__ г.

Председатель Совета _____ доцент, к.ф.-м.н. А.А.Шпилевой
Менеджер ООП_____Е.П.Ставицкая

Содержание

1. Вид практики, способ и формы ее проведения

Вид практики: Учебная практика по получению первичных профессиональных умений и навыков научно-исследовательской деятельности (далее **учебная практика** или **практика**).

Учебная практика проводится в следующих **формах**:

- непрерывная – в период учебного времени для проведения практики, указанного в календарном учебном графике.

Способы проведения учебной практики:

- стационарная на рабочем месте (в лабораториях и компьютерных классах Института физико-математических наук и информационных технологий).

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

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.

Задачами учебной практики являются:

1) развитие способностей студента к аналитической работе;
2) освоение навыков планирования, проведения и анализа результатов прикладных (вычислительных) работ в области компьютерной безопасности;
3) формирование и развитие у студентов устойчивого интереса к профессиональной деятельности, потребности в самообразовании;
4) подготовка алгоритмической вычислительной части курсовых работ.

В результате освоения ООП обучающийся должен овладеть следующими результатами обучения при прохождении практики:

Код компетенции	**Результаты освоения ООП Содержание компетенций**	**Перечень планируемых результатов обучения при прохождении практики**
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	В результате прохождения практики обучающийся должен: • ***знать*:** нормы корректного поведения в обществе; социально-культурные характеристики основных этносов; • ***уметь*:** толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей и на этой основе грамотно стро-

		ить взаимоотношения с членами трудового коллектива; планировать и осуществлять производственную деятельность в коллективе; • ***владеть*:** навыками урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий при планировании и реализации производственной деятельности трудового коллектива.
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	В результате прохождения практики обучающийся должен: • ***знать*:** современные информационные методики и технологии; перечень и возможности распространённых систем компьютерной алгебры; методы математической обработки информации, используемые при решении задач защиты информации; • ***уметь*:** грамотно применять математические пакеты компьютерной алгебры для решения вычислительных задач в области защиты информации; использовать инструментарий операционных систем для проектирования простейших криптографических алгоритмов; • ***владеть*:** практическими навыками применения компьютерных технологий для формирования алгоритмов и проведения вычислений, связанных с защитой информации.
ОПК-8	Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	В результате прохождения практики обучающийся должен: • ***знать*:** 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; • ***уметь*:** правильно строить алгоритмы и компьютерные программы с использованием различных инструментальных средств; • ***владеть*:** языками программирования различного уровня; практическими навыками использования различных систем и методов программирования для решения профессиональных, исследовательских и прикладных задач в области защиты информации.
ОПК-10	Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	В результате прохождения практики обучающийся должен: • ***знать*:** 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; • ***уметь*:** 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; • ***владеть:*** 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..
ПСК-2.1	Способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	В результате прохождения практики обучающийся должен: • ***знать*:** 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*:** анализировать корректность и быстродействие вычислительных алгоритмов, специфичных для перспективных систем защиты информации; • ***владеть*:** практическими навыками построения вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования.

3. Место учебной практики в структуре ООП

Учебная практика относится к базовой части блока 2 «Практики, в том числе научно-исследовательская работа (НИР)» ООП подготовки специалистов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

Логическая и содержательная связь дисциплин и практик, участвующих в формировании представленных в п.2 компетенций, содержится в ниже представленных таблицах:

Компетенция	Предшествующие дисциплины	Данная дисциплина	Последующие дисциплины
ОК-6	− Основы деловых коммуникаций	Учебная практика **2 семестр**	− Производственная практика по получению профессиональных умений и опыта профессиональной деятельности. − Подготовка к процедуре защиты ВКР. − Управление командой.
ОПК-7	− Языки программирования. − Информатика.		− Методы программирования. − Компьютерные сети. − Системы управления базами данных. − Аппаратные средства вычислительной техники. − Системы компьютерной алгебры и реализация криптографических алгоритмов. − Внешний аудит безопасности корпоративных сетей. − Системы тестового вторжения. − Подготовка к процедуре защиты ВКР. − Основы HTML5.
ОПК-8	− Языки программирования		− Методы программирования.. − Операционные системы. − Системы и сети передачи информации. − Компьютерный практикум по криптографии на эллиптических кривых. − Компьютерный практикум по криптографии на гиперэллиптических кривых. − Системы компьютерной алгебры и реали-

			зация криптографических алгоритмов. − Методы алгебраической теории чисел в криптографии. − Методы и алгоритмы генерации эллиптических кривых для криптографии. − Спаривания на эллиптических кривых. − Подготовка к процедуре защиты ВКР.
ОПК-10	− Алгебра. − Информатика.		− Математическая логика и теория алгоритмов. − Быстрые мультипликаторы. − Криптографические методы защиты информации. − Криптографические протоколы. − Методы алгебраической геометрии в криптографии. − Системы компьютерной алгебры и реализация криптографических алгоритмов. − Аналитические методы в задачах защиты информации. − Прикладная алгебра. − Вычислительная алгебра. − Производственная практика (научно-исследовательская работа). − Подготовка к процедуре защиты ВКР.
ПСК-2.1	−		− Методы алгебраической геометрии в криптографии. − Компьютерный практикум по криптографии на эллиптических кривых. − Компьютерный практикум по криптографии на гиперэллиптических кривых. − Методы и алгоритмы генерации гиперэллиптических кривых для криптографии. − Аналитические методы в задачах защиты информации. − Методы алгебраической теории чисел в криптографии. − Функциональные поля и их приложения. − Локальные поля и их приложения. − Методы и алгоритмы генерации эллиптических кривых для криптографии. − Спаривания на эллиптических кривых. − Подготовка к процедуре защиты ВКР.

Компетенция	Предшествующие дисциплины	Данная дисциплина	Последующие дисциплины
ОК-6	− Основы деловых коммуникаций	Учебная практика **4 семестр**	− Производственная практика по получению профессиональных умений и опыта профессиональной деятельности. − Подготовка к процедуре защиты ВКР. − Управление командой.
ОПК-7	− Языки программирования.		− Компьютерные сети.

	− Информатика. − Методы программирования.		− Системы управления базами данных. − Аппаратные средства вычислительной техники. − Системы компьютерной алгебры и реализация криптографических алгоритмов. − Внешний аудит безопасности корпоративных сетей. − Системы тестового вторжения. − Подготовка к процедуре защиты ВКР. − Основы HTML5.
ОПК-8	− Языки программирования. − Методы программирования.		− Операционные системы. − Системы и сети передачи информации. − Компьютерный практикум по криптографии на эллиптических кривых. − Компьютерный практикум по криптографии на гиперэллиптических кривых. − Системы компьютерной алгебры и реализация криптографических алгоритмов. − Методы алгебраической теории чисел в криптографии. − Методы и алгоритмы генерации эллиптических кривых для криптографии. − Спаривания на эллиптических кривых. − Подготовка к процедуре защиты ВКР.
ОПК-10	− Алгебра. − Информатика. − Математическая логика и теория алгоритмов. − Прикладная алгебра. − Вычислительная алгебра.		− Быстрые мультипликаторы. − Криптографические методы защиты информации. − Криптографические протоколы. − Методы алгебраической геометрии в криптографии. − Системы компьютерной алгебры и реализация криптографических алгоритмов. − Аналитические методы в задачах защиты информации. − Производственная практика (научно-исследовательская работа). − Подготовка к процедуре защиты ВКР.
ПСК-2.1	−		− Методы алгебраической геометрии в криптографии. − Компьютерный практикум по криптографии на эллиптических кривых. − Компьютерный практикум по криптографии на гиперэллиптических кривых. − Методы и алгоритмы генерации гиперэллиптических кривых для криптографии. − Аналитические методы в задачах защиты информации. − Методы алгебраической теории чисел в криптографии. − Функциональные поля и их приложения. − Локальные поля и их приложения. − Методы и алгоритмы генерации эллиптических кривых для криптографии. − Спаривания на эллиптических кривых.

			− Подготовка к процедуре защиты ВКР.

Компетенция	Предшествующие дисциплины	Данная дисциплина	Последующие дисциплины
ОК-6	− Основы деловых коммуникаций	Учебная практика **6 семестр**	− Производственная практика по получению профессиональных умений и опыта профессиональной деятельности. − Подготовка к процедуре защиты ВКР. − Управление командой.
ОПК-7	− Языки программирования. − Информатика. − Методы программирования. − Компьютерные сети. − Системы управления базами данных. − Системы компьютерной алгебры и реализация криптографических алгоритмов.		− Аппаратные средства вычислительной техники. − Внешний аудит безопасности корпоративных сетей. − Системы тестового вторжения. − Подготовка к процедуре защиты ВКР. − Основы HTML5.
ОПК-8	− Языки программирования. − Методы программирования. − Операционные системы. − Системы и сети передачи информации. − Системы компьютерной алгебры и реализация криптографических алгоритмов.		− Компьютерный практикум по криптографии на эллиптических кривых. − Компьютерный практикум по криптографии на гиперэллиптических кривых. − Методы алгебраической теории чисел в криптографии. − Методы и алгоритмы генерации эллиптических кривых для криптографии. − Спаривания на эллиптических кривых. − Подготовка к процедуре защиты ВКР.
ОПК-10	− Алгебра. − Информатика. − Математическая логика и теория алгоритмов. − Прикладная алгебра. − Вычислительная алгебра. − Системы компьютерной алгебры и реализация криптографических алгоритмов.		− Быстрые мультипликаторы. − Криптографические методы защиты информации. − Криптографические протоколы. − Методы алгебраической геометрии в криптографии. − Аналитические методы в задачах защиты информации. − Производственная практика (научно-исследовательская работа). − Подготовка к процедуре защиты ВКР.
ПСК-2.1	−		− Методы алгебраической геометрии в криптографии. − Компьютерный практикум по криптографии на эллиптических кривых. − Компьютерный практикум по криптографии на гиперэллиптических кривых. − Методы и алгоритмы генерации гиперэллиптических кривых для криптографии. − Аналитические методы в задачах защиты информации. − Методы алгебраической теории чисел в криптографии. − Функциональные поля и их приложения. − Локальные поля и их приложения.

			− Методы и алгоритмы генерации эллиптических кривых для криптографии. − Спаривания на эллиптических кривых. − Подготовка к процедуре защиты ВКР.

4. Объем практики в зачетных единицах и ее продолжительность в неделях либо в академических или астрономических часах

Учебная практика для обучающихся по специальности 10.05.01 – «Компьютерная безопасность», специализация: «Математические методы защиты информации» проводится во 2, 4 и 6 семестрах в течение 2 недель в каждом; трудоемкость учебной практики – 9 зачетных единиц.

Объём учебной практики	**Всего часов**	
	Контактные часы	**Самостоятельная работа**
Контактная работа обучающихся с преподавателем (самостоятельная работа студента под руководством преподавателя).	216	
Самостоятельная работа обучающихся		105
Промежуточная аттестация – зачет с оценкой	0,75	2,25
Итого	216,75	107,25
Общая трудоемкость практики	324 часа (9 ЗЕ)	

5. Содержание практики

Студенты-практиканты выполняют программу практики в соответствии с планом-графиком практики, утверждаемым руководителем практики.

По итогам практики составляется заключительный отчет, который защищается после окончания практики и утверждается руководителем практики.

Студентам должна быть предоставлена возможность ознакомиться с учебно-научной литературой по теме полученных заданий.

Студенты-практиканты проходят практику в лабораториях компьютерной безопасности и компьютерных классах Института физико-математических наук и информационных технологий. Они должны иметь доступ к программно-техническим комплексам, программным комплексам, математическому обеспечению и техническим средствам, необходимым для выполнения заданий, иметь возможность непосредственных консультаций во время работы с руководителем практики. Практиканты ежедневно работают в течение 3-4 часов в лабораториях и компьютерных классах Института.

Учебная практика состоит в выполнении индивидуальных заданий программно-вычислительного характера по тематике изучаемых дисциплин по заданию руководителя практики и / или реализации небольшого исследовательского проекта в рамках утверждённой темы курсовой работы.

При прохождении учебной практики студенты **изучают**:

- Основные объекты MAPLE.
- Типы переменных.
- Команды преобразования выражений.
- Структура выражений.
- Основные типы данных.
- Операции с векторами и матрицами. Решение задач линейной алгебры.
- Язык MAPLE. Операторы.
- Организация циклических и разветвляющихся вычислительных процессов.
- Процедуры в MAPLE. Локальные и глобальные переменные. Передача параметров.
- Работа с массивами.
- Базовые теоретико-числовые алгоритмы.
- Алгоритмы вычислений в конечных полях.
- Простейшие криптографические алгоритмы.
- Инструментальные средства операционной системы Windows, используемые для защиты информации.
- Свободно распространяемые в Интернете программные средства анализа защищённости компьютерных систем.
- Свободно распространяемые в Интернете программные средства защиты компьютерных систем.

При прохождении учебной практики студенты **разрабатывают** и **исследуют**:

- алгоритмы быстрых вычислений с большими целыми числами;
- методы представления данных в больших конечных полях и алгоритмы быстрых вычислений в таких полях;
- простые алгоритмы и протоколы шифрования на основе целых чисел и конечных полей;
- системы защиты данных, используя встроенные инструментальные средства операционной системы Windows.
- инструментарий и порядок настройки свободно распространяемых в Интернете программных средств анализа защищённости компьютерных систем.
- инструментарий и порядок настройки свободно распространяемых в Интернете программных средства защиты компьютерных систем.

Задание на практику определяется руководителем практики в начале практики. В конце практики студент должен представить результаты практики в виде отчета и сдать его руководителю. Руководитель практики организует защиту отчетов, по результатам которой выставляется промежуточный контроль в виде зачета с оценкой.

Кроме того, при прохождении учебной практики студент обязан:

- пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка, принятого в лабораториях ИФМНиИТ;
- подчиняться действующим в лабораториях правилам внутреннего трудового распорядка;
- изучить и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии.

Особое внимание следует уделить анализу возможности применения результатов практики в качестве вычислительной основы для курсовых работ.

5.1. Примерная тематика заданий по учебной практике по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации»

При прохождении учебной практики возможен следующий перечень **индивидуальных заданий**:

2 семестр

Задание 1.

Условие: Пусть p – простое число, $q = p^m$.

1. Построить конечное поле Φ_q, а именно:
   a. Найти круговой многочлен Φ_{q-1};
   b. Разложить Φ_{q-1} на неприводимые многочлены над подполем Φ_p, выбрать один из этих неприводимых многочленов, обозначить ζ его корень;
   c. Указать базис поля Φ_q над Φ_p;
   d. Построить таблицу индексов поля Φ_q;
   e. Найти все примитивные корни степени $q-1$ из единицы в Φ_q;
   f. Записать группу Галуа $G(\Phi_q / \Phi_p)$;
   g. Указать все подполя поля Φ_q.
2. Указать n-круговое расширения $\mathsf{F}_q^{(n)}$ поля Φ_q.
3. Вычислить $N_{K/k}(\alpha_i)$ и $Tr_{K/k}(\alpha_i)$ для элементов α_i базиса поля Φ_q над Φ_p.
4. Подсчитать квадратичный характер $\chi(x_i)$ элемента $x_i \in \Phi_q$ и вычислить $\sqrt{x_i}$ в поле Φ_q, если это возможно.
5. Пусть s – простое число. Подсчитать квадратичный характер $\chi(y_i)$ элемента $y_i \in \Phi_s$ и вычислить $\sqrt{y_i}$ в поле Φ_s, если это возможно.

Варианты заданий:

№	p	m	n	x_1	x_2	x_3	s	y_1	y_2	y_3
1	2	7	81	ζ	$\zeta^3+\zeta$	$\zeta^5+\zeta^2+1$	151	2	3	5
2	3	4	80	ζ	$\zeta^3+\zeta$	$\zeta^3+\zeta+2$	157	5	7	8
3	5	3	79	ζ	ζ^2+3	$\zeta^2+\zeta+2$	163	10	11	52
4	7	2	78	ζ	$\zeta+3$	$\zeta+6$	167	13	14	15
5	11	2	76	ζ	$\zeta+3$	$\zeta+6$	173	17	38	19
6	13	2	75	ζ	$\zeta+3$	$\zeta+6$	179	20	21	22
7	2	7	83	$\zeta+1$	$\zeta^4+\zeta$	$\zeta^5+\zeta^3+1$	181	23	39	26
8	3	4	85	$\zeta+1$	$\zeta+2$	$\zeta^3+2\zeta+2$	191	27	28	29
9	5	3	84	$\zeta+1$	$\zeta+2$	$\zeta^2+\zeta+3$	193	30	31	32
10	7	2	86	$\zeta+1$	$\zeta+4$	$2\zeta+1$	197	33	34	35

Задание 2.

Условие: Построить криптосистему в заданном диапазоне параметров, т.е. выбрать:

- алфавит,
- шифровальный ключ,
- дешифровальный ключ,
- длину единичных сообщений исходного текста,
- длину единичных сообщений зашифрованного текста,
- подходящее кольцо Z/nZ или конечное поле Φ_q.

Зашифровать и расшифровать собственное имя и фамилию.

Для системы Diffie-Hellman'а построить конечное поле и найти общий секретный ключ для организации приватной криптосистемы.

Варианты заданий:

1. RSA – криптосистема,
   - число символов алфавита N: $15 \le N \le 20$,
   - длина единичного сообщения исходного текста $m = 2$,
   - длина единичного сообщения зашифрованного текста $l = 3$.

2. RSA – криптосистема,
   - число символов алфавита N: $100 \le N \le 150$,
   - длина единичного сообщения исходного текста $m = 1$,
   - длина единичного сообщения зашифрованного текста $l = 2$

3. RSA – криптосистема,
   - число символов алфавита N: $21 \le N \le 25$,
   - длина единичного сообщения исходного текста $m = 2$,
   - длина единичного сообщения зашифрованного текста $l = 3$.

4. Криптосистема Massey – Omur'ы,
   - число символов алфавита N: $15 \le N \le 20$,
   - длина единичного сообщения $m = 2$,
   - $p = \text{char}\,\Phi_q = 2$.

5. Криптосистема ElGamal,
   - число символов алфавита N: $15 \le N \le 20$,
   - длина единичного сообщения $m = 2$,
   - $p = \text{char}\,\Phi_q = 2$.

6. Криптосистема Massey – Omur'ы,
   - число символов алфавита N: $15 \le N \le 20$,
   - длина единичного сообщения $m = 2$,
   - $p = \text{char}\,\Phi_q = 3$.

7. Система Diffie – Hellman'а,
   - конечное поле Φ_q, $p = \text{char}\,\Phi_q = 3$, $200 \le q \le 250$,
   - примитивный корень $g = \xi$ – корень неприводимого многочлена, с помощью которого строится поле Φ_q,
   - $50 \le a \le 60$, $100 \le b \le 110$.

8. Матричную криптосистему:
   - число символов алфавита N: $51 \le N \le 70$,
   - длина единичного сообщения $m = 3$,

- шифровальный ключ $k = (A, B)$, $A = \begin{pmatrix} 32 & 12 & 7 \\ 18 & 39 & 0 \\ 4 & 49 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 43 \\ 14 \\ 7 \end{pmatrix}$

9. Матричную криптосистему:
   - число символов алфавита N: $45 \le N \le 50$,
   - длина единичного сообщения $m = 3$,
   - шифровальный ключ $k = (A, B)$, $A = \begin{pmatrix} 12 & 26 & 17 \\ 0 & 13 & 10 \\ 4 & 48 & 23 \end{pmatrix}$, $B = \begin{pmatrix} 23 \\ 18 \\ 37 \end{pmatrix}$

10 Криптосистема Massey – Omur'ы,
   - число символов алфавита N: $21 \le N \le 25$,
   - длина единичного сообщения $m = 2$,
   - $p = \text{char } \Phi_q = 3$.

4 семестр

Задание.

Условие: Выполнить
- описание используемого программного инструмента (функции, структура, возможности, натройка);
- разработать не менее 5 примеров его использования;
- выполнить анализ (желательно сравнительный) эффективности рассматриваемого инструмента.

Варианты заданий

1. Использование объектов парольной политики (Password Settings Objects, PSOs) в домене Windows Server 2008 R2 или 2012 R2 для формирования различных требований к паролям у разных категорий пользователей. *Источники:*
   a. Configuring Granular Password Settings in Windows Server 2008, Part 1
   b. Configuring Granular Password Settings in Windows Server 2008, Part 2
   c. Configuring Fine-Grained Password Policies in Windows Server 2012
   d. AD DS: Fine-Grained Password Policies
   e. AD DS Password Fine-Grained and Account Lockout Policy Step-by-Step Guide
   f. Черновая версия моего конспекта по Active Directory в WS 2008 R2

2. Использование контроллеров домена, доступных только для чтения (read-only domain controllers, RDOCs) для снижения угроз информационной безопасности на подразделениях предприятия, где не удаётся обеспечить надлежащий уровень защиты сети и оборудования. *Источники:*
   a. Read-Only Domain Controllers Step-by-Step Guide (всё не надо, только установка и администрирование)
   b. RODC Installation
   c. RODC Administration
   d. Черновая версия моего конспекта по Active Directory в WS 2008 R2

3. Обзор и анализ основных возможностей Центра сертификации Active Directory. *Источники:*
    a. Глава 15 (Chapter 15) из этой книги: Holme, Ruests, Kellington - Configuring WS 2008 AD DS
4. Обзор и анализ основных возможностей программы Symantech Endpoint Protection. *Источники:*
    a. Ознакомительный ролик
    b. Встроенная справка
5. Обзор и анализ основных возможностей программы PGP Desktop (качать отсюда). *Источники:*
    a. Многочисленные обучающие руководства в Интернете.
    b. Встроенная справка.
6. Освоение метода шифрования данных на жёстком диске с помощью технологии BitLocker. *Источники:*
    a. Что такое BitLocker
    b. BitLocker. вопросы и ответы
    c. Пошаговое руководство по шифрованию диска с помощью BitLocker
7. Установка и настройка службы обновлений Windows Server (Windows Server Update Services) в локальной сети. *Источники:*
    a. Пошаговое руководство
    b. Многочисленные обучающие ролики на YouTube
8. Настройка политики аудита и расширенного аудита в Windows. *Источники:*
    a. Managing Security Auditing
    b. Использование аудита для отслеживания действий пользователей
    c. Черновая версия моего конспекта по Active Directory в WS 2008 R2
9. Обзор и анализ способов и средств по взлому паролей в беспроводных сетях. *Источники:*
    a. Главы 3 и 4 из этой книги.
    b. Глава 14 из этой книги.
10. Базовые классы .NET Framework, реализующие операции шифрования, цифровой подписи и ключевого обмена. *Источники:*
    a. .NET Framework Cryptography Model

6 семестр

Задание.

Условие: Выполнить
- описание используемого программного инструмента или программно-аппаратного средства (функции, структура, возможности, натройка);
- разработать не менее 5 примеров его использования;
- выполнить анализ (желательно сравнительный) эффективности рассматриваемого инструмента или программно-аппаратного средства.

Варианты заданий:

1. Настройка и работа с персональным средством криптографической защиты информации “Шипка”. *Источники:*
    a. Руководство по эксплуатации к устройству.
2. Настройка и работа с программно-аппаратным средством защиты информации от несанкционированного доступа “Аккорд”. *Источники:*
    a. Руководство по эксплуатации к устройству.
3. Настройка и работа с программным средством защиты информации от несанкционированного доступа Dallas Lock. *Источники:*
    a. Встроенная справка.
4. Настройка и работа со сканером сетевой безопасности XSpider. *Источники:*
    a. Встроенная справка.
5. Обзор популярных библиотек языка Python, предназначенных для выполнения криптографических операций (*Для тех, кто знаком с программированием на Python*). Например, можно рассмотреть такие библиотеки:
    a. pyca/cryptography: https://cryptography.io/en/latest/
    b. PyNaCl: https://pynacl.readthedocs.io/en/stable/
    c. PyCryptodome: https://www.pycryptodome.org/en/latest/
6. Освоение основных методов по подбору пароля для доступа к беспроводной сети, защищённой технологией WPA2 (*Для тех, кто интересуется защитой в Wi-Fi*). Можно рассмотреть, например, популярную утилиту aircrack-ng в Kali Linux, которая работает в “содружестве” с airmon-ng и airodump-ng, можно использовать и другие программы. В Интернете информации по этой теме очень много, да и сама тема уже стала классикой. Следует набрать в поиске Google фразу “wlan kali linux” -- и получите тысячу ссылок на обучающие руководства и видеоуроки по теме “как взломать Wi-Fi”.
7. Освоение защиты веб-сервера с помощью WAF ModSecurity (*Для тех, кого интересует веб-разработки*). Нужно не просто перечислить шаги по настройке этого средства для какого-либо веб-сервера, а установить на своём ПК какой-нибудь веб-сервер (например, Apache), “прикрутить” к нему это расширение и проверить, как оно работает.
8. Настройка SSH-сервера в операционной системе Linux для организации удалённой работы с терминалом (*Для тех, кто интересуется удалённой работой с Linux через PuTTY.*). Иными словами, настроить сервер SSH в Linux (например, Open SSH) и клиент SSH в Windows (например, PuTTY), чтобы из Windows можно было удалённо работать с терминалом Linux. Наберите в Google фразу “ssh ubuntu putty” или “ssh debian putty”.
9. Реализация стандартных криптографических процедур на языке C# с использованием базовых классов .NET Framework (*Для тех, кто знаком с программированием на C#*). Зашифровать / расшифровать файл, вычислить для него хэш и создать к нему, а потом проверить цифровую подпись, используя классы стандартной библиотеки .NET

(они, подсказываю, находятся в пространстве имён `System.Security.Cryptography`).

10. Реализация стандартных криптографических процедур на языке Java с использованием классов стандартной библиотеки Java (*Для тех, кто знаком с программированием на Java.*). Зашифровать / расшифровать файл, вычислить для него хэш и создать к нему, а потом проверить цифровую подпись, используя классы стандартной библиотеки Java (JCA -- Java Cryptography Architecture).

5.2. Краткий план-график учебной практики

№ п/п	Этапы (периоды) практики	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
1	Организационно-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.	4	Запись в журнале по технике безопасности о прохождении соответствующего инструктажа, подписанное задание на учебную практику
2	Основной 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.	86	Письменный отчет о прохождении практики.
3	Заключительный этап	1. Подготовка отчета по учебной практике, представления отчета и прилагаемых документов для защиты. 2. Прохождение промежуточной аттестации по результатам прохождения практики.	18	Отчет по практике, отзыв руководителя о ра-

№ п/п	Этапы (периоды) практики	Вид работ	Трудоемкость (в часах)	Форма текущего контроля
				боте практиканта. Ведомость с дифференцированной оценкой за учебную практику.
	Итого часов		**108**	

6. Формы отчетности по практике

Формы отчетности студентов по учебной практике (заверенные подписью руководителя практики):

- индивидуальное задание на практику;
- рабочий график (план) на практику;
- отчет о результатах прохождения практики.

Формы отчетности руководителя практики:

- не позднее 1 месяца после окончания практики предоставляет в институт отчет о проведенной учебной практике;
- предоставляет отзыв о работе каждого студента-практиканта на практике.

Оформление результатов практики

По окончании учебной практики студент обязан составить письменный отчет и сдать его руководителю практики. Отчет о практике должен содержать сведения о конкретной выполненной студентом запланированной работе (в соответствии с индивидуальным заданием на практику) в период прохождения практики.

Для оформления отчета студенту выделяется в конце практики 2 дня.

Требования, предъявляемые к оформлению отчета по учебной практике

Отчет по учебной практике должен состоять из Оглавления, Введения, описание основной части отчета (содержания практики), Заключения, Списка цитированной литературы.

Описание основной части отчета по учебной практике должно содержать:

– задание на учебную практику, полученное от руководителя;

- план-график прохождения учебной практики;

– описание выполнения заданий, а также текущих поручений руководителя практики.

Рекомендуемый объем отчета не менее 10 страниц. Образец титульного листа прилагается (Приложение 1). Переплет отчета может быть произвольным и исключать рассыпание листов. Оформление отчета – см. Приложение 3.

Порядок аттестации студентов по результатам практики

По окончании учебной практики студент сдают отчёт по практике на проверку руководителю практики. После получения отчёта студента руководитель практики оценивает проделанную в ходе практики работу и дает отзыв на неё. В случае положительного отзыва защита отчета осуществляется перед руководителем практики на ***дифференцированном зачёте***. По результатам защиты выставляется оценка.

При проведении зачета используются следующие критерии итоговой оценки за учебную практику:

- полный и аккуратно оформленный в соответствии с требованиями отчет;
- верные результаты проделанных расчётов;
- наличие разработанного и успешно протестированного программного продукта, реализующего вычислительные алгоритмы или отдельные аспекты безопасности компонент компьютерной системы;
- правильные ответы студента на вопросы преподавателя, касающиеся предмета практики.

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

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной практики

Компетенция	**Этапы формирования компетенции**	**Показатели оценивания компетенции**	**Критерии оценивания компетенций**	**Шкала оценивания**	**Виды аттестации и виды оценочных средств**
ОК-6 Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Начальный этап	***знать*:** нормы корректного поведения в обществе; социально-культурные характеристики основных этносов; ***уметь*:** толерантно воспринимать социальные, этнические, конфессиональные и культурные различия лю-	Обучающийся ***на продвинутом уровне*** демонстрирует: Знание норм корректного поведения в обществе; социально-культурных характеристик основных этносов, принципов функционирования команд / коллективов работников; Умение 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;	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет

		дей и на этой основе грамотно строить взаимоотношения с членами трудового коллектива; планировать и осуществлять производственную деятельность в коллективе; ***владеть*:** навыками урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий при планировании и реализации производственной деятельности трудового коллектива.	Владение практическими навыками урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий при планировании и реализации производственной деятельности трудового коллектива.		
			Обучающийся ***на высоком уровне*** демонстрирует: Знание норм корректного поведения в обществе; ряда социально-культурных характеристик основных этносов, некоторых принципов функционирования команд / коллективов работников; Умение толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей; планировать и осуществлять производственную деятельность в коллективе; Владение некоторыми практическими навыками урегулирования возникающих противоречий между членами трудового коллектива; навыками применения методики учёта социально культурных различий.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: Знание основных норм корректного поведения в обществе; отдельных социально-культурных характеристик основных этносов, отдельных принципов функционирования команд / коллективов работников; Умение в основном толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей; осуществлять производственную деятельность в коллективе; Владение практическими навыками избегать возникающие противоречия между членами трудового коллектива; отдельными навыками применения методики учёта социально культурных различий.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: Незнание социально-культурных характеристик основных этносов, принципов функционирования команд / коллективов работников; Неумение толерантно воспринимать социальные, этнические, конфессиональные и культурные различия людей; осуществлять производственную деятельность в коллективе; избегать возникающих противоречий между членами трудового коллектива.	< 50%	
ОПК-7 Способность учитывать современные	Промежуточный этап	***знать*:** современные информационные методики и технологии; перечень и возможно-	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** современных информационных методик и технологий; перечней и возможностей распространённых систем компьютерной алгебры; ме-	от 85% до 100%	Отчет по практике Отзыв руководителя

тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		сти распространённых систем компьютерной алгебры; методы математической обработки информации, используемые при решении задач защиты информации; ***уметь*:** грамотно применять математические пакеты компьютерной алгебры для решения вычислительных задач в области защиты информации; использовать инструментарий операционных систем для проектирования простейших криптографических алгоритмов; ***владеть*:** практическими навыками применения компьютерных технологий для формирования алгоритмов и проведения вычислений, связанных с защитой информации.	тодов математической обработки информации, используемые при решении задач защиты информации; ***умение*** грамотно применять математические пакеты компьютерной алгебры для решения вычислительных задач в области защиты информации; использовать инструментарий операционных систем для проектирования простейших криптографических алгоритмов; ***владение практическими навыками*** применения компьютерных технологий для формирования алгоритмов и проведения вычислений, связанных с защитой информации.		практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** основных информационных методик и технологий; перечней и возможностей отдельных систем компьютерной алгебры; основных методов математической обработки информации, используемые при решении задач защиты информации; ***умение*** применять математические пакеты компьютерной алгебры для решения основных вычислительных задач в области защиты информации; использовать основной инструментарий операционных систем для проектирования простейших криптографических алгоритмов; ***владение практическими навыками*** применения некоторых компьютерных технологий для формирования алгоритмов и проведения вычислений, связанных с защитой информации.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных информационных методик и технологий; перечней и возможностей, по крайней мере, одной из систем компьютерной алгебры; отдельных методов математической обработки информации, используемые при решении задач защиты информации; ***умение*** применять математические пакеты компьютерной алгебры для решения отдельных вычислительных задач в области защиты информации; ***владение практическими навыками*** применения отдельных компьютерных технологий для формирования алгоритмов и проведения вычислений, связанных с защитой информации.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** информационных методик и технологий; перечней и возможностей систем компьютерной алгебры; методов математической обработки информации; ***неумение*** применять математические пакеты	< 50%	

			компьютерной алгебры для решения вычислительных задач в области защиты информации; использовать инструментарий операционных систем для проектирования криптографических алгоритмов; ***отсутствие практических навыков*** применения компьютерных технологий для формирования алгоритмов и проведения вычислений, связанных с защитой информации.		
ОПК-8 Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Промежуточный этап	***знать*:** 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; ***уметь*:** правильно строить алгоритмы и компьютерные программы с использованием различных инструментальных средств; ***владеть*:** языками программирования различного уровня; практическими навыками использования различных систем и методов программирования для решения профессиональных, исследовательских и прикладных задач в области защиты информации.	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** языков программирования различного уровня, их назначения и возможностей; систем и методов построения компьютерных программ для задач защиты информации; перечней и возможностей современных инструментальных средств решения задач в области информационной безопасности; ***умение*** правильно строить алгоритмы и компьютерные программы с использованием различных инструментальных средств; ***Владение практическими навыками*** использования языков программирования различного уровня; использования различных систем и методов программирования для решения профессиональных, исследовательских и прикладных задач в области защиты информации.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** отдельных языков программирования различного уровня; систем и методов построения компьютерных программ для задач защиты информации; возможностей отдельных инструментальных средств решения задач в области информационной безопасности; ***умение*** строить алгоритмы и компьютерные программы с использованием некоторых инструментальных средств; ***Владение практическими навыками*** использования некоторых языков программирования; использования некоторых систем и методов программирования для решения профессиональных, исследовательских и прикладных задач в области защиты информации.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных языков программирования различного уровня; систем и методов построения компьютерных программ для отдельных задач защиты информации; ***умение*** строить алгоритмы и компьютерные программы с использованием отдельных инструментальных средств; ***Владение практическими навыками*** использо-	от 50% до 70%	

			вания отдельных языков программирования; использования отдельных систем и методов программирования для решения прикладных задач в области защиты информации.		
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** языков программирования; систем и методов построения компьютерных программ для задач защиты информации; незнание инструментальных средств решения задач в области информационной безопасности; ***неумение*** строить алгоритмы и компьютерные программы; ***Отсутствие практических навыков*** использования языков программирования; использования систем и методов программирования для решения задач в области защиты информации.	< 50%	
ОПК-10 Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Промежуточный этап	***знать*:** 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; ***уметь*:** 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	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** математических моделей преобразования информации в компьютерных системах; алгоритмов обработки информации в её представления на языках программирования высокого уровня; блоков и структуры алгоритмов, реализуемых на языках программирования высокого уровня; ***умение*** строить эффективные вычислительные алгоритмы, используя численные методы моделирования физических явлений и процессов; строить эффективные 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; ***Владение практическими 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.	от 85% до 100%	Отчет по практике Отзыв руководителя практики Дифференцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** основных математических моделей преобразования информации в компьютерных системах; основных алгоритмов обработки информации в её представления на языках программирования высокого уровня; основных блоков и структуры алгоритмов, реализуемых на языках программирования высокого уровня; ***умение*** строить вычислительные алгоритмы, используя численные методы моделирования	от 70% до 85%	

		алгоритма, включая анализ быстродействия и объём необходимой памяти; ***владеть:*** 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..	физических явлений и процессов; строить вычислительные алгоритмы на алгебраических структурах с помощью систем компьютерной алгебры; проводить анализ вычислительной эффективности алгоритма; ***Владение практическими навыками*** написания алгоритмов на отдельных языках программирования высокого уровня; навыками реализации алгоритмов с помощью, по крайней мере, одной из систем компьютерной алгебры; навыками анализа вычислительной эффективности алгоритмов.		
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных математических моделей преобразования информации в компьютерных системах; отдельных алгоритмов обработки информации в её представления на языках программирования высокого уровня; ***умение*** строить отдельные вычислительные алгоритмы, используя численные методы моделирования физических явлений и процессов; строить вычислительные алгоритмы на алгебраических структурах с помощью систем компьютерной алгебры; ***Владение практическими навыками*** написания алгоритмов на отдельных языках программирования высокого уровня; навыками реализации алгоритмов с помощью, по крайней мере, одной из систем компьютерной алгебры.	от 50% до 70%	
			Обучающийся ***на низком уровне*** демонстрирует: ***незнание*** математических моделей преобразования информации в компьютерных системах; алгоритмов обработки информации; ***неумение*** строить вычислительные алгоритмы, используя численные методы моделирования физических явлений и процессов; строить вычислительные алгоритмы на алгебраических структурах; проводить анализ вычислительной эффективности алгоритма; ***Отсутствие практических навыков*** написания алгоритмов на языках программирования высокого уровня; навыков реализации алгоритмов с помощью математических пакетов; навыков анализа вычислительной эффективности алгоритмов.	< 50%	
ПСК-2.1 Способность разрабатывать вычислительные алгоритмы,	Промежуточный этап	***знать*:** перспективные методы криптографической защиты информации и помехоустойчивого кодирования; принципы	Обучающийся ***на продвинутом уровне*** демонстрирует: ***знание*** перспективных методов криптографической защиты информации и помехоустойчивого кодирования; принципов функционирования и возможностей перспективных инструментальных средств и компьютерных технологий для реали-	от 85% до 100%	Отчет по практике Отзыв руководителя практики Диффе-

реализующие современные математические методы защиты информации		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*:** анализировать корректность и быстродействие вычислительных алгоритмов, специфичных для перспективных систем защиты информации; ***владеть*:** практическими навыками построения вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования.	зации вычислительных алгоритмов; структуры данных и методов построения вычислительных алгоритмов в алгебраических структурах, специфичных для перспективных систем защиты информации; ***умение*** анализировать корректность и быстродействие вычислительных алгоритмов, специфичных для перспективных систем защиты информации; ***Владение практическими навыками*** построения вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования.		ренцированный зачет
			Обучающийся ***на высоком уровне*** демонстрирует: ***знание*** ряда методов криптографической защиты информации и помехоустойчивого кодирования; основных принципов функционирования и возможностей ряда инструментальных средств и компьютерных технологий для реализации вычислительных алгоритмов; структуры данных и методов построения ряда вычислительных алгоритмов в алгебраических структурах, специфичных для систем защиты информации; ***умение*** анализировать корректность и быстродействие ряда вычислительных алгоритмов, специфичных для перспективных систем защиты информации; ***Владение практическими навыками*** построения ряда вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования.	от 70% до 85%	
			Обучающийся ***на среднем уровне*** демонстрирует: ***знание*** отдельных методов криптографической защиты информации и помехоустойчивого кодирования; возможностей отдельных инструментальных средств и компьютерных технологий для реализации вычислительных алгоритмов; структуры данных и методов построения отдельных вычислительных алгоритмов в алгебраических структурах, специфичных для перспективных систем защиты информации; ***умение*** анализировать корректность и быстродействие ряда вычислительных алгоритмов, специфичных для систем защиты информации; ***Владение практическими навыками*** построения отдельных вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования.	от 50% до 70%	
			Обучающийся ***на низком уровне***	< 50%	

			демонстрирует: ***незнание*** методов криптографической защиты информации и помехоустойчивого кодирования; принципов функционирования и возможностей инструментальных средств и компьютерных технологий для реализации вычислительных алгоритмов; структуры данных и методов построения вычислительных алгоритмов в алгебраических структурах; ***неумение*** анализировать корректность и быстродействие вычислительных алгоритмов; ***Отсутствие практических навыков*** построения вычислительных алгоритмов в алгебраических структурах.		

Указанные компетенции формируются у студентов в процессе прохождения учебной практики. Формой текущего контроля за сформированностью компетенций является написание отчета по учебной практике.

7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкалы оценивания

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания приведены в п. 7.1.

Для оценивания уровня сформированности компетенций используется следующая шкала, где оценки определяются по результатам (R), полученным во время аттестации, для каждой из компетенций исходя из следующих условий:

- «отлично»: $R \geq 85$ %;
- «хорошо»: $70 \leq R < 85$ %;
- «удовлетворительно»: $50\ \% \leq R < 70$ %;
- «неудовлетворительно»: $R < 50$ %.

Далее рассчитывается итоговая оценка (S) по следующей формуле:

$$S = \frac{\sum_{k=0}^{n} R_k}{n},$$

где: R_k – оценка по k-ой компетенции, n – общее количество оцениваемых компетенций.

В качестве оценки за зачет с оценкой выставляется следующая, в зависимости от полученного значения S:

- «отлично»: $S \geq 85$ %;
- «хорошо»: $70\ \% \leq S < 85$ %;
- «удовлетворительно»: $50\ \% \leq S < 70$ %;
- «неудовлетворительно»: $S < 50$ %.

7.3. Комплект оценочных средств по всем заявленным в рабочей программе видам занятий и самостоятельной работы обучающихся

В комплект оценочных средств входят оценочные средства по контролю промежуточной

аттестации обучающихся по всем заявленным в рабочей программе видам работ обучающихся:

- индивидуальные задания для прохождения практики;
- контрольные вопросы к дифференцируемому зачету;
- отзыв руководителя практики;
- отчет студента о прохождении практики.

Примерные контрольные вопросы к дифференцированному зачету по практике:

1. Сформулировать задачи, решаемые в процессе практики.
2. Какие языки программирования использовались? Каковы возможности и ограничения в использовании этих языков?
3. Какие инструментальные средства операционной системы использовались? Каковы возможности и ограничения в использовании этих средств?
4. Какие системы программирования и пакеты программ использовались?
5. Какие программно-аппаратные средства защиты информации использовались? Каковы их основные характеристики?
6. Какие свободно распространяемые средства анализа защищённости компьютерных систем использовались? Каковы их возможности и ограничения?
7. Какие свободно распространяемые средства защиты компьютерных систем использовались? Каковы их возможности и ограничения?
8. Представить описание разработанных вычислительных алгоритмов.
9. Обосновать оценки вычислительной сложности разработанных алгоритмов.
10. Представить схемы разработанных программных комплексов.
11. Представить результаты расчёта числовых примеров.
12. Дать анализ полученных численных результатов.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка сформировавшихся компетенций по учебной практике проводится в форме текущей и промежуточной аттестации.

Текущий контроль осуществляется руководителем практики. Руководитель практики контролирует выполнение индивидуального задания на практику.

Промежуточный контроль осуществляется на дифференцированном зачете.

На зачет студенты предоставляют следующие документы, заверенные подписью руководителя практики:

- индивидуальное задание на практику;
- отчет о результатах прохождения практики.

Защита отчета осуществляется перед руководителем практики.

Критерии выставления итоговой оценки- см. п . 7.2.

8. Перечень учебной литературы и ресурсов сети Интернет, необходимых для проведения практики

8.1. Основная литература

1. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. - Ч. 1: Алгебраические методы on-line, 156 с.. - Библиогр.: с. 151-153. - ISBN 978-5-9971-0391-0: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)
2. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. - Ч. 4: Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых on-line, 60 с.. - Библиогр.: с. 58-59. - ISBN 978-5-9971-0389-7: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)
3. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы/ А. А. Болотов [и др.]. - 2-е изд., доп.. - М.: КомКнига, 2012. - 355 с.: граф., табл.. - (Защита информации). - Вариант загл.: Алгебраические и алгоритмические основы. - Библиогр.: с. 312-320 (187 назв.) - Предм. указ.: с. 321-324. - ISBN 978-5-484-01290-9: 401.00, 401.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 12: УБ(11), ч.з.N3(1)

8.2. Дополнительная литература

1. Абрамов, С. А. Лекции о сложности алгоритмов: учеб. пособие для вузов/ С. А. Абрамов. - 2-е изд., перераб.. - Москва: МЦНМО, 2012. - 245 с. - (Современные лекционные курсы). - Библиогр.: с. 236-240 (68 назв.). - Предм. указ.: с. 241-242. - ISBN 978-5-4439-0204-3: 266.00, 266.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 12: УБ(11), ч.з.N3(1)
2. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. Ч. 3: Вычислительный практикум по числовым полям и криптографии в квадратичных полях on-line, 93 с.. - Библиогр. в конце кн.. - ISBN 978-5-9971-0388-0: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)
3. Быстрые мультипликаторы [Электронный ресурс]: учеб.-метод. комплекс/ сост. Е. С. Алексеенко. - Калининград: БФУ им. И. Канта, 2015. - 1 on-line, 95 с.. - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)
4. Введение в теоретико-числовые методы криптографии: учеб. пособие/ М. М. Глухов [и др.]. - СПб.; М.; Краснодар: Лань, 2011. - 400 с. - (Учебники для вузов. Специальная литература). - Библиогр.: с. 382-389. - ISBN 978-5-8114-1116-0: 695.64, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
5. Защита информации [Электронный ресурс]: учеб. пособие для вузов/ А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 2-е изд.. - Москва: РИОР; Москва: ИНФРА-М, 2015. - 1 эл. опт. диск (CD-ROM), 391, [1]: ил. - (Высшее образование - бакалавриат). - Библиогр.: с. 386-389 (55 назв.). - Лицензия до 23.06.2020 г.. - Соответствует ФГОС (третьего поколения). - ISBN 978-5-369-01378-6. - ISBN 978-5-16-010188-0: 15100.00 р. Имеются экземпляры в отделах /There are copies in departments: всего /all 2: ЭБС Кантиана(1), ч.з.N1(1)
6. Нестеренко, Ю. В. Теория чисел: учеб. для вузов/ Ю. В. Нестеренко. - М.: Академия, 2008. - 264, [1] с. - (Высшее профессиональное образование. Физико-математические науки). - (Учебник). - Библиогр.: с. 262 (17 назв.). - ISBN 978-5-7695-4646-4: 354.53, 354.53,

514.80, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 16: ч.з.N3(1), УБ(15)
7. Основы информационной безопасности: учеб. пособие/ Е. Б. Белов [и др.]. - М.: Горячая линия-Телеком, 2006. - 544 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр. в конце частей. - ISBN 5-93517-292-5: 316.25, 351.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 16: УБ(14), ч.з.N3(1), НА(1)
8. Проскурин, В. Г. Защита в операционных системах: учеб. пособие для вузов/ В. Г. Проскурин. - Москва: Горячая линия-Телеком, 2014. - 192 с.. - Библиогр.: с. 189-190. - ISBN 978-5-9912-0379-1: 392.15, 392.15, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 10: УБ(9), ч.з.N3(1)
9. Платонов, В. В. Программно-аппаратные средства защиты информации: учеб. для вузов/ В. В. Платонов. - 2-е изд., стер.. - Москва: Академия, 2014. - 330, [1] с.: табл.. - (Высшее образование. Информационная безопасность). - (Бакалавриат). - Библиогр.: с. 326-327. - ISBN 978-5-4468-1302-5: 880.03, 888.03, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 10: УБ(9), ч.з.N3(1)
10. Смарт, Н. Криптография/ Н. Смарт ; пер. с англ. С. А. Кулешов под ред. С. К. Ландо. - Москва: Техносфера, 2006. - 525 с. - (Мир программирования). - Предм. указ.: с. 524-525. - ISBN 5-94836-043-1: 314.05, 370.00, 314.05, 454.96, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 17: УБ(15), НА(2)
11. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие / П. Б. Хорев. - 2-е изд., стер.. - М.: Академия, 2006. - 255 с.: ил., табл.. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 251-252 (28 назв.). - ISBN 5-7695-3288-2 : 197.60, 197.60, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 18: УБ(16), ч.з.N3(1), НА(1)

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для выполнения учебной практики

1. http://xn--90ax2c.xn--p1ai/ – «Национальная электронная библиотека».
2. http://lib.kantiana.ru/irbis/standart/ELIB – ЭБС Кантиана.
3. http://elibrary.ru/defaultx.asp – Научная электронная библиотека eLIBRARY.RU.
4. https://www.coursehero.com/file/p7t1rf7/External-links-Certicom-ECC-Tutorial-http-www-certicom-com-index-php-ecc/ - Online Elliptic Curve Cryptography Tutorial, Certicom Corp.
5. https://technet.microsoft.com/ru-ru/library/cc753471%28v=ws.10%29.aspx – Справочник по синтаксису ADMX групповой политики.
6. http://windows.microsoft.com/ru-ru/windows/protect-files-bitlocker-drive-encryption#1TC=windows-8, - Защита файлов с помощью шифрования дисков BitLocker в Windows 8.
7. http://winitpro.ru/index.php/2010/12/14/vklyuchaem-bitlocker-to-go-v-windows-7/ - защита файлов с помощью шифрования дисков BitLocker в Windows 7.
8. http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/ - ащита файлов с помощью шифрования дисков BitLocker в Windows 8.1 и 10.
9. http://interface31.ru/tech_it/2010/11/windows-server-sozdanie-avtonomnogo-centra-sertifikacii.html - Создание автономного центра сертификации. Windows Server.

10. http://interface31.ru/tech_it/2010/11/zashhita-rdp-soedineniya-pri-pomoshhi-ssl.html - защита RDP-соединения при помощи SSL.
11. http://interface31.ru/tech_it/2014/07/windows-server-2012-ustanovka-i-nastroyka-wsus.html - Windows Server 2012 – установка и настройка WSUS.
12. http://www.acronis.com/ru-ru/business/backup-advanced/workstation/ - резервное копирование для защиты данных.
13. https://msdn.microsoft.com/en-us/library/bb510589%28v=sql.120%29.aspx – Security Center for SQL Server Database Engine and Azure SQL Database.
14. http://dorlov.blogspot.ru/p/blog-page_3151.html - Перечень сайтов по информационной безопасности.
15. http://lib.itsec.ru/articles2/allpubliks - Форум по информационной безопасности.
16. http://www.securitylab.ru – Информационный сайт по компьютерной безопасности.

9. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

9.1. Перечень программного обеспечения (используемое при необходимости)

Windows 7 Pro 32-bit SP1 –договор №1980/12 14.12.2012 ООО "ЭСЭМДЖИ", акт АА-118 от 21.12.2012
Entity Framework 6.1.3 Tools for Visual Studio 2015- договор № 494/12 от 4.04.12 ЗАО "СофтЛайн Трейд"
LibreOffice 5.0.2.2 общественная лицензия MPL 2.0
Microsoft Visual Studio Professional 2015- договор № 494/12 от 4.04.12 ЗАО "СофтЛайн Трейд"

9.2. Информационные справочные системы

1. http://xn--90ax2c.xn--p1ai/ – «Национальная электронная библиотека».
2. http://lib.kantiana.ru/irbis/standart/ELIB – ЭБС Кантиана.
3. http://elibrary.ru/defaultx.asp – Научная электронная библиотека eLIBRARY.RU.
4. http://ibooks.ru/ – ЭБС «Айбукс.ру/ibooks.ru».
5. http://www.iprbookshop.ru/ – ЭБС «IPRbooks».
6. http://e.lanbook.com/ – Издательство «Лань», ЭБС.
7. http://infomag.biz/index.php – Служба ИНФОМАГ - Библиографическая и другая научная информация, в первую очередь оглавления научных и технических журналов, а также зарубежных научных электронных бюллетеней.
8. http://window.edu.ru/ – Информационная система «Единое окно доступа к образовательным ресурсам».
9. http://www.rsl.ru/ – Российская государственная библиотека
10. http://www.biblioclub.ru/ – Университетская библиотека онлайн

10. Описание материально-технической базы, необходимой для проведения прак-

тики

Класс персональных компьютеров, объединенных в локальную сеть с выходом в сеть Интернет. Стандартное программное обеспечение. Программные продукты, указанные в п.11.1.

Учебный дисплейный класс (аудитории №№ 214, 220, 230а и 235 Учебного корпуса №2 БФУ им.И.Канта), в которых установлены персональные компьютеры с параметрами - Intel Core I3-3220, 3.3 GHz, 4Gb RAM, 1 Tb HDD, 21,5", keyboard, Mouse, LAN, Internet access. Компьютеры включены в соответствующий домен компьютерной сети БФУ им.И.Канта.

На данных ПК установлено обычное ПО, а также указанное в разделе 9.1. специализированное ПО.

Программно-аппаратные средства лаборатории программно-аппаратных средств защиты информации согласно имеющемуся перечню.

1. Маршрутизатор Cisco 2821. Коммутатор switch d-link des-3526. Стойка серверная 1000 мм 42u с дополнительным пассивным и организующим оборудованием.
2. АПКШ «Континент» (криптошлюз) в корпусе промышленного PC (1U), ЦУС «Континент» (центр управления сетью) в корпусе промышленного PC (1U) с сервером доступа, Абонентский пункт «Континент-АП».
3. «Аккорд-NT/2000» v. 2.0.1 на базе комплекса СЗИ НСД «Аккорд-АМДЗ» v.3.1 (PCI).
4. Средство криптографической защиты информации, включающее библиотеки шифрования и электронную цифровую подпись Верба-W.
5. Средство криптографической защиты информации КРИПТО-ПРО УЦ.
6. Система обеспечения безопасности информации в корпоративной сети «Secret Net» версии 5.0. (обновление) в составе: - Сервер безопасности Secret Net 5.0 -C (до 50 защищаемых серверов и рабочих станций); - «Secret Net» для Windows 2000/XP/2003 (клиенты сервера безопасности); - Системы обеспечения безопасности информации автономных компьютеров «Secret Net» версии 5.0. (обновление); - «Secret Net 5.0 – C» для Windows 2000|XP/2003.
7. Система обнаружения атак Real Secure Network 10/100.
8. Программный продукт для обеспечения сетевой безопасности Internet Scanner.
9. Программный продукт для обеспечения сетевой безопасности X Spider 7.
10. Средство контроля защищенности от несанкционированного доступа "Ревизор сети" (версия 1.2.1.0).
11. Средство контроля защищенности от несанкционированного доступа "Ревизор системы" (версия 1.0).
12. Средство контроля защищенности от несанкционированного доступа "TERRIER (версия 3.0).
13. Средство контроля защищенности от несанкционированного доступа "Ревизор 1 XP".
14. Средство контроля защищенности от несанкционированного доступа "Ревизор 2 XP".
15. Средство контроля защищенности от несанкционированного доступа ФИКС 3.0.
16. Персональное средство криптографической защиты информации ПСКЗИ ШИПКА-1.5.

17. Межсетевой экран ССПТ-1М, исполнение 54323649.401350.003-03 (корпус Iwill G478_XG(19” 1U).
18. Программное средство для защиты от несанкционированного доступа к информации в персональном компьютере с возможностью подключения аппаратных идентификаторов Dallas Lock 7.0.

11. Приложения

Приложение 1

Титульный лист отчета по учебной практике

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Балтийский федеральный университет им. И.Канта

Институт физико-математических наук и информационных технологий

Отчёт
о прохождении учебной практики по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности

Обучающийся _____
(*Ф.И.О. подпись*)

Направление подготовки 10.05.01 Компьютерная безопасность
(*шифр, название*)

Профиль Математические методы защиты информации
(*название*)

Место прохождения практики Институт физико-математических наук и информационных технологий БФУ имени И. Канта, лаборатория программно-аппартных средств защиты информации, 236016, г. Калининград, ул. А. Невского, д. 14.

Срок прохождения практики: с «___» 2019 г. по «___» 2019 г.

Руководитель практики:

_____
(*Ф.И.О., должность, подпись*)

Отчет подготовлен _____ _____
(*подпись обучающегося*) (*И.О. Фамилия*)

Калининград, 2019

Структура отчёта по практике

Титульный лист
Оглавление
ВВЕДЕНИЕ
Во введении ставятся цель и задачи прохождения практики, а также раскрывается суть деятельности обучающегося во время практики. Обязательно указывается, что был пройден инструктаж по технике безопасности и прочие виды инструктажа, предусмотренные программой практики.

ОСНОВНАЯ ЧАСТЬ
В основной части содержится перечень информации, предусмотренный Программой соответствующей практики и обозначенный в индивидуальном задании.

ЗАКЛЮЧЕНИЕ
В заключении формулируются основные результаты проделанной работе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ
Список использованных источников может содержать перечень учебных, научных и периодических изданий, используемых обучающимся для выполнения программы практики, список использованных сайтов.

ПРИЛОЖЕНИЯ К ОТЧЕТУ ПО ПРАКТИКЕ:

Приложение 1 – Индивидуальное задание на практику
Приложение 2 – Отзыв руководителя практики
Приложение 3 – Рабочий график (план) на практику
Приложение 4 – Дополнительная информация

В приложение 4 *могут включаться копии инструкций по работе с программно-аппаратными средствами, листинги заимствованных компьютерных программ и т.д.*

Структура оглавления отчёта по практике

Оглавление

Приложение 2

Форма индивидуального задания на учебную практику

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

«УТВЕРЖДАЮ»
Руководитель практики от БФУ им. И. Канта
_____ / _____ /
«_____»_____ 20__ г.

для _____,
(ФИО студента)

Место прохождения: _____

Срок прохождения: с «___» _____ 20___ г. по «___» _____ 20___ г.

Цель прохождения: _____
_____
_____
_____

Задачи: _____
_____
_____
_____
_____
_____

Содержание: _____
_____
_____
_____
_____
_____

Планируемые результаты:

1	
2	
3	
4	
5	
…	

Форма отчетности: _____

Форма контроля: _____

Ознакомлен(а) _____ «____» _____ 20___ г.
(подпись студента)

Цель прохождения практики:

- 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;

Задачи практики:

Изучить:

- изучить учебно-научную литературу по теме задания на практику;
- систему компьютерной алгебры MAPLE;
- базовые теоретико-числовые алгоритмы;
- алгоритмы вычислений в конечных полях;
- простейшие криптографические алгоритмы;
- инструментальные средства операционной системы Windows, используемые для защиты информации;
- свободно распространяемые в Интернете программные средства анализа защищённости компьютерных систем;
- свободно распространяемые в Интернете программные средства защиты компьютерных систем;

Разработать и исследовать:

- алгоритмы быстрых вычислений с большими целыми числами;
- методы представления данных в больших конечных полях и алгоритмы быстрых вычислений в таких полях;
- простые алгоритмы и протоколы шифрования на основе целых чисел и конечных полей;
- системы защиты данных, используя встроенные инструментальные средства операционной системы Windows;
- инструментарий и порядок настройки свободно распространяемых в Интернете программных средств анализа защищённости компьютерных систем;
- инструментарий и порядок настройки свободно распространяемых в Интернете программных средства защиты компьютерных систем.

Планируемые результаты практики:

- выполненное индивидуальное задание программно-вычислительного характера по тематике изучаемых дисциплин по заданию руководителя практики;
- реализация небольшого исследовательского проекта в рамках утверждённой темы курсовой работы.

Приложение 3

Рекомендации по техническому оформлению отчета о результатах прохождения учебной практики

Оформление отчета о результатах прохождения учебной практики необходимо выполнять в соответствии со следующими правилами.

Объем работы: до 15 страниц формата А4 (210 х 297), но не менее 10 страниц, набранных через полтора интервала на одной стороне листа белой бумаги в текстовом процессоре Word, 2/3 из которых должна занимать практическая часть. Допускается представлять иллюстрации и таблицы на листах формата А3.

Поля: левое - 3 см, правое – 1,5 см, верхнее – 2 см, нижнее – 2 см.

Шрифт: TimesNewRoman, размер шрифта – 14 пунктов.

Титульный лист оформляется по образцу.

Все страницы отчета, включая иллюстрации и приложения, нумеруются по порядку от титульного листа до последней страницы без пропусков и повторений.

Первой страницей является титульный лист, оформленный в соответствующем порядке, номер страницы на нем не ставится. Далее, после титульного листа, вшивается отзыв руководителя, который не нумеруется. После вшивается индивидуальное задание на практику и рабочий график (план) прохождения практики, подписанные руководителем учебной практики, которые не нумеруются. Затем вшивается содержание работы, совпадающее с утвержденным заданием, номер страницы на нем не ставится. Элементы: введение, заключение, список использованной литературы, приложение в содержании и плане не нумеруются.

Далее вшивается первый лист введения, номер страницы на нем не ставится. На последующих страницах порядковый номер печатается в правом верхнем углу без точки в конце, начиная с четвертой страницы, которая является второй страницей введения.

Заголовки основных и дополнительных разделов отчета следует располагать на расстоянии не менее трех интервалов от текста в середине строки без точки в конце и печатать жирным шрифтом, прописными буквами, не подчеркивая.

Заголовки подразделов и пунктов следует начинать с абзацного отступа и печатать жирным шрифтом с прописной буквы, не подчеркивая, без точки в конце.

Если заголовок включает несколько предложений, их разделяют точками. Переносы слов в заголовках не допускаются.

Иллюстрации должны иметь названия. Иллюстрации обозначаются словом "Рисунок", которое помещают под иллюстрацией, и нумеруются последовательно арабскими цифрами в пределах всего отчета. Иллюстрации и таблицы, расположенные на отдельных листах, включают в общую нумерацию страниц. На все иллюстрации должны быть ссылки в отчете. Например,

На рис. 1 представлен...

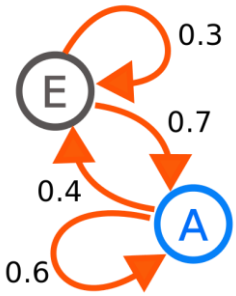

Рис. 1. Название.

Таблицы нумеруют последовательно арабскими цифрами в пределах всего отчёта. В левом верхнем углу таблицы помещают слово "Таблица" с указанием номера этой таблицы и соответствующим заголовком. На все таблицы должны быть ссылки в отчете. Например,… также по итогам работы за первые 3 месяца с заполнением формы (смотри табл. 1).

Таблица 1. Оценка поставщика по критериям

Показатель	Критерий	Важность	Коэффициент	Балл	Результат	Цель	Оценка прошлого периода
а) Закупка		0,4				2	

(если текста в таблице много, то кегль можно уменьшить до 12, если таблица занимает более 1 страницы, то она убирается в приложения).

Если в отчёте одна таблица, ее не нумеруют и слово "Таблица" не пишут.

Таблицу размещают непосредственно после первого упоминания о ней в тексте на этой же или следующей странице таким образом, чтобы читать ее можно было без поворота или с поворотом по часовой стрелке. Ссылка на таблицу по ходу текста выполняется так: "в таблице 2 приводятся данные о ... ".

Примечания к таблицам, иллюстрациям или пунктам и подпунктам текста размещают непосредственно после пункта, подпункта, таблицы, иллюстрации, к которым они относятся, и печатают с прописной буквы с абзацного отступа. Слово "Примечание" следует печатать с абзацного отступа жирным шрифтом.

Ссылки на разделы, подразделы, пункты, подпункты, иллюстрации, таблицы, формулы, уравнения, перечисления, приложения, следуют указывать порядковым номером, например: "... в разделе 4", "... по пункту 3.3.4", "... в подпункте 2.3.41, перечисление 3", "...по формуле (3)", "... в уравнении (2)",-"... на рисунке 8", "... в приложении 6".

Формулы могут быть вписаны в текст от руки тщательно и разборчиво или напечатаны на компьютере. Не разрешается одну часть формулы вписывать от руки, а другую впечатывать. Выше и ниже каждой формулы должно быть оставлено не менее одной свободной строки. Размеры знаков для формулы рекомендуются следующие: прописные буквы и цифры – 7-8 мм, строчные – 4 мм, показатели степени и индексы – не менее 2 мм.

Формулы обычно располагают отдельными строками посередине листа или внутри текстовых строк. В тексте рекомендуется помещать формулы короткие, простые, не имеющие

самостоятельного значения и не пронумерованные. Наиболее важные формулы, а также длинные и громоздкие формулы, содержащие знаки суммирования, произведения, дифференцирования, интегрирования, располагают на отдельных строках. Для экономии места несколько коротких однотипных формул, выделенных из текста, можно помещать на одной строке, а не одну под другой.

Нумеровать следует наиболее важные формулы, на которые имеются ссылки в последующем тексте. Порядковые номера формул обозначают арабскими цифрами в круглых скобках у правого края страницы, например,

$$(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k} \qquad (1)$$

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой даны в формуле. Значение каждого символа и числового коэффициента следует давать с новой строки. Первую строку пояснения начинают со слова "где" без двоеточия.

Формулы в отчёте следует нумеровать порядковой нумерацией в пределах всего отчета арабскими цифрами в круглых скобках в крайнем правом положении на строке. Если в отчете только одна формула или уравнение, их не нумеруют.

Список использованной литературы должен быть выполнен в соответствии с ГОСТ Р 7.0.5 – 2008 «Библиографическая ссылка».

Рекомендуется представлять единый список литературы к работе в целом. Список обязательно должен быть пронумерован. Каждый источник упоминается в списке один раз, вне зависимости от того, как часто на него делается ссылка в тексте работы. Например,

1. Белл Р.Т. Социолингвистика. Цели, методы, проблемы / пер. с англ. — М.: Международные отношения, 1980. — 318 с.
2. Барт Р. Лингвистика текста // Новое в зарубежной лингвистике. — М.: Прогресс, 1978. — Вып. VIII: Лингвистика текста. — С. 442-449.
3. Войскунский А.Е. Метафоры Интернета // Вопросы философии. — 2001. — № 11. — С. 64-79.
4. Школовая М.С. Лингвистические и семиотические аспекты конструирования идентичности в электронной коммуникации: дис. канд. филол. наук. — Тверь, 2005. — 174 с.
5. Сиротинина О.Б. Структурно-функциональные изменения в современном русском литературном языке: проблема соотношения языка и его реального функционирования // Русская словесность в контексте современных интеграционных процессов: материалы междунар. науч. конф. — Волгоград: Изд-во ВолГУ, 2007. — Т. 1. — С. 14-19.
6. Бахтин М.М. Творчество Франсуа Рабле и народная культура средневековья и Ренессанса. — 2-е изд. — М.: Худож. лит., 1990. — 543 с. [Электронный ресурс]. URL: http://www.philosophy.ru/library/bahtin/rable.html#_ftn1 (дата обращения: 05.10.2008).
7. Белоус Н.А. Прагматическая реализация коммуникативных стратегий в конфликтном дискурсе // Мир лингвистики и коммуникации: электронный научный журнал. — 2006. — № 4 [Электронный ресурс]. URL: http://www.tverlingua.by.ru/archive/005/5_3_1.htm (дата обращения: 15.12.2007).
8. Новикова С.С. Социология: история, основы, институционализация в России. — М.: Московский психолого-социальный институт; Воронеж: Изд-во НПО «МОДЭК», 2000.

— 464 с. [Электронный ресурс]. Систем. требования: Архиватор RAR. — URL: http://ihtik.lib.ru/edu_21sept2007/edu_21sept2007_685.rar (дата обращения: 17.05.2007).
9. Парпалк Р. Общение в Интернете // Персональный сайт Романа Парпалака. — 2006. — 10 декабря [Электронный ресурс]. URL: http://written.ru (дата обращения: 26.07.2006).

На всю использованную литературу должны быть ссылки в тексте работы.

Приложения оформляются следующим образом:

Приложения

(при их наличии)

Приложение 1

Название приложения 1

На каждое приложение должна быть ссылка в тексте.

Отчет о результатах прохождения учебной практики вшивается в папку-скоросшиватель с прозрачной верхней обложкой.

Приложение 4

Форма рабочего графика (плана) на практику

РАБОЧИЙ ГРАФИК (ПЛАН) НА ПРАКТИКУ

«УТВЕРЖДАЮ»
Руководитель практики от БФУ им. И. Канта

_____ / _____ /
«_____»_____ 20__ г.

для _____,
(ФИО студента)

Срок прохождения: с «___» _____ 20___ г. по «___» _____ 20___ г.
Место прохождения: _____

№ п/п	Наименование этапа практики	Виды работ (ПРИМЕР формулировок)	Сроки выполнения	Отметка о выполнении
1	**Организационно – подготовительный этап**	- ознакомление с индивидуальным заданием; - прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также действующими в организации правилами внутреннего трудового распорядка организации; - ознакомление с отчетной документацией о прохождении практики	«___» _____ 20___ г.	
2	**Основной этап**	- выполнение индивидуального задания; - ежедневное выполнение установленных программой практики видов работ; - сбор, обработка и систематизация материала по конкретному этапу прохождения практики; - заполнение отчета о прохождении практики	с «___» _____ 20___ г. по «___» _____ 20___ г.	
3	**Заключительный этап**	- прохождение промежуточной аттестации по результатам прохождения практики	«___» _____ 20___ г.	

Приложение 5

Форма отзыва руководителя практики

ОТЗЫВ
о работе обучающегося в период прохождения учебной практики

Обучающийся _____
(Ф.И.О.)
Института физико-математических наук и информационных технологий проходил учебную практику по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности_____
(вид и тип практики)

в период с «____»_____2019 г. по «____»_____2019 г.

На время прохождения практики _____
(*Фамилия, И.О. обучающегося*)
поручалось решение следующих задач: _____
_____

Результаты работы обучающегося:

Полнота выполнения задания_____
_____

Достоверность результатов исследования _____
_____

Положительные стороны отчета_____
_____

Недостатки отчета_____
_____

Самостоятельность и инициативность студента_____
_____

Навыки, приобретенные за время НИР_____
_____

Отношения студента к работе_____
_____

Считаю, что по итогам практики обучающийся может (не может) быть допущен к защите отчета по практике.

Рекомендуемая оценка за практику _____
(дифференцированный зачет)

Руководитель практики_____
(Ф.И.О. подпись)
«____»_____2019 г.