МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Балтийский федеральный университет им. Иммануила Канта

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ Е.П.Новикова
«15» февраля 2019 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«25» февраля 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Подготовка к процедуре защиты выпускной квалификационной работы»

для студентов 6 курса
очной формы обучения
специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»
уровень высшего образования - специалитет

Калининград
2019

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. Общая характеристика процедуры государственной итоговой аттестации выпускника по специальности 10.05.01 «Компьютерная безопасность», уровень высшего образования – специалитет....4
1.1 Общие положения....4
1.2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы....4
1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся....14
2. Порядок подготовки к защите выпускной квалификационной работы....15
2.1. Процессы подготовки защиты выпускной квалификационной работы....15
2.2. Требования и нормы подготовки выпускной квалификационной работы....15
2.2.1. Общие требования к выпускной квалификационной работе....15
2.2.2. Порядок оформления выпускной квалификационной работы....17
2.2.3. Порядок составления отзыва и рецензии на выпускную квалификационную работу....17
2.3. Описание показателей и критериев оценивания компетенций....18
2.4. Шкала оценивания степени сформированности компетенций....19
3. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины....20
3.1. Основная литература....20
3.2. Дополнительная литература....20
4. Фонд оценочных средств для проведения ГИА....21
4.1. Примерная тематика выпускных квалификационных работ по специальности 10.05.01 «Компьютерная безопасность» (специализация «Математические методы защиты информации»). 31
4.2. Примеры формулировки тем и содержания выпускных квалификационных работ 33
ПРИЛОЖЕНИЯ....37

1. Общая характеристика процедуры государственной итоговой аттестации выпускника по специальности 10.05.01 «Компьютерная безопасность», уровень высшего образования – специалитет

1.1 Общие положения

Программа ГИА является частью основной профессиональной образовательной программы в соответствии с ФГОС ВО в части государственных требований к минимуму содержания и уровню подготовки выпускников по специальности 10.05.01 «Компьютерная безопасность».

ГИА выпускников по специальности 10.05.01 «Компьютерная безопасность» является заключительным этапом обучения, подтверждающего квалификацию «Специалист по защите информации».

К ГИА допускаются лица, выполнившие требования, предусмотренные курсом обучения по основной образовательной программе по специальности 10.05.01 «Компьютерная безопасность» и успешно прошедшие все промежуточные аттестационные испытания по теоретическому и практическому этапам обучения, предусмотренные утвержденным учебным планом специальности «Компьютерная безопасность», специализации «Математические методы защиты информации».

Видом ГИА в соответствии с п. 6.8 ФГОС ВО и учебным планом является защита выпускной квалификационной работы.

Аттестацию проводит Государственная Экзаменационная Комиссия (ГЭК). Председатель ГЭК и состав ГЭК утверждаются в установленном порядке.

Выпускная квалификационная работа выполняется в обязательном порядке, в установленные сроки, проходит рецензирование и защищается в ГЭК.

Государственная итоговая аттестация (ГИА) специальности включает в себя два основных этапа – этап подготовки к процедуре защиты выпускной квалификационной работы (Б3.Б.01(Д)) и этап защиты выпускной квалификационной работы (Б3.Б.02(Д)).

Наименование дисциплины (модуля) – «Подготовка к процедуре защиты выпускной квалификационной работы».

1.2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Целью освоения дисциплины «Подготовка к процедуре защиты выпускной квалификационной работы» является подготовка к защите выпускной квалификационной работы.

При выполнении выпускной квалификационной работы, обучающиеся должны показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные универсальные и профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

Выпускник специальности 10.05.01 «Компьютерная безопасность» (специализация «Математические методы защиты информации») с квалификацией Специалист по защите информации в соответствии с целями основной образовательной программы и задачами

профессиональной деятельности в результате освоения данной дисциплины ООП специальности должен обладать следующими компетенциями:

Код компетенции	Результаты освоения ООП Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОК-1	Способность использовать основы философских знаний для формирования мировоззренческой позиции.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** основные принципы философии, принципы теории познания, концепцию личности. • ***уметь*:** применять методологию теории познания к оценке конкретных профессиональных знаний, к принятию решений в рамках профессиональной деятельности. • ***владеть*:** практическими навыками логического анализа и философского осмысления проблем профессиональной области (компьютерной безопасности), методов и перспектив их решения.
ОК-2	Способность использовать основы экономических знаний в различных сферах деятельности.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** принципы функционирования рынка; основы законодательства в области экономической деятельности; знать основные субъекты рынка программно-аппаратных и технических средств защиты информации; • ***уметь***: находить поставщиков программно-аппаратных и технических средств защиты информации; составлять заявку на проведение конкурса по закупке средств защиты информации; • ***владеть*:** методами оценки экономической эффективности систем защиты информации.
ОК-3	Способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** основные вехи становления Российского государства; основных государственных деятелей России на протяжении её истории и их вклад в развитие России; историю и роль служб государственной безопасности; историю и роль компьютерной безопасности в условиях информационного противоборства; • ***уметь***: анализировать основные этапы и закономерности исторического развития Российского государства, ее место и роль в современном мире; • ***владеть*:** навыками отстаивания в дискуссии гражданской позиции на основе патриотизма.

ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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 социальные, культурные и иные различия	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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 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-9	Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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 подготовки к процедуре защиты выпускной квалификационной работы студент 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 ис-

		следования 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 физических явлений и процессов; навыками построения математических моделей и исследования их свойств, методами решения математических задач.
ОПК-2	Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей и математической статистики, теории информации, теоретико-числовых методов.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** основные определения и свойства структур математического анализа, алгебраических и числовых структур, структур дискретной математики и геометрии кривых, математической логики и теории информации; основные направления приложения математических методов в области информационной безопасности. • ***уметь*:** применять математические методы и модели из различных областей математики для формализации, исследования и решения задач, связанных с различными аспектами обеспечения информационной безопасности: математическими, физическими, логическими и техническими. • ***владеть*:** основными методами и алгоритмами вычислений с целыми числами, матрицами, многочленами, классами вычетов, комплексными числами; алгоритмом решения линейных сравнений и систем сравнений; правилом сложения точек эллиптической кривой; алгоритмами численного дифференцирования и интегрирования, решения дифференциальных уравнений; алгоритмами получения точечных и интервальных оценок случайных величин, проверки статистических гипотез.
ОПК-3	Способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** методы формального представления информации; основные процедуры машинной обработки информации; основные поисковые системы, их функции, возможности и способы работы с ними; основные источники информации по дисциплинам; • ***уметь*:** работать с научно-технической литературой по тематике дисциплины; запускать и использовать поисковые системы; анализировать и систематизировать большие массивы информации; составлять аналитические обзоры литературы по информационной безопасности; • ***владеть*:** навыками использования поисковых систем в сети Интер-

	обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации.	нет; навыками составления библиографических описаний.
ОПК-4	Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** современные методы исследований из различных областей математики, физики, электроники, и других; знать методологические принципы применения этих методов в задачах защиты информации; • ***уметь*:** корректно формулировать задачи обеспечения информационной безопасности, строить план их решения, подбирать подходящие теоретические или экспериментальные методы решения, интегрировать данные методы в единую схему при работе над междисциплинарными проектами; • ***владеть*:** навыками применения теоретических и экспериментальных методов для решения задач обеспечения информационной безопасности.
ОПК-5	Способность использовать нормативные правовые акты в своей профессиональной деятельности	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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.
ОПК-6	Способность применять методы оказания первой помощи, методы защиты производственного персонала и	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** методы оказания первой помощи в чрезвычайных ситуациях; основные правовые нормы в области охраны труда; методы защиты производственного персонала, работающего со средствами обеспечения информационной безопасности; • ***уметь***: оказывать первую помощь в чрезвычайных ситуациях; проводить первичный инструктаж по технике безопасности на рабочем месте;

	населения в условиях чрезвычайных ситуаций	• ***владеть*:** навыками оказания первой помощи в чрезвычайных ситуациях; навыками планирования технических мероприятий с целью защиты производственного персонала, работающего со средствами обеспечения информационной безопасности.
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 подготовки к процедуре защиты выпускной квалификационной работы студент 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 базовых 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 подготовки к процедуре защиты выпускной квалификационной работы студент 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-9	Способность разрабатывать формальные модели политик безопасности, политик управления доступом и	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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 управлени-

	информационными потоками в компьютерных системах с учетом угроз безопасности информации.	ем 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.
ОПК-10	Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***Знать*** математические основы криптографических алгоритмов и алгоритмов теории кодирования, современное программное обеспечение для решения алгебраических задач. • ***Уметь*** формализовать и алгоритмизировать математические методы, моделировать алгоритмы в системах компьютерной алгебры, оценивать их работоспособность и эффективность. • ***Владеть*** приемами реализации алгоритмов вычислений, реализуемых в системах обеспечения защиты компьютерной информации; приемами работы с программными средствами прикладного, системного и специального назначения.
ПК-1	Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***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-5	Способность участвовать в разработке и конфигурировании программно-	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать:*** методы и сертифицированные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем; способы и средства антивирусной защиты; принципы построения и оценки эффективности криптографических алгоритмов, а также раз-

	аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.	решённые 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 участвовать в разработке проектной и технической документации	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***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-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.
ПК-8	Способность участвовать в	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен:

	разработке подсистемы информационной безопасности компьютерной системы.	• **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** методологией проектирования систем защиты информации, практическими навыками применения современных компьютерных технологий, построением математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, оценивать эффективность их применения.
ПСК-2.1	Способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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.
ПСК-2.2	Способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** 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.
ПСК-2.3	Способность строить математические модели для оценки без-	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** типовые алгоритмы преобразования информации в компьютерных системах и оценки их эффективности; перспективные методы и алгоритмы преобразования информации в компьютерных системах и

	опасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.	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; проводить 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 вычислительной эффективности алгоритмов.
ПСК-2.4	Способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** методы алгебры, теории чисел, алгебраической геометрии и дискретной математики и их применение в моделях информационных процессов и в сертифицированных программно-аппаратных средствах защиты информации; знать методологию оценки адекватности применяемых математических моделей; • ***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.
ПСК-2.5	Способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты ин-	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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.

	формации.	

1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины **«Подготовка к процедуре защиты выпускной квалификационной работы»** составляет 7 зачетных единиц и 252 академических часа.

Объем дисциплины по видам учебных занятий (в часах)

Объем дисциплины	**Всего часов**		
	для очной формы обучения	**для заочной формы обучения**	**очно-заочной формы обучения**
Общая трудоемкость дисциплины	**252**	–	–
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	**2**	–	–
Аудиторная работа (всего):		–	–
в т. числе:			
Лекции		–	–
Практические занятия		–	–
Лабораторные работы		–	–
Групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем		–	–
Самостоятельная работа обучающихся (всего)	**250**	–	–
Вид промежуточной аттестации обучающегося (зачет / экзамен)		–	–

Место и время проведения государственной итоговой аттестации

Порядок и сроки проведения аттестационных испытаний устанавливаются в соответствии с графиком учебного процесса по специальности 10.05.01 «Компьютерная безопасность» специализации «Математические методы защиты информации» на основании Поло-

жения об организации выполнения и защиты выпускной квалификационной работы обучающимися (студентами) от 15.05.2014 г., утвержденного Ученым советом БФУ (протокол № 10 от 12 мая 2014 г.).

2. Порядок подготовки к защите выпускной квалификационной работы

2.1. Процессы подготовки защиты выпускной квалификационной работы

1. Методический руководитель 10.05.01 «Компьютерная безопасность» распределяет руководство подготовкой выпускных квалификационных работ (ВКР) среди преподавателей Института физико-математических наук и информационных технологий с требуемым уровнем квалификации и образования.
2. Обучающийся выбирает тему ВКР и совместно с научным руководителем готовит календарный план-график работы над ВКР, который подписывается студентом, научным руководителем и утверждается методическим руководителем направления.
3. На заседании Учебно-методического совета Института физико-математических наук и информационных технологий обсуждаются темы ВКР, закрепляются научные руководители. Методический руководитель направления вносит представление в приказ об утверждении тем и научных руководителей ВКР.
4. Приказом ректора утверждаются темы ВКР и закрепляются научные руководители.
5. После завершения работы над ВКР заверенная обучающимся ВКР передаётся научному руководителю для проверки.
6. Научный руководитель принимает решение о допуске к защите, которое подтверждается методическим руководителем направления.
7. Защита ВКР организуется в соответствии с графиком учебного процесса.
8. Защита ВКР проводится на открытых заседаниях ГЭК с участием не менее двух третей ее состава.

2.2. Требования и нормы подготовки выпускной квалификационной работы

2.2.1. *Общие требования к выпускной квалификационной работе*

Изложение материала в выпускной квалификационной работе должно быть последовательным и логичным. Все разделы должны быть связаны между собой. Следует обращать внимание на логические переходы от одной главы к другой, от параграфа к параграфу, а внутри параграфа – от вопроса к вопросу.

Написание текста ВКР необходимо начинать с введения и первой главы, последовательно прорабатывая все разделы, включенные в план. Изложение материала в ВКР должно быть конкретным и опираться на результаты практик, при этом важно не просто описание, а критический разбор и анализ полученных данных.

Введение – важная часть ВКР. Во введении обосновываются актуальность выбранной темы, цель и содержание поставленной задачи, формулируются объект и предмет исследования, указываются избранные методы исследования, определяется значимость полученных результатов.

Обзор литературы – должен показать знакомство студента со специальной литературой и Интернет-источниками, его умение систематизировать материалы, критически их рассматривать, выделять существенное, оценивать ранее сделанное другими исследователями, определять главное в современном состоянии изученности темы. Результаты такого обзора следует систематизировать в определенной логической последовательности. Поскольку выпускная квалификационная работа обычно посвящается достаточно узкой теме, то обзор работ предшественников следует делать только по вопросам выбранной темы, а не по всей проблеме в целом. Обычно сюда же включается обзор предварительных сведений, на которые имеются ссылки в основной части ВКР.

При изложении в ВКР спорных вопросов темы необходимо приводить мнения различных авторов. Если в работе критически рассматривается точка зрения какого-либо автора, при изложении его мысли следует приводить цитаты, только при этом условии критика может быть объективной. Обязательным, при наличии различных подходов к решению изучаемой проблемы, является сравнение рекомендаций, содержащихся в действующих инструктивных материалах и работах различных авторов. Только после этого следует обосновывать свое мнение по спорному вопросу или соглашаться с одной из уже имеющихся точек зрения, выдвигая в любом случае соответствующие аргументы.

В главах ***основной части*** выпускной квалификационной работы подробно рассматриваются и обобщаются результаты исследования. Для выпускных квалификационных работ в области компьютерной безопасности и математических методов защиты информации в основную часть включается описание применяемых логических схем, математических методов и моделей, структура компьютерных программ, планы и результаты компьютерных экспериментов, способы их использования для решения поставленной задачи. Содержание глав основной части должно точно соответствовать теме работы и полностью её раскрывать. Эти главы должны показать умение автора сжато, логично и аргументировано излагать материал.

Отдельные положения ВКР должны быть иллюстрированы соответствующими моделями и результатами расчетов, компьютерных экспериментов, цифровыми данными из справочников, монографий и других литературных источников, при необходимости оформленными в справочные или аналитические таблицы. При составлении аналитических таблиц используемые исходные данные выносятся в приложение к выпускной квалификационной работе, а в тексте приводятся расчёты отдельных показателей. Таблица должна занимать не более одной страницы. Если аналитическая таблица по размеру превышает одну страницу, её следует включать в приложение. В отдельных случаях можно заимствовать некоторые таблицы из литературных источников. Ссылаться на таблицу нужно в том месте текста, где формулируется положение, подтверждаемое или иллюстрируемое ею. В тексте, анализирующем или комментирующем таблицу, не следует пересказывать её содержание, а уместно формулировать основной вывод, к которому подводят табличные данные, или вводить дополнительные показатели, более отчётливо характеризующие то или иное явление или его отдельные стороны.

Логические и структурные схемы, а также графические модели могут оформляться в виде рисунков. Рисунок должен занимать не более одной страницы. Если рисунок по размеру превышает одну страницу, его следует включать в приложение. Ссылаться на рисунок нужно в том месте текста, где формулируется положение, подтверждаемое или иллюстрируемое им.

Все материалы, не являющиеся необходимыми для решения поставленных в работе задач, также выносятся в приложения.

Заключение **–** последовательное логически стройное изложение итогов работы и их соотношение с общей целью и конкретными задачами, поставленными и сформулированными во введении, а также возможных перспектив дальнейших исследований и направлений практического использования результатов работы.

Законченные главы ВКР сдаются научному руководителю на проверку в установленные планом-графиком сроки.

Проверенные главы дорабатываются в соответствии с полученными от научного руководителя замечаниями, после чего студент приступает к оформлению работы.

2.2.2. *Порядок оформления выпускной квалификационной работы*

Тексты ВКР оформляются в соответствии с едиными требованиями:

- Выпускная квалификационная работа должна быть напечатана, шрифт Times New Roman, размер шрифта 14, через 1,5-й интервал, поля: слева – 3 см, справа – 1,5 см, сверху, снизу – 2 см. Объем ВКР может быть в пределах 40-50 страниц стандартного печатного текста (без приложений). Все страницы работы (включая список литературы и приложения) последовательно нумеруются. Листы работы прошиваются.
- Каждый раздел текста ВКР начинается с новой страницы.
- Заголовки глав и разделов выделяются жирным шрифтом.
- Таблицы и рисунки могут располагаться как непосредственно в тексте ВКР, так и в приложениях. Таблицы и рисунки должны содержать заголовки и названия, достаточно полно отражающие их содержание и специфику.

2.2.3. *Порядок составления отзыва и рецензии на выпускную квалификационную работу*

Законченная и оформленная в соответствии с указанными выше требованиями выпускная квалификационная работа подписывается студентом и консультантами (при их наличии) и не позднее двух недель до защиты представляется научному руководителю, который даёт письменный отзыв на работу и подписывает её. ВКР, представленная позднее указанного срока, к защите не допускается.

Отзыв научного руководителя. После получения окончательного варианта ВКР научный руководитель, в недельный срок составляет письменный отзыв, в котором всесторонне характеризует качество работы, отмечает положительные стороны, особое внимание обращает на отмеченные ранее недостатки, не устранённые студентом, обосновывает возможность или нецелесообразность представления выпускной квалификационной работы в ГЭК. В отзыве руководитель отмечает также ритмичность выполнения работы в соответствии с планом-графиком, добросовестность, определяет степень самостоятельности, активности и творческого подхода, проявленные студентом в период написания выпускной квалификационной работы, степень соответствия требованиям, предъявляемым к выпускным квалификационным работам, и рекомендует оценку. Форма отзыва представлена в *Приложении* №4

Переплетённая работа вместе с положительным письменным отзывом научного руководителя передаётся методическому руководителю специальности на рассмотрение. Методический руководитель принимает решение о допуске работы к защите, о чём ставит соот-

ветствующую резолюцию на титульном листе работы. Образец титульного листа представлен в *Приложении* №1.

В случае, если методический руководитель, исходя из содержания отзывов научного руководителя, а также содержания и оформления работы, не считает возможным допустить студента к защите выпускной квалификационной работы в ГЭК, вопрос об этом должен рассматриваться на заседании Учебно-методического совета Института с привлечением научного руководителя и автора работы. Решение Учебно-методического совета Института является окончательным.

Выпускные квалификационные работы, выполняемые по завершении освоения программы подготовки специалиста, подлежат обязательному рецензированию.

Полностью оформленная выпускная квалификационная работа, допущенная к защите методическим руководителем, направляется на рецензию.

Рецензия. В рецензии должен быть дан квалифицированный анализ существа и основных положений рецензируемой работы, оценка актуальности избранной темы, самостоятельности подхода к её раскрытию, наличия собственной точки зрения автора, умения пользоваться методами сбора и обработки информации, степени обоснованности выводов и рекомендаций, достоверности полученных результатов, их новизну и практическую значимость. Наряду с положительными сторонами работы отмечаются недостатки, в частности, указываются отступления от логичности и грамотности изложения материала, выявляются фактические ошибки. В заключение рецензент излагает свою точку зрения об общем уровне выпускной квалификационной работы и оценивает её, после чего подписывает титульный лист работы. Объём рецензии должен составлять от одной до трех страниц машинописного текста. Рецензия должна быть получена не позднее, чем за три дня до защиты. Форма рецензии представлена в *Приложении* №5.

После получения положительного отзыва рецензента работа передается в Государственную экзаменационную комиссию (ГЭК).

2.3. Описание показателей и критериев оценивания компетенций

Степень сформированности компетенций в ходе подготовки к защите выпускной квалификационной работы осуществляется научным руководителем и членами комиссии при знакомстве с текстом ВКР.

1. В качестве критериев для оценки ВКР научные руководители и члены ГЭК должны иметь в виду:

- актуальность темы и задач работы;
- соответствие тематики специальности «Компьютерная безопасность»;
- обоснованность результатов и выводов;
- определенную оригинальность и новизну полученных данных;
- самостоятельность (личный вклад студента);
- возможности практического использования полученных результатов.

2. Обоснованность результатов и выводов определяются с позиций:

- соответствия известным научным положениям и фактам;
- логичности в изложении и обсуждении собственных данных;
- корректности постановки опыта, эксперимента;

- корректности использования математических методов.

При этом должны учитываться:

- уровень устного доклада на защите;
- соответствие оформления работы установленным требованиям;
- качество иллюстративного материала к докладу.

3. Оригинальность и новизна полученных данных определяется как:

- установление нового научного факта или подтверждение известного факта для новых условий;
- получение сведений, приводящих к формулировке проверяемых гипотез, которые требуют дальнейшей проверки;
- разработка оригинального метода решения известной задачи;
- применение известных методик для решения новых задач;
- введение в научный оборот новых данных;
- обоснованное решение поставленной задачи.

4. Личный вклад студента определяется: степенью самостоятельности в выборе темы, постановке задач, планировании и организации исследования, обработке и осмыслении полученных результатов.

5. Возможность практического использования данных, полученных в ВКР, определяется в отношении НИР, выполняемых в университете или в других организациях; задачами совершенствования учебного процесса; возможностью публикации в печати.

2.4. Шкала оценивания степени сформированности компетенций

Выпускная квалификационная работа оценивается по четырёхбалльной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».

ВКР, получающая по мнению руководителя или рецензента оценку «неудовлетворительно», может быть в отдельных случаях направлена на дополнительное рецензирование по распоряжению председателя ГЭК.

Оценка **«Отлично»** выставляется за выпускную квалификационную работу, которая имеет исследовательский характер, грамотно изложенную теоретическую часть, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями. ВКР имеет положительный отзыв научного руководителя и рецензента.

Оценка **«Хорошо»** выставляется за выпускную квалификационную работу, которая содержит элементы научного исследования, грамотно изложенную теоретическую часть, последовательное изложение материала соответствующими выводами, однако с не вполне обоснованными предложениями. ВКР имеет положительный отзыв научного руководителя и рецензента.

Оценка **«Удовлетворительно»** выставляется за выпускную квалификационную работу, которая имеет технический характер. ВКР базируется на практическом материале, но анализ выполнен поверхностно, в ней просматривается непоследовательность изложения материала. Представлены необоснованные предложения. ВКР имеет реферативный или обзорный характер с элементами анализа и оригинальности. В отзывах научного руководителя и рецензента имеются замечания по содержанию работы и методике анализа.

Оценка **«Неудовлетворительно»** выставляется за выпускную квалификационную работу, которая не носит исследовательского характера, не отвечает требованиям, изложен-

ным в методических рекомендациях. В работе нет выводов, либо они носят декларативный характер. В отзывах научного руководителя и рецензента имеются серьезные критические замечания.

Итоговая оценка ГЭК выводится по принципу учета оценок большинства членов ГЭК, а также руководителя. Оцениваемые компетенции и оценочный лист приведены в *Приложениях* №2 и №3, соответственно.

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

3.1. Основная литература

1. Емельянова, И. Н. Основы научной деятельности студента. Магистерская диссертация [Электронный ресурс]: учеб. пособие для вузов/ И. Н. Емельянова; Тюмен. гос. ун-т. – Москва: Юрайт, 2018 1r=**on-line**, 115 с. Language: Russian, База данных: Каталог НБ БФУ им. И. Канта – Книги.
2. Методические рекомендации по подготовке выпускной квалификационной работы (магистерской диссертации) для магистрантов [Электронный ресурс]: метод. рекомендации/ Балт. федер. ун-т им. И. Канта, Ин-т образования; [сост. А. О. Бударина [и др.]. - Калининград: Изд-во БФУ им. И. Канта, 2018 **on-line**, 45 с.. - Библиогр.: с. 25 (2 назв.). - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1) Свободны / free: ЭБС Кантиана(1)

3.2. Дополнительная литература

1. Байбородова, Л. В. Методология и методы научного исследования [Электронный ресурс]: учеб. пособие для бакалавриата и магистратуры/ Л. В. Байбородова, А. П. Чернявская. – Москва: Юрайт, 2018 1r=**on-line**, 221 с. Language: Russian, База данных: Каталог НБ БФУ им. И. Канта – Книги.
2. Горелов, Н. А. Методология научных исследований [Электронный ресурс]: учеб. и практикум для бакалавриата и магистратуры/ Н. А. Горелов, Д. В. Круглов, О. Н. Кораблева. - 2-е изд., перераб. и доп.. - Москва: Юрайт, 2019 1r=**on-line**, 365 с.: а-ил. Language: Undetermined, База данных: Каталог НБ БФУ им. И. Канта - Книги
3. Дрещинский, В. А. Методология научных исследований [Электронный ресурс]: учеб. для бакалавриата и магистратуры/ В. А. Дрещинский. - 2-е изд., перераб. и доп.. – Москва: Юрайт, 2018 1r=**on-line**, 324 с. Language: Russian, База данных: Каталог НБ БФУ им. И. Канта – Книги.
4. Методические рекомендации по написанию и защите выпускных квалификационных работ студентов-бакалавров [Электронный ресурс]: метод. рекомендации/ Балт. федер. ун-т им. И. Канта, Ин-т образования; [сост. А. О. Бударина [и др.]. - Калининград: Изд-во БФУ им. И. Канта, 2018 **on-line**, 25 с.. - Библиогр.: с. 17 (2 назв.). - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1) Свободны / free: ЭБС Кантиана(1).

Программное обеспечение и Интернет-ресурсы

1. Операционная система Microsoft Windows.
2. Пакет Microsoft Office (MS Word, MS Excel, MS PowerPoint, MS Access, MS Project, MS Visio).
3. Справочно-поисковые системы «Консультант плюс» или «Гарант».
4. Microsoft SQL Srv Standard Core 2014 (Количество лицензий – 4, Номер акта / накладной – Tr063168, Дата акта – 24.11.14);
5. Microsoft Visual Studio 2005 (Количество лицензий – 30, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).

4. Фонд оценочных средств для проведения ГИА

Компетенция	*Перечень планируемых результатов*	*Диагностический инструмент*	*Критерии оценки*
ОК-1 Способность использовать основы философских знаний для формирования мировоззренческой позиции.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*** основные принципы философии, принципы теории познания, концепцию личности; • ***уметь*** применять методологию теории познания к оценке конкретных профессиональных знаний, к принятию решений в рамках профессиональной деятельности. • ***владеть*:** практическими навыками логического анализа и философского осмысления проблем профессиональной области (компьютерной безопасности), методов и перспектив их решения.	1. Актуальность тематики работы и её соответствие профилю специальности «Компьютерная безопасность». 2. Степень полноты обзора состояния вопроса и корректность постановки задачи. 3. Уровень и корректность использования в работе методов исследований, математического моделирования, расчетов. 4. Степень комплексности работы, применение в ней знаний общепрофессиональных и специаль-	Глубокое раскрытие темы, качественное оформление работы, обоснованность сделанных выводов и их аргументированность, оригинальность и новизна полученных результатов.
ОК-2 Способность использовать основы экономических знаний в различных сферах деятельности.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** принципы функционирования рынка; основы законодательства в области экономической деятельности; знать основные субъекты рынка программно-аппаратных и технических средств защиты информации; • ***уметь***: находить поставщиков программно-аппаратных и технических средств защиты информации; составлять заявку на проведение конкурса по закупке средств защиты информации; • ***владеть*:** методами оценки экономической эффективности систем защиты информации.		
ОК-3 Способность анализировать основные этапы и закономерно-	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** основные вехи становления Российского государства; основных государственных деятелей России на протяжении её истории и их вклад в развитие Рос-		

сти исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	сии; историю и роль служб государственной безопасности; историю и роль компьютерной безопасности в условиях информационного противоборства; • ***уметь***: анализировать основные этапы и закономерности исторического развития Российского государства, ее место и роль в современном мире; • ***владеть*****:** навыками отстаивания в дискуссии гражданской позиции на основе патриотизма.	ных дисциплин. 5. Ясность, четкость, последовательность и обоснованность изложения. 6. Применение современного математического и программного обеспечения, компьютерных технологий в работе. 7. Качество оформления (общий уровень грамотности, стиль изложения, качество иллюстраций, соответствие требованиям стандартов). 8. Объем и качество выполнения графического материала, его соответствие тексту. 9. Обоснованность и доказательность выводов работы. 10. Оригинальность и новизна полученных результатов, научно-исследовательских, технических или методических реше-	
ОК-4 Способность использовать основы правовых знаний в различных сферах деятельности.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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 социальные, культурные и иные различия	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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 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-9 Способность использовать методы и средства физической культуры для обеспечения полноцен-	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*****:** факторы здорового образа жизни; методы оценки физического развития, телосложения, двигательной и функциональной подготовленности средствами физической культуры и спорта в студенческом возрасте;		

ной социальной и профессиональной деятельности	• ***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;	ний.	
ОПК-1 Способность анализировать физические явления и процессы при решении профессиональных задач	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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 физических явлений и процессов; навыками построения математических моделей и исследования их свойств, методами решения математических задач.		
ОПК-2 Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математи-	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** основные определения и свойства структур математического анализа, алгебраических и числовых структур, структур дискретной математики и геометрии кривых, математической логики и теории информации; основные направления приложения математических методов в области информационной безопасности. • ***уметь*:** применять математические методы и модели из различных областей математики для формализа-		

ческой логики, теории алгоритмов, теории вероятностей и математической статистики, теории информации, теоретико-числовых методов.	ции, исследования и решения задач, связанных с различными аспектами обеспечения информационной безопасности: математическими, физическими, логическими и техническими. • ***владеть*:** основными методами и алгоритмами вычислений с целыми числами, матрицами, многочленами, классами вычетов, комплексными числами; алгоритмом решения линейных сравнений и систем сравнений; правилом сложения точек эллиптической кривой; алгоритмами численного дифференцирования и интегрирования, решения дифференциальных уравнений; алгоритмами получения точечных и интервальных оценок случайных величин, проверки статистических гипотез.		
ОПК-3 Способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** методы формального представления информации; основные процедуры машинной обработки информации; основные поисковые системы, их функции, возможности и способы работы с ними; основные источники информации по дисциплинам; • ***уметь*:** работать с научно-технической литературой по тематике дисциплины; запускать и использовать поисковые системы; анализировать и систематизировать большие массивы информации; составлять аналитические обзоры литературы по информационной безопасности; • ***владеть*:** навыками использования поисковых систем в сети Интернет; навыками составления библиографических описаний.		
ОПК-4 Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** современные методы исследований из различных областей математики, физики, электроники, и других; знать методологические принципы применения этих методов в задачах защиты информации; • ***уметь*:** корректно формулировать задачи обеспечения информационной безопасности, строить план их решения, подбирать подходящие теоретические или экспериментальные методы решения, интегрировать данные методы в единую схему при работе над междисциплинарными проектами; • ***владеть*:** навыками применения теоретических и экспериментальных методов для решения задач		

	обеспечения информационной безопасности.		
ОПК-5 Способность использовать нормативные правовые акты в своей профессиональной деятельности	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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.		
ОПК-6 Способность применять методы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** методы оказания первой помощи в чрезвычайных ситуациях; основные правовые нормы в области охраны труда; методы защиты производственного персонала, работающего со средствами обеспечения информационной безопасности; • ***уметь***: оказывать первую помощь в чрезвычайных ситуациях; проводить первичный инструктаж по технике безопасности на рабочем месте; • ***владеть*:** навыками оказания первой помощи в чрезвычайных ситуациях; навыками планирования технических мероприятий с целью защиты производственного персонала, работающего со средствами обеспечения информационной безопасности.		
ОПК-7 Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специ-	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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 базовых криптографических алгоритмов; • ***владеть*:** практическими навыками применения компьютерных технологий для формирования алгоритмов и проведения вычислений, связанных с защитой информации.		

ального назначения			
ОПК-8 Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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-9 Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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.		
ОПК-10 Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***Знать*** математические основы криптографических алгоритмов и алгоритмов теории кодирования, современное программное обеспечение для решения алгебраических задач. • ***Уметь*** формализовать и алгоритмизировать математические методы, моделировать алгоритмы в системах компьютерной алгебры, оценивать их работоспособность и эффективность. • ***Владеть*** приемами реализации алгоритмов вычисле-		

	ний, реализуемых в системах обеспечения защиты компьютерной информации; приемами работы с программными средствами прикладного, системного и специального назначения.		
ПК-1 Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***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-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 подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать:*** методы и сертифицированные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем; способы и средства антивирусной защиты; принципы построения и оценки эффективности криптографических алгоритмов, а также разрешённые к применению средства криптографической защиты; процедуры распределения и сертификации криптографических ключей; типовые схемы обеспечения информационной безопасности компьютерных систем; • ***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 информа-		

	ции и подготовки соответствующей научно-технической документации.		
ПК-6 Способность участвовать в разработке проектной и технической документации	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***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-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.		
ПК-8 Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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** методологией проектирования систем защиты информации, практическими навыками применения современных компьютерных технологий, построением математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры, оценивать эффективность их применения.		
ПСК-2.1 Способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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.		
ПСК-2.2 Способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах.	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** 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.		
ПСК-2.3 Способность строить математические модели для оценки безопасности компьютерных си-	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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		

стем и анализировать компоненты системы безопасности с использованием современных математических методов.	иностранные стандарты безопасности компьютерных систем; • ***уметь*:** строить 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; • ***владеть*:** навыками построения математических моделей информационных процессов в компьютерных системах и навыками их алгоритмизации; методикой анализа вычислительной эффективности алгоритмов.		
ПСК-2.4 Способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	В результате подготовки к процедуре защиты выпускной квалификационной работы студент должен: • ***знать*:** методы алгебры, теории чисел, алгебраической геометрии и дискретной математики и их применение в моделях информационных процессов и в сертифицированных программно-аппаратных средствах защиты информации; знать методологию оценки адекватности применяемых математических моделей; • ***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.		
ПСК-2.5 Способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных	В результате подготовки к процедуре защиты выпускной квалификационной работы студент 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;		

средств защиты информации учетом современных и перспективных математических методов 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.		

4.1. Примерная тематика выпускных квалификационных работ по специальности 10.05.01 «Компьютерная безопасность» (специализация «Математические методы защиты информации»).

1. Исследование асимптотической сложности проблемы «Скрытой информации».
2. Оптимизация алгоритма Коча с использованием искусственной нейронной сети и выбор наиболее подходящего блока для встраивания цифрового водяного знака.
3. Построение комплексной системы информационной безопасности в учреждении здравоохранения.
4. Построение кодов, ассоциированных с торическими поверхностями.
5. Исследование условий применимости атаки Винера на криптосистему Ривеста – Шамира – Адлемана.
6. Реализация метода вычисления числа рациональных точек на кривых Артина – Шрайера над конечными полями.
7. Разработка комплекса лабораторных работ по применению средств защиты информации от несанкционированного доступа.
8. Организация централизованной аутентификации пользователей для распределённых систем.
9. Анализ, оптимизация и распараллеливание алгоритма декодирования Фенга – Рао на алгебраических кривых.
10. Анализ математических оснований криптосистемы с открытым ключом, основанной на группе Судзуки.
11. Разработка системы защищенного обмена для мобильных телефонов с использованием отечественной криптографии.
12. Разработка программной системы обнаружения вторжений с возможностью анализа трафика службы доменных имен.
13. Построение политики информационной безопасности для критически важного объекта на основе формальной модели управления доступом и информационными потоками.
14. Анализ безопасности цифровых подписей Ксинмея и Алабади – Викера.
15. Сравнительный анализ процедур декодирования на эрмитовой кривой и квартике Клейна.
16. Реализация алгоритма слепой подписи на базе стандарта цифровой подписи
17. Разработка, анализ стойкости и реализация основных алгоритмов шифрования СМС-сообщений на основе решёток в мобильной системе Windows Phone 8.
18. Обеспечение устойчивости цифровых водяных знаков, используемых для защиты авторских прав.

19. Обнаружение стеговложений в графических файлах.
20. Реализация алгоритма короткой цифровой подписи на основе спариваний Вейля.
21. Реализация криптосистемы с открытым ключом на основе идентификационных данных.
22. Сравнительный анализ стеганографических методов сокрытия информации в графических файлах.
23. Анализ эффективности алгоритма сложения в якобиане кривой Пикара и его реализация для криптографии.
24. Вычисление группы автоморфизмов некоторых кодов, ассоциированных с квартикой Клейна.
25. Реализация и анализ безопасности некоторых пороговых цифровых подписей.
26. Классификация экстремальных кодов с использованием их групп автоморфизмов.
27. Сравнительный анализ параметров однолинейных и двухлинейных кодов, ассоциированных с антиканоническими поверхностями.
28. Анализ безопасности схемы компактных электронных денег.
29. Вычисление дзета-функции башни Гарсии – Штихтенота.
30. Вычисление производящей функции графа, связанного с кривой Ван дер Хеера – Ван дер Флухта.
31. Особенности межсетевого экранирования и реализация персонального межсетевого экрана для протокола IPv6.
32. Защита от атак на протоколы шифрования беспроводных сетей.
33. Разработка схемы распределения ключей для облачных систем, допускающих перешифрование.
34. Анализ и реализация расширенного протокола Джоукса для многосторонней сверки ключей.
35. Анализ и реализация алгоритмов кодирования и декодирования NXL и XNL-кодов на основе алгоритма Судана.
36. Исследование свойств алгеброгеометрических кодов, ассоциированных с кривой Пикара
37. Исследование свойств первых ступеней башни функциональных полей Гарсии – Штихтенота и свойств соответствующих алгеброгеометрических кодов.
38. Моделирование угроз информационной безопасности критически важного объекта с использованием национального Банка угроз и уязвимостей.
39. Разработка и реализация политики безопасности для защиты виртуальной инфраструктуры
40. Разработка и исследование свойств протоколов почтового обмена внутри гибридного облака с двумя перешифрованиями на основе спаривания Хесса.
41. Приложение кодов Гоппы к криптосистемам Мак-Элиса и Нидеррайтера.
42. Разработка и анализ вычислительной эффективности основных криптографических алгоритмов на суперэллиптических кривых.
43. Разработка семейства протоколов на эллиптических кривых для децентрализованных приложений в индустрии азартных игр.
44. Анализ структуры и стойкости криптосистемы «Три медведя».
45. Анализ состояния защищенности информационной системы с помощью средств тестирования на проникновение.

46. Разработка и реализация специализированного комплекса для сбора и классификации информации на основе открытых источников (OSINT).
47. Исследование структуры якобиана гиперэллиптической кривой рода 3.
48. Оптимизация вычислений в группе точек эллиптической кривой.
49. Реализация и анализ BLS-схемы на эллиптических кривых.
50. Сведение дискретного логарифма на гиперэллиптических кривых рода 2 к конечному полю с помощью билинейных спариваний.
51. Гомоморфное выполнение нейронных сетей.
52. Построение модели защиты персональных данных пользователей в социальных сетях.
53. Анализ производительности типовых операций над точками эллиптической кривой при использовании различных систем координат.

4.2. Примеры формулировки тем и содержания выпускных квалификационных работ

Тема: ***Анализ стойкости криптосистемы «Три медведя»***

Содержание:

Введение

1. Предварительные сведения

1.1. Понятие решетки

1.2. Кратчайший вектор решетки

1.3. Фундаментальный параллелепипед .

1.4. Ортогонализация Грама-Шмидта

1.5. Задачи на решетках

1.6. Редукция решеток

2. Концепция обучения с ошибками

2.1. Определение задачи LWE

2.2. Определение задачи RLWE

2.3. Определение задачи I-RLWE

2.4. Сводимость задачи I-RLWE к задаче RLWE и наоборот

3. Описание криптосистемы «Три медведя»

3.1. Выбор параметров криптосистемы

3.2. Распределение ошибок криптосистемы

3.3. Режимы работы криптосистемы

3.4. Корректировка шумового параметра

3.5. Ключевой обмен, использующий I-RLWE

3.6. Процесс передачи сообщения

4. Решение задачи I-RLWE

4.1. Число целочисленных векторов в сфере заданного радиуса

4.2. Задача о рюкзаке

4.3. Решение задачи I-RLWE с помощью решетки

4.4. Время нахождения короткого вектора в решетке

Заключение

Список литературы

Приложение 1

Приложение 2 .

Литература:

1. P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science : Conference Publications, 1997. – 25 с.
2. M. Roetteler, M. Naehrig, K.M. Svore, K. Lauter. Quantum resource esti-mates for computing elliptic curve discrete logarithms. In: Takagi, T., Peyrin, T. (eds.), Asiacrypt 2017 (2), Springer LNCS 10625, 2017. – С. 241–270.
3. V. Lyubashevsky, C. Peikert, O. Regev. On ideal lattices and learning with er-rors over rings. In Advances in Cryptology – Eurocrypt 2010, 2010. – 23 с.
4. Gu Chunsheng. Integer version of ring-LWE and its applications. Cryptology ePrint Archive, Report 2017/641, 2017. – 15 с.
5. M. Hamburg. Module-LWE key exchange and encryption: The three bears. Technical report, National Institute of Standards and Technology, 2017.− 28 с.
6. M.R. Albrecht, et al. Estimate all the {{LWE, NTRU}} schemes! IACR Cryptology ePrint Archive, 2018. − 54 с.
7. M.J. Coster, A. Joux, B.A. La Macchia, A.M. Odlyzko, C.P. Schnorr and J. Stern, An improved lowdensity subset sum algorithm, Computational Complexity 2, 1992. – С. 111-128.
8. M.R. Albrecht, F. Gopfert, F. Virdia, T. Wunderer. Revisiting the expected cost of solving uSVP and applications to LWE. Cryptology ePrint Archive, Report 2017/815, 2017. – 28 с.
9. S. Khot. Hardness of approximating the shortest vector problem in lattices. In Proceedings of the 45th IEEE Symposium on Foundations of Computer Science, 2004.– 20 с.
10. O. Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In Proc. of STOC ’05, 2005. – С. 84–93.
11. O. Regev . The learning with errors problem. Invited survey in CCC 2010, 2010. − 23 с.
12. Blum, A. Kalai, H. Wasserman. Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model. Journal of the ACM 50(4), 2003. – 13 с.
13. M. Alekhnovich. More on average case vs approximation complexity. In Proc. 44th Annual IEEE Symp. on Foundations of Computer Science (FOCS), 2003.− С. 298-307. 46
14. V. Singh, A Practical Key Exchange for the Internet using Lattice Cryptography, 2015. − С. 21-22.
15. C. Peikert. How (not) to instantiate ring-LWE. Cryptology ePrint Archive, Report 2016/351 2016. – 29 с.
16. C. Peikert, A Decade of Lattice Cryptography. Cryptology ePrint Archive, Report 2015/939, 2016. – 90 с.
17. D. Dadush, O. Regev, N. Stephens-Davidowitz, "On the Closest Vector Problem with a distance guarantee", IEEE 29th Conference on Computational Com-plexity, 2014. – С. 98-109.
18. О.В. Кузьмин, В.С. Усатюк. Программный комплекс приведения базиса целочисленных решеток// Программные продукты и системы, №4(100), 2012. – С. 180-183.
19. Becker, L. Ducas, N. Gama, T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In SODA ’16 Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete Algorithms, SIAM, 2016. – 15 с.

Тема: ***Разработка и исследование свойств протоколов почтового обмена внутри гибридного облака с двумя перешифрованиями на основе спаривания Хесса*»**

Содержание:

Введение
1. Обзор предварительных результатов
1.1. Краткие сведения по эллиптическим кривым над конечными полями
1.2. Обзор спариваний на эллиптических кривых
1.3. Алгоритм Миллера
1.4. Обзор систем защиты облачных вычислений
2. Основные теоретические результаты
2.1. Протокол
2.2. Схема цифровой подписи и аутентификации пользователей
2.3. Обзор и анализ различных спариваний на эллиптических кривых
2.4. Общий алгоритм спаривания Хесса
2.5. Общие оценки вычислительной эффективности алгоритмов Хесса и перешифрования
2.6. Оценка криптостойкости протокола
3. Алгоритмы
3.1. Детализированный алгоритм вычисления спаривания Хесса на эллиптических кривых
4. Описание программного комплекса
4.1. Выбор языка программирования
4.2. Описание программного комплекса
5. Примеры
5.1 Пример 1
5.2. Пример 2
5.3. Пример 3
Заключение
Список литературы
Приложение
Тексты компьютерных программ

Литература:

1. Miller V.S.. The Weil pairing, and its efficient calculation. Journal of Cryptology, 17:235–261, 2004.
2. Hess F. Pairing lattices. In S. D. Galbraith and K. Paterson, editors, Pairing-Based Cryptography – Pairing 2008, volume 5209 of Lecture Notes in Computer Science, pages 18–38, Berlin, 2008. Springer-Verlag.
3. Washington L.C. Elliptic curves: number theory and cryptography. – Chapman & Hall/CRL, 2008.
4. Boneh D., Franklin M. Identity-Based Encryption from the Weil Pairing. SIAM J. of Computing, Vol. 32, № 3, pp. 586-615, 2003.
5. Enge A. Bilinear pairings on elliptic curves. 2013. HAL Id: hal-00767404.

6. Батура Т.В., Мурзин Ф.А., Семич Д.Ф. Облачные технологии: основные понятия, задачи и тенденции развития. — Программные продукты и системы и алгоритмы, №1, 2014.
7. Безкоровайный Д. Комплексная защита данных в публичных облаках. — Storage News №1, pp. 16-19, 2013.
8. Wu X., Xu L., Zhang X. A Certificateless Proxy Re-Encryption Scheme for Cloud-based Data Sharing. 2011.
9. Алешников С.И., Алешникова М.В., Горбачёв А.А. Протокол доверенного шифрования на основе модифицированного алгоритма вычисления спаривания Вейля на алгебраических кривых для облачных вычислений. — Информационные технологии. – 2013. - №9. - С.36-39.
10. Menezes A. J., Oorschot P. v., Vanstone S. A. 11.5.2 The ElGamal signature scheme. — Handbook of Applied Cryptography — CRC Press, 1996.
11. FIPS PUB 186-4. — Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD, 2013.
12. Koblitz N., Menezes A. Another Look at Generic Groups. — 1995.
13. ГОСТ Р 34.10-2012. Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — ФГУП Стандартинформ, 2013.
14. Barreto P.S.L.M., Galbraith S.D., .O'h.Eigeartaigh C., Scott M. Efficient pairing computation on supersingular abelian varieties. Designs, Codes and Cryptography, 42:239–271, 2007.
15. Hess F., Smart N.P., Vercauteren F.. The eta pairing revisited. IEEE Transactions on Information Theory, 52(10):4595–4602, 2006.
16. Zhao C., Zhang F., Huang J.. A note on the Ate pairing. International Journal of Information Security, 7(6):379–382, 2008.
17. Lee E., Lee H., Park C.. Efficient and generalized pairing computation on abelian varieties. IEEE Transactions on Information Theory, 55(4):1793–1803, 2009.
18. Vercauteren F.. Optimal pairings. IEEE Transactions on Information Theory, 56(1):455–461, 2010.
19. Страуструп Б. Язык программирования C++. Специальное издание — М.: Бином-Пресс, 2007. — 1104 с. — ISBN 5-7989-0223-4.
20. User's Guide to the PARI library. — The PARI Group, 2016.
21. Tilborg H.v.C.A., Jajodia S. Encyclopedia of Cryptography and Security. — Springer, 2011. – 1416 с. — ISBN 978-1-4419-5905-8.
22. Gashkov S.B., Sergeev I.S.. Complexity of computation in Finite Fields. — Journal of Mathematical Sciences, Vol. 191, No. 5, 2013.

ПРИЛОЖЕНИЯ

Приложение 1

Титульный лист ВКР

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
Балтийский федеральный университет им. И. Канта
Институт физико-математических наук и информационных технологий

Рекомендована к защите:
методический руководитель
направления подготовки

к.т.н., доцент ИФМНиИТ
_____ С.И.Алешников

"____"_____ 2019 г.

Допущена к защите:
первый заместитель директора
института физико-математических
наук и информационных технологий
к. ф.-м. н., доцент
_____ А.А. Шпилевой

"____"_____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: «XXXXXXX»

ВКР защищена на оценку:
_____

Руководитель: к.ф.-м.н., доцент
_____ А.А.Петров

Выполнил: студент 6 курса специальности «Компьютерная безопасность»
_____ И.И.Иванов

Рецензент: генеральный директор ООО «XXX»
_____ П.П.Сидоров

Калининград
2019

Приложение 2

Оценочный лист сформированности компетенций для руководителя ВКР и членов ГЭК

Коды проверяемых компетенций	Текст ВКР	Этап подготовки к процедуре защиты ВКР
ОК-1	+	+
ОК-2	+	+
ОК-3	+	+
ОК-4	+	+
ОК-6	+	+
ОК-9	+	+
ОПК-1	+	+
ОПК-2	+	+
ОПК-3	+	+
ОПК-4	+	+
ОПК-5	+	+
ОПК-6	+	+
ОПК-7	+	+
ОПК-8	+	+
ОПК-9	+	+
ОПК-10	+	+
ПК-1	+	+
ПК-5	+	+
ПК-6	+	+
ПК-7	+	+
ПК-8	+	+
ПСК-2.1	+	+
ПСК-2.2	+	+
ПСК-2.3	+	+
ПСК-2.4	+	+
ПСК-2.5	+	+

Приложение 3

Оценочный лист членов ГЭК

Оценка уровня сформированности компетенций студента _____ специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» в процессе защиты выпускной квалификационной работы, выполненной на тему

_____

_____

Коды проверяемых компетенций	Показатели оценки результата	Показатели уровня сформированности компетенций			
		2 – низкий	3 – средний	4 – достаточный	5 – высокий
ОК-1	Способность использовать основы философских знаний для формирования мировоззренческой позиции.				
ОК-2	Способность использовать основы экономических знаний в различных сферах деятельности.				
ОК-3	Способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма				
ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности.				
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия				
ОК-9	Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности				
ОПК-1	Способность анализировать физические явления и процессы при решении профессиональных задач				
ОПК-2	Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей и математической статистики, теории информации, теоретико-числовых методов.				
ОПК-3	Способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных ис-				

	точниках информации.				
ОПК-4	Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.				
ОПК-5	Способность использовать нормативные правовые акты в своей профессиональной деятельности				
ОПК-6	Способность применять методы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций				
ОПК-7	Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения				
ОПК-8	Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач				
ОПК-9	Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.				
ОПК-10	Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах				
ПК-1	Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности.				
ПК-5	Способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.				
ПК-6	Способность участвовать в разработке проектной и технической документации				
ПК-7	Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем.				
ПК-8	Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы.				
ПСК-2.1	Способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации				

ПСК-2.2	Способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах.				
ПСК-2.3	Способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.				
ПСК-2.4	Способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации				
ПСК-2.5	Способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации.				

Приложение 4

Форма отзыва руководителя

Отзыв

на выпускную квалификационную работу
студента(ки) 6-го курса института физико-математических наук и информационных технологий
специальности «Компьютерная безопасность» Ф.И.О. студента
«……*Тема ВКР*……»

- Формулировка проблемы.
- Актуальность проблемы.
- Состояние решения проблемы на данный момент.
- Конкретная задача, решению которой посвящена данная ВКР, её актуальность.
- Что реально сделано по главам ВКР.
- Достоинства работы: оригинальность, новизна и научная значимость результатов; научный уровень и глубина работы; доказательность и достоверность результатов; широта охвата материала и качество обзора литературы по теме, обоснованность выводов; наличие компьютерной реализации; степень практической реализации.
- Отношение студента к работе: добросовестность, дисциплинированность, систематичность, самостоятельность, активность, глубина и эрудированность, творческий подход.
- Недостатки работы:
  - отступления от утверждённого плана работы……
  - недостатки содержания…….
  - недостатки оформления……
- В какой степени студент справился с решением поставленной задачи – оценка соответствия ВКР требованиям, предъявляемым к выпускным квалификационным работам студентов института физико-математических наук и информационных технологий специальности «Компьютерная безопасность».
- Предлагаемая оценка.

Научный руководитель,

должность, уч. степень, уч. звание. Ф.И.О.

Приложение 5

Форма рецензии

РЕЦЕНЗИЯ
на выпускную квалификационную работу
студента(ки) 6 курса института физико-математических наук и
информационных технологий
специальности «Компьютерная безопасность» Ф.И.О. студента
«……*Тема ВКР*……..»

- Формулировка проблемы.
- Актуальность проблемы.
- Состояние решения проблемы на данный момент.
- Конкретная задача, решению которой посвящена данная ВКР, её актуальность.
- Критический анализ общего замысла, основных положений и результатов работы по главам ВКР.
- Достоинства работы: оригинальность, новизна и научная значимость результатов; научный уровень и глубина работы; доказательность и достоверность результатов; широта охвата материала и качество обзора литературы по теме, обоснованность выводов; наличие компьютерной реализации; степень практической реализации.
- Недостатки работы:
  - недостатки содержания: …..……
  - недостатки оформления……..
- Оценка соответствия ВКР требованиям, предъявляемым к выпускным квалификационным работам студентов института физико-математических наук и информационных технологий специальности «Компьютерная безопасность».
- Предлагаемая оценка.

Должность, уч. звание, уч. степень
Рецензента Ф.И.О.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Балтийский федеральный университет им. Иммануила Канта

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ Е.П.Новикова
«15» февраля 2019 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«25» февраля 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование: «Защита выпускной квалификационной работы»

для студентов 6 курса
очной формы обучения
специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»
уровень высшего образования - специалитет

Калининград

2019

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. Общая характеристика процедуры государственной итоговой аттестации выпускника по специальности 10.05.01 «Компьютерная безопасность», уровень высшего образования – специалитет 4
1.1 Общие положения 4
1.2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы 4
1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 7
2. Процедура защиты выпускной квалификационной работы в Государственной экзаменационной комиссии 8
2.1. Порядок защиты выпускной квалификационной работы на заседании ГЭК 8
2.2. Описание показателей и критериев оценивания компетенций 9
2.3. Шкала оценивания степени сформированности компетенций 10
3. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины 12
3.1. Основная литература 12
3.2. Дополнительная литература 12
4. Фонд оценочных средств для проведения защиты выпускной квалификационной работы 13
4.1. Примерная тематика выпускных квалификационных работ по специальности 10.05.01 «Компьютерная безопасность» (специализация «Математические методы защиты информации»). 16
4.2. Примеры формулировки тем и содержания выпускных квалификационных работ 18
ПРИЛОЖЕНИЯ 22

1. Общая характеристика процедуры государственной итоговой аттестации выпускника по специальности 10.05.01 «Компьютерная безопасность», уровень высшего образования – специалитет

1.1 Общие положения

Программа ГИА является частью основной профессиональной образовательной программы в соответствии с ФГОС ВО в части государственных требований к минимуму содержания и уровню подготовки выпускников по специальности 10.05.01 «Компьютерная безопасность».

ГИА выпускников по специальности 10.05.01 «Компьютерная безопасность» является заключительным этапом обучения, подтверждающего квалификацию «Специалист по защите информации».

К ГИА допускаются лица, выполнившие требования, предусмотренные курсом обучения по основной образовательной программе по специальности 10.05.01 «Компьютерная безопасность» и успешно прошедшие все промежуточные аттестационные испытания по теоретическому и практическому этапам обучения, предусмотренные утвержденным учебным планом специальности «Компьютерная безопасность», специализации «Математические методы защиты информации».

Видом ГИА в соответствии с п. 6.8 ФГОС ВО и учебным планом является защита выпускной квалификационной работы.

Аттестацию проводит Государственная Экзаменационная Комиссия (ГЭК). Председатель ГЭК и состав ГЭК утверждаются в установленном порядке.

Выпускная квалификационная работа выполняется в обязательном порядке, в установленные сроки, проходит рецензирование и защищается в ГЭК.

Государственная итоговая аттестация (ГИА) специальности включает в себя два основных этапа – этап подготовки к процедуре защиты выпускной квалификационной работы (Б3.Б.01(Д)) и этап защиты выпускной квалификационной работы (Б3.Б.02(Д)).

Наименование дисциплины (модуля) – «Защита выпускной квалификационной работы».

1.2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Целью освоения дисциплины «Защита выпускной квалификационной работы» является защита выпускной квалификационной работы.

В ходе защиты выпускной квалификационной работы, обучающиеся должны показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные универсальные и профессиональные компетенции, профессионально презентовать результаты своей работы, научно аргументировать и защищать свою точку зрения в ходе презентации.

Выпускник специальности 10.05.01 «Компьютерная безопасность» (специализация «Математические методы защиты информации») с квалификацией Специалист по защите

информации в соответствии с целями основной образовательной программы и задачами профессиональной деятельности в результате освоения данной дисциплины ООП специальности должен обладать следующими компетенциями:

Код компетенции	**Результаты освоения ООП Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
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.	В ходе защиты выпускной квалификационной работы студент должен: • ***знать*****:** роль и значение компьютерной безопасности в обеспечении интересов России и её граждан; характер профессиональной деятельности по обеспечению информационной безопасности в условиях информационного противоборства; проблемы и задачи, возникающие при обеспечении информационной безопасности предприятия и защиты персональных данных. • ***уметь*****:** объяснять познавательную и практическую сущность математических, компьютерных и технических методов защиты информации как мотивационной основы профессиональной деятельности; • ***владеть*****:** базовыми математическими методами обеспечения информационной безопасности; профессиональными компетенциями, необходимыми для применения основных правовых актов, регулирующих сферу информационной безопасности.
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 ходе защиты выпускной квалификационной работы студент 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.
ОК-8	Способность к самоорганизации и самообразованию.	В ходе защиты выпускной квалификационной работы студент должен: • ***знать*****:** свои ресурсы и их пределы (личностные, ситуативные, временные); правила и нормы здорового образа жизни; основную профессиональную литературу и Интернет-ресурсы в области компьютерной безопасности и смежных областях, способные служить для самообразования; • ***уметь*****:** определять приоритеты профессиональной деятельно-

		сти; 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; навыками выстраивания гибкой траектории своего доклада и презентации.
ПК-1	Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности.	В ходе защиты выпускной квалификационной работы студент должен: • ***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-3	Способность про-	В ходе защиты выпускной квалификационной работы студент

	водить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.	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 ходе защиты выпускной квалификационной работы студент 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 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.

1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины **«Защита выпускной квалификационной работы»** составляет 2 зачетные единицы и 72 академических часа.

Объем дисциплины по видам учебных занятий (в часах)

Объем дисциплины	**Всего часов**		
	для очной формы обучения	**для заочной формы обучения**	**очно-заочной формы обучения**
Общая трудоемкость дисциплины	**72**	–	–
Контактная работа обучающихся с преподавателем (по видам учебных занятий)	**1**	–	–

(всего)			
Аудиторная работа (всего):		–	–
в т. числе:			
Лекции		–	–
Практические занятия		–	–
Лабораторные работы		–	–
Групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем		–	–
Самостоятельная работа обучающихся (всего)	**71**	–	–
Вид промежуточной аттестации обучающегося (зачет / экзамен)		–	–

Место и время проведения государственной итоговой аттестации

Порядок и сроки проведения аттестационных испытаний устанавливаются в соответствии с графиком учебного процесса по специальности 10.05.01 «Компьютерная безопасность» специализации «Математические методы защиты информации» на основании Положения об организации выполнения и защиты выпускной квалификационной работы обучающимися (студентами) от 15.05.2014 г., утвержденного Ученым советом БФУ (протокол № 10 от 12 мая 2014 г.).

2. Процедура защиты выпускной квалификационной работы в Государственной экзаменационной комиссии

Защита выпускной квалификационной работы проводится в установленное время на заседании экзаменационной комиссии по соответствующей специальности ГЭК БФУ им. И. Канта. Кроме членов комиссии на защите необходимо присутствие научного руководителя или рецензента, а также возможно присутствие других студентов, преподавателей и администрации БФУ им. И. Канта.

2.1. Порядок защиты выпускной квалификационной работы на заседании ГЭК

1. Защита начинается с доклада студента по теме выпускной квалификационной работы. На доклад по выпускной квалификационной работе отводится до 8 минут.

Доклад следует начинать с обоснования актуальности избранной темы, описания научной проблемы и формулировки цели работы (не более 2 мин), а затем в последовательности, установленной логикой проведенного исследования, по главам раскрывать основное содержание работы, обращая особое внимание на наиболее важные разделы и интересные

результаты, критические сопоставления и оценки (около 5 мин). Заключительная часть доклада строится по тексту заключения выпускной квалификационной работы, перечисляются общие выводы из её текста без повторения частных обобщений, сделанных при характеристике глав основной части, собираются воедино основные рекомендации (примерно 1 мин). Студент должен излагать основное содержание своей выпускной квалификационной работы свободно, не читая письменного текста.

Рекомендуется в процессе доклада использовать заранее подготовленный наглядный графический материал (таблицы, схемы), иллюстрирующий основные положения работы. Все материалы, выносимые на наглядную графику, должны быть оформлены так, чтобы студент мог демонстрировать их без особых затруднений, и они были видны всем присутствующим в аудитории. В среднем насыщенность одного плаката (слайда) информацией должна быть эквивалентна 10-15 строкам текста, не более. Плакаты (слайды) нумеруются в первом верхнем углу. Весь плакат (слайд) или его части должны иметь заголовок–название: Постановка задачи, Структурная схема системы и т.д. Обычно плакаты (слайды) соответствуют разделам или подразделам работы.

2. После завершения доклада члены ГЭК задают студенту вопросы, как непосредственно связанные с темой ВКР, так и близко к ней относящиеся. При ответах на вопросы студент имеет право пользоваться своей работой.

3. После ответов студента на вопросы слово предоставляется научному руководителю. В конце своего выступления научный руководитель даёт свою оценку выпускной квалификационной работе.

4. При защите выпускной квалификационной работы после выступления научного руководителя слово предоставляется рецензенту. В случае отсутствия последнего на заседании ГЭК его отзыв зачитывает секретарь ГЭК. В конце своего выступления рецензент даёт свою оценку работе.

5. После выступления рецензента начинается обсуждение работы или дискуссия. В дискуссии могут принять участие как члены ГЭК, так и присутствующие заинтересованные лица.

6. После окончания дискуссии студенту предоставляется заключительное слово. В своём заключительном слове студент должен ответить на замечания рецензента, соглашаясь с ними или давая обоснованные возражения. Признаком хорошего тона являются слова благодарности в адрес членов ГЭК, научного руководителя и рецензента.

7. Решение ГЭК об итоговой оценке основывается на:

- оценке научного руководителя за работу, включая текущую работу в семестре;
- оценке рецензента за работу в целом;
- оценке членов ГЭК за содержание работы, её защиту, включая доклад, ответы на вопросы и замечания рецензента.

2.2. Описание показателей и критериев оценивания компетенций

Степень сформированности компетенций в результате защиты выпускной квалификационной работы осуществляется комиссией в ходе доклада по теме ВКР и ответах студента на вопросы в дискуссии.

1. В качестве **критериев** для оценки выпускной квалификационной работы научные руководители и члены ГЭК должны иметь в виду:

- актуальность темы и задач работы;
- соответствие тематики специальности «Компьютерная безопасность»;
- обоснованность результатов и выводов;
- определенную оригинальность новизну полученных данных;
- самостоятельность (личный вклад студента);
- возможности практического использования полученных результатов.

2. Обоснованность результатов и выводов определяются с позиций:

- соответствия известным научным положениям и фактам;
- логичности в изложении и обсуждении собственных данных;
- корректности постановки опыта, эксперимента;
- корректности использования математических методов.

При этом должны учитываться:

- уровень устного доклада на защите;
- соответствие оформления работы установленным требованиям;
- качество иллюстративного материала к докладу.

3. Оригинальность и новизна полученных данных определяется как:

- установление нового научного факта или подтверждение известного факта для новых условий;
- получение сведений, приводящих к формулировке проверяемых гипотез, которые требуют дальнейшей проверки;
- разработка оригинального метода решения известной задачи;
- применение известных методик для решения новых задач;
- введение в научный оборот новых данных;
- обоснованное решение поставленной задачи.

4. Личный вклад студента определяется: степенью самостоятельности в выборе темы, постановке задач, планировании и организации исследования, обработке и осмыслении полученных результатов.

5. Возможность практического использования данных, полученных в ВКР, определяется в отношении НИР, выполняемых в университете или в других организациях; задачами совершенствования учебного процесса; возможностью публикации в печати.

2.3. Шкала оценивания степени сформированности компетенций

Выпускная квалификационная работа оценивается по четырехбальной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».

ВКР, получающая, по мнению руководителя или рецензента оценку «неудовлетворительно», может быть в отдельных случаях направлена на дополнительное рецензирование по распоряжению председателя ГЭК.

Выпускная квалификационная работа оценивается членами ГЭК на основании доклада студента и выступления рецензента. Члены ГЭК оценивают уровень работы не только на основе перечисленных критериев (см. предшествующий раздел), а также обязательно принимают во внимание умение выпускника представить свою работу и правильно ответить на вопросы членов ГЭК.

Оценка **«ОТЛИЧНО»** ставится за реализацию всех необходимых компетенций в ходе доклада по теме ВКР и ответах на вопросы в дискуссии (высокий уровень сформированных компетенций): выпускная квалификационная работа имеет исследовательский характер, грамотно изложена теоретическая часть, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями. При её защите студент показывает глубокие знания вопросов темы. Выпускная квалификационная работа имеет положительные отзывы научного руководителя и рецензента.

Оценка **«ХОРОШО»** ставится за частичную реализацию всех необходимых компетенций в ходе доклада по теме ВКР и ответах на вопросы в дискуссии (уровень освоения компетенций достаточный): выпускная квалификационная работа содержит элементы научного исследования, грамотно изложена теоретическая часть, логичное, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными предложениями. При её защите студент показывает знания вопросов темы, оперирует данными исследования, во время доклада использует наглядные пособия, без особых затруднений отвечает на поставленные вопросы. Выпускная квалификационная работа имеет положительные отзывы научного руководителя и рецензента.

Оценка **«УДОВЛЕТВОРИТЕЛЬНО»** ставится в том случае, если студент демонстрирует частичную сформированность компетенций (средний уровень), предусмотренных ФГОС: выпускная квалификационная работа имеет технический характер, базируется на практическом материале, но анализ выполнен поверхностно, в ней просматривается непоследовательность изложения материала. Представлены необоснованные предложения. При её защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не дает полных аргументированных ответов на заданные вопросы. В отзывах научного руководителя и рецензента имеются замечания по содержанию работы и методике анализа.

Оценка **«НЕУДОВЛЕТВОРИТЕЛЬНО»** выставляется, если демонстрируется несформированность (низкий уровень сформированности) соответствующих компетенций, предусмотренных ФГОС ВО: выпускная квалификационная работа не носит исследовательского характера, не отвечает требованиям, изложенным в методических рекомендациях. В работе нет выводов, либо они носят декларативный характер. При защите работы студент затрудняется отвечать на поставленные вопросы, при ответе допускает существенные ошибки. В отзывах научного руководителя и рецензента имеются серьезные критические замечания.

Итоговая оценка ГЭК выводится по принципу учета оценок большинства членов ГЭК, а также руководителя. Оцениваемые компетенции и оценочный лист приведены в *Приложениях* №1 и №2, соответственно.

Итоговая оценка за защиту ВКР складывается из оценок:

- демонстрационных материалов (презентации результатов работы);
- доклада на защите;
- ответов на вопросы членов комиссии.

Руководитель ВКР и члены ГЭК по итогам защиты ВКР оценивают уровень сформированности компетенций по:

- качеству демонстрационного материала,
- содержательности и логичности представленного доклада,
- ответам на заданные вопросы.

По результатам группового обсуждения всех присутствующих членов ГЭК председатель заполняет оценочный лист (*Приложение* №2).

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

3.1. Основная литература

1. Емельянова, И. Н. Основы научной деятельности студента. Магистерская диссертация [Электронный ресурс]: учеб. пособие для вузов/ И. Н. Емельянова; Тюмен. гос. ун-т. – Москва: Юрайт, 2018 1r=**on-line**, 115 с. Language: Russian, База данных: Каталог НБ БФУ им. И. Канта – Книги.

3.2. Дополнительная литература

1. Байбородова, Л. В. Методология и методы научного исследования [Электронный ресурс]: учеб. пособие для бакалавриата и магистратуры/ Л. В. Байбородова, А. П. Чернявская. – Москва: Юрайт, 2018 1r=**on-line**, 221 с. Language: Russian, База данных: Каталог НБ БФУ им. И. Канта – Книги.
2. Горелов, Н. А. Методология научных исследований [Электронный ресурс]: учеб. и практикум для бакалавриата и магистратуры/ Н. А. Горелов, Д. В. Круглов, О. Н. Кораблева. - 2-е изд., перераб. и доп.. - Москва: Юрайт, 2019 1r=**on-line**, 365 с.: а-ил. Language: Undetermined, База данных: Каталог НБ БФУ им. И. Канта - Книги
3. Дрещинский, В. А. Методология научных исследований [Электронный ресурс]: учеб. для бакалавриата и магистратуры/ В. А. Дрещинский. - 2-е изд., перераб. и доп.. – Москва: Юрайт, 2018 1r=**on-line**, 324 с. Language: Russian, База данных: Каталог НБ БФУ им. И. Канта – Книги.
4. Методические рекомендации по написанию и защите выпускных квалификационных работ студентов-бакалавров [Электронный ресурс]: метод. рекомендации/ Балт. федер. ун-т им. И. Канта, Ин-т образования; [сост. А. О. Бударина [и др.]. - Калининград: Изд-во БФУ им. И. Канта, 2018 **on-line**, 25 с.. - Библиогр.: с. 17 (2 назв.). - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1) Свободны / free: ЭБС Кантиана(1).

Программное обеспечение и Интернет-ресурсы

1. Операционная система Microsoft Windows.
2. Пакет Microsoft Office (MS Word, MS Excel, MS PowerPoint, MS Access, MS Project, MS Visio).
3. Справочно-поисковые системы «Консультант плюс» или «Гарант».
4. Microsoft SQL Srv Standard Core 2014 (Количество лицензий – 4, Номер акта / накладной – Tr063168, Дата акта – 24.11.14);
5. Microsoft Visual Studio 2005 (Количество лицензий – 30, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).

4. Фонд оценочных средств для проведения защиты выпускной квалификационной работы

Компетенция	*Перечень планируемых результатов*	*Диагностический инструмент*	*Критерии оценки*
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.	В ходе защиты выпускной квалификационной работы студент должен: • ***знать*:** роль и значение компьютерной безопасности в обеспечении интересов России и её граждан; характер профессиональной деятельности по обеспечению информационной безопасности в условиях информационного противоборства; проблемы и задачи, возникающие при обеспечении информационной безопасности предприятия и защиты персональных данных. • ***уметь*:** объяснять познавательную и практическую сущность математических, компьютерных и технических методов защиты информации как мотивационной основы профессиональной деятельности; • ***владеть*:** базовыми математическими методами обеспечения информационной безопасности; профессиональными компетенциями, необходимыми для применения основных правовых актов, регулирующих сферу информационной безопасности.	1. Актуальность тематики работы и её соответствие профилю специальности «Компьютерная безопасность». 2. Степень полноты обзора состояния вопроса и корректность постановки задачи. 3. Уровень и корректность использования в работе методов исследований, математического моделирования, расчетов. 4. Степень комплексности работы, применение в ней знаний общепрофессиональных и специальных дисциплин. 5. Ясность, четкость, последовательность и обоснованность изложения.	Глубокое раскрытие темы, качественное оформление работы, содержательность доклада и презентации.
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 ходе защиты выпускной квалификационной работы студент 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.		
ОК-8	В ходе защиты выпускной квалификационной работы		

Способность к самоорганизации и самообразованию.	студент должен: • ***знать*:** свои ресурсы и их пределы (личностные, ситуативные, временные); правила и нормы здорового образа жизни; основную профессиональную литературу и Интернет-ресурсы в области компьютерной безопасности и смежных областях, способные служить для самообразования; • ***уметь*:** определять приоритеты профессиональной деятельности; 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; навыками выстраивания гибкой траектории своего доклада и презентации.	6. Применение современного математического и программного обеспечения, компьютерных технологий в работе. 7. Качество оформления (общий уровень грамотности, стиль изложения, качество иллюстраций, соответствие требованиям стандартов). 8. Объем и качество выполнения графического материала, его соответствие тексту. 9. Обоснованность и доказательность выводов работы. 10. Оригинальность и новизна полученных результатов, научно-исследовательских, технических или методических решений.	
ПК-1 Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности.	В ходе защиты выпускной квалификационной работы студент должен: • ***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-	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		

исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований.	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-3 Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	В ходе защиты выпускной квалификационной работы студент 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 ходе защиты выпускной квалификационной работы студент 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 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.		

4.1. Примерная тематика выпускных квалификационных работ по специальности 10.05.01 «Компьютерная безопасность» (специализация «Математические методы защиты информации»).

1. Исследование асимптотической сложности проблемы «Скрытой информации».
2. Оптимизация алгоритма Коча с использованием искусственной нейронной сети и выбор наиболее подходящего блока для встраивания цифрового водяного знака.
3. Построение комплексной системы информационной безопасности в учреждении здравоохранения.
4. Построение кодов, ассоциированных с торическими поверхностями.
5. Исследование условий применимости атаки Винера на криптосистему Ривеста – Шамира – Адлемана.
6. Реализация метода вычисления числа рациональных точек на кривых Артина – Шрайера над конечными полями.
7. Разработка комплекса лабораторных работ по применению средств защиты информации от несанкционированного доступа.
8. Организация централизованной аутентификации пользователей для распределённых систем.
9. Анализ, оптимизация и распараллеливание алгоритма декодирования Фенга – Рао на алгебраических кривых.
10. Анализ математических оснований криптосистемы с открытым ключом, основанной на группе Судзуки.
11. Разработка системы защищенного обмена для мобильных телефонов с использованием отечественной криптографии.
12. Разработка программной системы обнаружения вторжений с возможностью анализа трафика службы доменных имен.
13. Построение политики информационной безопасности для критически важного объекта на основе формальной модели управления доступом и информационными потоками.
14. Анализ безопасности цифровых подписей Ксинмея и Алабади – Викера.
15. Сравнительный анализ процедур декодирования на эрмитовой кривой и квартике Клейна.
16. Реализация алгоритма слепой подписи на базе стандарта цифровой подписи
17. Разработка, анализ стойкости и реализация основных алгоритмов шифрования СМС-сообщений на основе решёток в мобильной системе Windows Phone 8.
18. Обеспечение устойчивости цифровых водяных знаков, используемых для защиты авторских прав.
19. Обнаружение стеговложений в графических файлах.
20. Реализация алгоритма короткой цифровой подписи на основе спариваний Вейля.
21. Реализация криптосистемы с открытым ключом на основе идентификационных данных.

22. Сравнительный анализ стеганографических методов сокрытия информации в графических файлах.
23. Анализ эффективности алгоритма сложения в якобиане кривой Пикара и его реализация для криптографии.
24. Вычисление группы автоморфизмов некоторых кодов, ассоциированных с квартикой Клейна.
25. Реализация и анализ безопасности некоторых пороговых цифровых подписей.
26. Классификация экстремальных кодов с использованием их групп автоморфизмов.
27. Сравнительный анализ параметров однолинейных и двухлинейных кодов, ассоциированных с антиканоническими поверхностями.
28. Анализ безопасности схемы компактных электронных денег.
29. Вычисление дзета-функции башни Гарсии – Штихтенота.
30. Вычисление производящей функции графа, связанного с кривой Ван дер Хеера – Ван дер Флухта.
31. Особенности межсетевого экранирования и реализация персонального межсетевого экрана для протокола IPv6.
32. Защита от атак на протоколы шифрования беспроводных сетей.
33. Разработка схемы распределения ключей для облачных систем, допускающих перешифрование.
34. Анализ и реализация расширенного протокола Джоукса для многосторонней сверки ключей.
35. Анализ и реализация алгоритмов кодирования и декодирования NXL и XNL-кодов на основе алгоритма Судана.
36. Исследование свойств алгеброгеометрических кодов, ассоциированных с кривой Пикара
37. Исследование свойств первых ступеней башни функциональных полей Гарсии – Штихтенота и свойств соответствующих алгеброгеометрических кодов.
38. Моделирование угроз информационной безопасности критически важного объекта с использованием национального Банка угроз и уязвимостей.
39. Разработка и реализация политики безопасности для защиты виртуальной инфраструктуры
40. Разработка и исследование свойств протоколов почтового обмена внутри гибридного облака с двумя перешифрованиями на основе спаривания Хесса.
41. Приложение кодов Гоппы к криптосистемам Мак-Элиса и Нидеррайтера.
42. Разработка и анализ вычислительной эффективности основных криптографических алгоритмов на суперэллиптических кривых.
43. Разработка семейства протоколов на эллиптических кривых для децентрализованных приложений в индустрии азартных игр.
44. Анализ структуры и стойкости криптосистемы «Три медведя».
45. Анализ состояния защищенности информационной системы с помощью средств тестирования на проникновение.
46. Разработка и реализация специализированного комплекса для сбора и классификации информации на основе открытых источников (OSINT).
47. Исследование структуры якобиана гиперэллиптической кривой рода 3.
48. Оптимизация вычислений в группе точек эллиптической кривой.
49. Реализация и анализ BLS-схемы на эллиптических кривых.

50. Сведение дискретного логарифма на гиперэллиптических кривых рода 2 к конечному полю с помощью билинейных спариваний.
51. Гомоморфное выполнение нейронных сетей.
52. Построение модели защиты персональных данных пользователей в социальных сетях.
53. Анализ производительности типовых операций над точками эллиптической кривой при использовании различных систем координат.

4.2. Примеры формулировки тем и содержания выпускных квалификационных работ

Тема: ***Анализ стойкости криптосистемы «Три медведя»***

Содержание:

Введение
1. Предварительные сведения
1.1. Понятие решетки
1.2. Кратчайший вектор решетки
1.3. Фундаментальный параллелепипед .
1.4. Ортогонализация Грама-Шмидта
1.5. Задачи на решетках
1.6. Редукция решеток
2. Концепция обучения с ошибками
2.1. Определение задачи LWE
2.2. Определение задачи RLWE
2.3. Определение задачи I-RLWE
2.4. Сводимость задачи I-RLWE к задаче RLWE и наоборот
3. Описание криптосистемы «Три медведя»
3.1. Выбор параметров криптосистемы
3.2. Распределение ошибок криптосистемы
3.3. Режимы работы криптосистемы
3.4. Корректировка шумового параметра
3.5. Ключевой обмен, использующий I-RLWE
3.6. Процесс передачи сообщения
4. Решение задачи I-RLWE
4.1. Число целочисленных векторов в сфере заданного радиуса
4.2. Задача о рюкзаке
4.3. Решение задачи I-RLWE с помощью решетки
4.4. Время нахождения короткого вектора в решетке
Заключение
Список литературы
Приложение 1
Приложение 2 .

Литература:

1. P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science : Conference Publications, 1997. – 25 с.
2. M. Roetteler, M. Naehrig, K.M. Svore, K. Lauter. Quantum resource esti-mates for computing elliptic curve discrete logarithms. In: Takagi, T., Peyrin, T. (eds.), Asiacrypt 2017 (2), Springer LNCS 10625, 2017. – С. 241–270.
3. V. Lyubashevsky, C. Peikert, O. Regev. On ideal lattices and learning with er-rors over rings. In Advances in Cryptology – Eurocrypt 2010, 2010. – 23 с.
4. Gu Chunsheng. Integer version of ring-LWE and its applications. Cryptology ePrint Archive, Report 2017/641, 2017. – 15 с.
5. M. Hamburg. Module-LWE key exchange and encryption: The three bears. Technical report, National Institute of Standards and Technology, 2017.− 28 с.
6. M.R. Albrecht, et al. Estimate all the {{LWE, NTRU}} schemes! IACR Cryptology ePrint Archive, 2018. − 54 с.
7. M.J. Coster, A. Joux, B.A. La Macchia, A.M. Odlyzko, C.P. Schnorr and J. Stern, An improved lowdensity subset sum algorithm, Computational Complexity 2, 1992. – С. 111-128.
8. M.R. Albrecht, F. Gopfert, F. Virdia, T. Wunderer. Revisiting the expected cost of solving uSVP and applications to LWE. Cryptology ePrint Archive, Report 2017/815, 2017. – 28 с.
9. S. Khot. Hardness of approximating the shortest vector problem in lattices. In Proceedings of the 45th IEEE Symposium on Foundations of Computer Science, 2004.– 20 с.
10. O. Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In Proc. of STOC ’05, 2005. – С. 84–93.
11. O. Regev . The learning with errors problem. Invited survey in CCC 2010, 2010. − 23 с.
12. Blum, A. Kalai, H. Wasserman. Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model. Journal of the ACM 50(4), 2003. – 13 с.
13. M. Alekhnovich. More on average case vs approximation complexity. In Proc. 44th Annual IEEE Symp. on Foundations of Computer Science (FOCS), 2003.− С. 298-307. 46
14. V. Singh, A Practical Key Exchange for the Internet using Lattice Cryptography, 2015. − С. 21-22.
15. C. Peikert. How (not) to instantiate ring-LWE. Cryptology ePrint Archive, Report 2016/351 2016. – 29 с.
16. C. Peikert, A Decade of Lattice Cryptography. Cryptology ePrint Archive, Report 2015/939, 2016. – 90 с.
17. D. Dadush, O. Regev, N. Stephens-Davidowitz, "On the Closest Vector Problem with a distance guarantee", IEEE 29th Conference on Computational Com-plexity, 2014. – С. 98-109.
18. О.В. Кузьмин, В.С. Усатюк. Программный комплекс приведения базиса целочисленных решеток// Программные продукты и системы, №4(100), 2012. – С. 180-183.
19. Becker, L. Ducas, N. Gama, T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In SODA ’16 Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete Algorithms, SIAM, 2016. – 15 с.

Тема: ***Разработка и исследование свойств протоколов почтового обмена внутри гибридного облака с двумя перешифрованиями на основе спаривания Хесса*»**

Содержание:

Введение

1. Обзор предварительных результатов

1.1. Краткие сведения по эллиптическим кривым над конечными полями

1.2. Обзор спариваний на эллиптических кривых

1.3. Алгоритм Миллера

1.4. Обзор систем защиты облачных вычислений

2. Основные теоретические результаты

2.1. Протокол

2.2. Схема цифровой подписи и аутентификации пользователей

2.3. Обзор и анализ различных спариваний на эллиптических кривых

2.4. Общий алгоритм спаривания Хесса

2.5. Общие оценки вычислительной эффективности алгоритмов Хесса и перешифрования

2.6. Оценка криптостойкости протокола

3. Алгоритмы

3.1. Детализированный алгоритм вычисления спаривания Хесса на эллиптических кривых

4. Описание программного комплекса

4.1. Выбор языка программирования

4.2. Описание программного комплекса

5. Примеры

5.1 Пример 1

5.2. Пример 2

5.3. Пример 3

Заключение

Список литературы

Приложение

Тексты компьютерных программ

Литература:

1. Miller V.S.. The Weil pairing, and its efficient calculation. Journal of Cryptology, 17:235–261, 2004.
2. Hess F. Pairing lattices. In S. D. Galbraith and K. Paterson, editors, Pairing-Based Cryptography – Pairing 2008, volume 5209 of Lecture Notes in Computer Science, pages 18–38, Berlin, 2008. Springer-Verlag.
3. Washington L.C. Elliptic curves: number theory and cryptography. – Chapman & Hall/CRL, 2008.
4. Boneh D., Franklin M. Identity-Based Encryption from the Weil Pairing. SIAM J. of Computing, Vol. 32, № 3, pp. 586-615, 2003.
5. Enge A. Bilinear pairings on elliptic curves. 2013. HAL Id: hal-00767404.
6. Батура Т.В., Мурзин Ф.А., Семич Д.Ф. Облачные технологии: основные понятия, задачи и тенденции развития. — Программные продукты и системы и алгоритмы, №1, 2014.
7. Безкоровайный Д. Комплексная защита данных в публичных облаках. — Storage News №1, pp. 16-19, 2013.

8. Wu X., Xu L., Zhang X. A Certificateless Proxy Re-Encryption Scheme for Cloud-based Data Sharing. 2011.
9. Алешников С.И., Алешникова М.В., Горбачёв А.А. Протокол доверенного шифрования на основе модифицированного алгоритма вычисления спаривания Вейля на алгебраических кривых для облачных вычислений. — Информационные технологии. – 2013. - №9. - С.36-39.
10. Menezes A. J., Oorschot P. v., Vanstone S. A. 11.5.2 The ElGamal signature scheme. — Handbook of Applied Cryptography — CRC Press, 1996.
11. FIPS PUB 186-4. — Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD, 2013.
12. Koblitz N., Menezes A. Another Look at Generic Groups. — 1995.
13. ГОСТ Р 34.10-2012. Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — ФГУП Стандартинформ, 2013.
14. Barreto P.S.L.M., Galbraith S.D., .O'h.Eigeartaigh C., Scott M. Efficient pairing computation on supersingular abelian varieties. Designs, Codes and Cryptography, 42:239–271, 2007.
15. Hess F., Smart N.P., Vercauteren F.. The eta pairing revisited. IEEE Transactions on Information Theory, 52(10):4595–4602, 2006.
16. Zhao C., Zhang F., Huang J.. A note on the Ate pairing. International Journal of Information Security, 7(6):379–382, 2008.
17. Lee E., Lee H., Park C.. Efficient and generalized pairing computation on abelian varieties. IEEE Transactions on Information Theory, 55(4):1793–1803, 2009.
18. Vercauteren F.. Optimal pairings. IEEE Transactions on Information Theory, 56(1):455–461, 2010.
19. Страуструп Б. Язык программирования C++. Специальное издание — М.: Бином-Пресс, 2007. — 1104 с. — ISBN 5-7989-0223-4.
20. User's Guide to the PARI library. — The PARI Group, 2016.
21. Tilborg H.v.C.A., Jajodia S. Encyclopedia of Cryptography and Security. — Springer, 2011. – 1416 с. — ISBN 978-1-4419-5905-8.
22. Gashkov S.B., Sergeev I.S.. Complexity of computation in Finite Fields. — Journal of Mathematical Sciences, Vol. 191, No. 5, 2013.

ПРИЛОЖЕНИЯ

Приложение 1

Оценочный лист сформированности компетенций для руководителя ВКР и членов ГЭК

Коды проверяемых компетенций	Элементы оценивания		
	Презентация	Доклад	Ответы на вопросы членов ГЭК
ОК-5	+	+	+
ОК-7	+	+	+
ОК-8	+	+	+
ПК-1	+	+	+
ПК-2	+	+	+
ПК-3	+	+	+
ПК-4	+	+	+

Приложение 2

Оценочный лист членов ГЭК

Оценка уровня сформированности компетенций студента _____ специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» в процессе защиты выпускной квалификационной работы, выполненной на тему

_____

_____

Коды проверяемых компетенций	Показатели оценки результата	Показатели уровня сформированности компетенций			
		2 – низкий	3 – средний	4 – достаточный	5 – высокий
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.				
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.				
ОК-8	Способность к самоорганизации и самообразованию.				
ПК-1	Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности.				
ПК-2	Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей и математической статистики, теории информации, теоретико-числовых методов				
ПК-3	Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности				
ПК-4	Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.				