

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное учреждение  
высшего профессионального образования  
"Казанский (Приволжский) федеральный университет"  
Институт вычислительной математики и информационных технологий



**Программа дисциплины**  
Научно-исследовательская работа Б2.Н.1

Направление подготовки: 02.04.02 - Фундаментальная информатика и информационные технологии

Профиль подготовки: Математические основы и программное обеспечение информационной безопасности и защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

**Автор(ы):**

Хабибуллин Р.Ф. , Андрианова А.А.

**Рецензент(ы):**

Латыпов Р.Х.

**СОГЛАСОВАНО:**

Заведующий(ая) кафедрой: Латыпов Р. Х.

Протокол заседания кафедры № \_\_\_\_ от "\_\_\_\_" 201\_\_ г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:

Протокол заседания УМК № \_\_\_\_ от "\_\_\_\_" 201\_\_ г

Регистрационный № 938214

Казань  
2014

## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) доцент, к.н. Андрианова А.А. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Anastasiya.Andrianova@kpfu.ru ; доцент, к.н. (доцент) Хабибуллин Р.Ф. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Rustem.Khabibullin@kpfu.ru

## 1. Цели освоения дисциплины

Целью является проведение научно-исследовательской работы по теме последующей магистерской диссертации. Тема магистерской диссертации должна иметь научный, исследовательский характер и должна быть связана с разработкой и исследованием методик, алгоритмов обработки информации для различных научных и прикладных задач.

Научно-исследовательская работа включает в себя обязательную разработку программного продукта за исключением случаев, когда тема работы предполагает серьезные научные исследования, проведение математических доказательств, предложение и обоснование новых методик применения средств защиты информации. Также курсовая работа включает оформление пояснительной записки, в которой подробно изложены цели и задачи работы, объект исследования, а также ход выполнения работы и подробное описание полученного результата.

## 2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б2.Н.1 Практика и научно-исследовательская работа" основной образовательной программы 02.04.02 Фундаментальная информатика и информационные технологии и относится к . Осваивается на 1, 2 курсах, 1, 2, 3 семестры.

Дисциплина "Научно-исследовательская работа" относится к научно-исследовательской работе магистра, раздел Б2.Н1. Данная дисциплина основывается на результатах изучения предшествующих дисциплин учебного плана.

## 3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	способностью к абстрактному мышлению, анализу, синтезу
ОК-2 (общекультурные компетенции)	готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения
ОК-3 (общекультурные компетенции)	готовностью к саморазвитию, самореализации, использованию творческого потенциала
ОПК-1 (профессиональные компетенции)	готовностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач профессиональной деятельности
ОПК-2 (профессиональные компетенции)	готовностью руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-3 (профессиональные компетенции)	способностью использовать и применять углубленные теоретические и практические знания в области фундаментальной информатики и информационных технологий
ОПК-4 (профессиональные компетенции)	способностью самостоятельно приобретать и использовать в практической деятельности новые знания и умения, в том числе, в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять своё научное мировоззрение
ОПК-5 (профессиональные компетенции)	способностью использовать углублённые знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов
ПК-1 (профессиональные компетенции)	способностью проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива
ПК-10 (профессиональные компетенции)	способностью к преподаванию математических дисциплин и информатики в образовательных организациях основного общего, среднего общего, среднего профессионального и высшего образования
ПК-11 (профессиональные компетенции)	способностью разрабатывать учебно-методические материалы по тематике информационных технологий для образовательных организаций среднего профессионального и высшего образования, проводить семинарские и практические занятия с обучающимися, а также лекционные занятия спецкурсов
ПК-12 (профессиональные компетенции)	способностью разрабатывать учебно-методические комплексы для электронного и мобильного обучения
ПК-13 (профессиональные компетенции)	способностью разрабатывать аналитические обзоры состояния области прикладной математики и информационных технологий
ПК-14 (профессиональные компетенции)	способностью выполнять работу экспертов в ведомственных, отраслевых или государственных экспертных группах по экспертизе проектов, тематика которых соответствует направленности (профилю) программы магистратуры
ПК-15 (профессиональные компетенции)	способностью работать в международных проектах по разработке открытых спецификаций новых информационных технологий, реализуемых международными профессиональными организациями и консорциумами на основе принципа консенсуса
ПК-16 (профессиональные компетенции)	способностью участвовать в деятельности профессиональных сетевых сообществ по конкретным направлениям
ПК-17 (профессиональные компетенции)	способностью осознавать корпоративную политику в области повышения социальной ответственности бизнеса перед обществом, принимать участие в ее развитии

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-2 (профессиональные компетенции)	способностью использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий
ПК-3 (профессиональные компетенции)	способностью разрабатывать концептуальные и теоретические модели решаемых научных проблем и задач проектной и производственно-технологической деятельности
ПК-4 (профессиональные компетенции)	способностью разрабатывать архитектурные и функциональные спецификации создаваемых систем и средств, а также разрабатывать абстрактные методы их тестирования
ПК-5 (профессиональные компетенции)	способностью управлять проектами, планировать научно-исследовательскую деятельность, анализировать риски, управлять командой проекта
ПК-6 (профессиональные компетенции)	способностью к углубленному анализу проблем, постановке и обоснованию задач научной и проектно-технологической деятельности
ПК-7 (профессиональные компетенции)	способностью разрабатывать и оптимизировать бизнес-планы научно-прикладных проектов
ПК-8 (профессиональные компетенции)	способностью организовывать процессы корпоративного обучения на основе электронных и мобильных технологий и развивать корпоративные базы знаний
ПК-9 (профессиональные компетенции)	способностью осознавать и разрабатывать корпоративные стандарты и политику развития корпоративной инфраструктуры информационных технологий на принципах открытых систем

В результате освоения дисциплины студент:

1. должен знать:

- правила оформления квалификационных работ
- правила работы с научно-технической литературой
- правила работы с сетями, компьютерными технологиями и мультимедийными технологиями

2. должен уметь:

- готовить презентации научных работ с использованием средств мультимедиа
- собирать материал необходимый для научно-исследовательской работы
- анализировать собранный материал и перерабатывать его
- работать с необходимыми пакетами прикладных программ

3. должен владеть:

- навыками написания научно-исследовательских работ
- навыками написания компьютерных программ на современных языках программирования
- навыками сбора и анализа информации с помощью сетевых технологий

4. должен демонстрировать способность и готовность:

- проводить научные исследования
- решать новые и мало изученные задачи

#### 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет зачетных(ые) единиц(ы) 756 часа(ов).

Форма промежуточного контроля дисциплины отсутствует в 1 семестре; отсутствует во 2 семестре; зачет в 3 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

#### 4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

##### Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Выбор темы научно-исследовательской работы и проведение начальных исследований	1	1-18	0	18	0	отчет научный доклад
2.	Тема 2. Определение основных направлений исследований, получение первых промежуточных результатов	2	1-18	0	18	0	отчет презентация научный доклад творческое задание
3.	Тема 3. Систематизация наработанного материала, формулировка конечной темы магистерской диссертации	3	1-18	0	18	0	отчет творческое задание презентация научный доклад
.	Тема . Итоговая форма контроля	3		0	0	0	зачет
	Итого			0	54	0	

#### 4.2 Содержание дисциплины

##### Тема 1. Выбор темы научно-исследовательской работы и проведение начальных исследований

**практическое занятие (18 часа(ов)):**

Ознакомление студентов с регламентом проведения и оценки научно-исследовательской работы, выбор тем магистерских диссертаций и научных руководителей, рекомендации по организации самостоятельной работы по диссертации и представлению ее промежуточных результатов, первый научный доклад по теме диссертации каждого из магистрантов с обоснованием актуальности исследований и постановкой основных целей и задач исследований.

**Тема 2. Определение основных направлений исследований, получение первых промежуточных результатов**

**практическое занятие (18 часа(ов)):**

Работа с научным руководителем, подбор современной литературы по теме исследований, составление обзора текущих достижений в области исследований, научный доклад и презентация первых результатов проведенных магистрантами исследований.

**Тема 3. Систематизация наработанного материала, формулировка конечной темы магистерской диссертации**

**практическое занятие (18 часа(ов)):**

Работа с научным руководителем, систематизация собранного материала, его анализ и определение основных выводов, окончательная формулировка темы магистерской диссертации, научный доклад с определением основных результатов, которые получены или будут получены при оформлении диссертации.

**4.3 Структура и содержание самостоятельной работы дисциплины (модуля)**

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Выбор темы научно-исследовательской работы и проведение начальных исследований	1	1-18	подготовка к научному докладу, дискуссии	200	научный доклад
				подготовка к отчету	34	отчет
2.	Тема 2. Определение основных направлений исследований, получение первых промежуточных результатов	2	1-18	выбор темы, изучение литературы по выбранной теме	60	научный доклад
				подготовка к отчету	20	отчет
				подготовка к презентации	20	презентация
				подготовка к реферату	34	реферат
				подготовка к творческому экзамену	100	творческое задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
3.	Тема 3. Систематизация наработанного материала, формулировка конечной темы магистерской диссертации	3	1-18	подготовка к научному докладу	100	научный доклад
				подготовка к отчету	14	отчет
				подготовка к презентации	20	презентация
				подготовка к творческому заданию	100	творческое задание
	Итого				702	

## 5. Образовательные технологии, включая интерактивные формы обучения

Занятия по данной дисциплине организуются в основном в виде самостоятельной работы студентов.

Самостоятельная работа заключается в выборе темы для научного исследования, сбора материала необходимого для выполнения работы, анализа и работы над материалом, выполнения проекта или доказательства некоторых утверждений, создание программного продукта, проверка программного продукта на тестовых задачах, оформления работы в установленном виде.

Аудиторные занятия заключаются во встречах с научным руководителем и обсуждением деталей работы, направлений, в которых лучше двигаться, методов, с помощью которых лучше решать ту или иную задачу, цели, к которой необходимо двигаться, анализе необходимых пакетов прикладных программ.

## 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

### Тема 1. Выбор темы научно-исследовательской работы и проведение начальных исследований

научный доклад , примерные вопросы:

Обсуждение с научным руководителем выбранной темы, разбор возможных направлений разработок. Представление темы дальнейших исследований на семинаре

отчет , примерные вопросы:

Оформление отчета в конце семестра с указанием основного направления исследования, основных целей и задач исследований и их актуальности.

### Тема 2. Определение основных направлений исследований, получение первых промежуточных результатов

научный доклад , примерные вопросы:

Подготовка научных докладов для представления на семинарах

отчет , примерные вопросы:

Оформление отчета в конце семестра с указанием основных полученных результатов по теме исследований.

презентация , примерные вопросы:

Подготовка презентации промежуточных полученных результатов в рамках семинара

реферат , примерные темы:

Оформление промежуточных результатов исследований и защита в рамках курсовой работы.

творческое задание , примерные вопросы:

Выполнение магистерской диссертации: формулировка темы, изучение литературы, определение направлений развития, составление обзора текущего состояния темы, промежуточные результаты.

### **Тема 3. Систематизация наработанного материала, формулировка конечной темы магистерской диссертации**

научный доклад , примерные вопросы:

Подготовка научных докладов для представления на семинарах

отчет , примерные вопросы:

Оформление отчета в конце семестра с указанием основных полученных результатов по теме исследований.

презентация , примерные вопросы:

одготовка презентации промежуточных полученных результатов в рамках семинара

творческое задание , примерные вопросы:

Выполнение магистерской диссертации: развитие результатов 2 семестра, анализ полученных результатов, предварительные выводы.

### **Тема . Итоговая форма контроля**

Примерные вопросы к зачету:

По завершению работы студентом над научно-исследовательской работой организуется защита работ, на которой студенты перед комиссией представляют презентацию научно-исследовательской работы, отчитываются о проделанной работе, излагают результаты численных экспериментов, отвечают на вопросы членов комиссии.

Типовые темы научных исследований и магистерских диссертаций.

1. Реализация и сравнительное исследование эффективности метода Монтгомери для процедуры факторизации на эллиптических кривых.
2. Реализации и сравнительное исследование алгоритмов "слепой подписи" на основе преобразований Вейля-Тейта.
3. Исследование эффективности MOV-атаки на суперсингулярные кривые с использованием преобразований Вейля-Тейта.
4. Реализация на компьютере и исследование эффективности метода факторизации на эллиптических кривых с использованием кривых Эдварда.
5. Исследование эффективности алгоритма Миллера-Рабина на наборах различных баз.
6. Тест простоты Гольдвассера и Килиана на эллиптических кривых.
7. Реализация и исследование теста простоты BPSW.
8. Разработка оценок сходимости различных алгоритмов на основе производящих функций и рядов Дирихле.
9. Сравнительное изучение различных методов реализации алгоритма Евклида вычисления НОД.
10. Анализ получения оценок средних параметров сходимости алгоритма Евклида на основе статьи Брента.
11. Задачи оптимального распределения ресурсов в сетях телекоммуникаций.
12. Игровые модели распределения ресурсов в сетях телекоммуникаций.
13. Модели распределения потоков в сетях телекоммуникаций и транспорта.
14. Модели устойчивого поддержания возобновляемых природных ресурсов
15. Решение задач оптимизации с векторным критерием.
16. Поиск решений антагонистических и бескоалиционных игр.
17. Итерационные методы для задач поиска точек равновесия.
18. 3D эффект, как результат слежения за лицом

19. Определение числа студентов в аудитории по фотографии
20. Синтез речевого сигнала
21. Очистка речевого сигнала от шума
22. Определение эмоций на основе анализа речевого сигнала

## **7.1. Основная литература:**

- 1.Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - . - Режим доступа:: <http://kpfu.ru/docs/F366166681/mzi.pdf>
2. Соловьев Е.Л. Генераторы случайных чисел в системах компьютерной безопасности[Электронный ресурс]. - Казань, 2014 - Режим доступа:: <http://shelly.kpfu.ru/e-ksu/docs/F833856100/FinalGen.pdf>. год
3. Информационная безопасность[Электронный ресурс]: Учебное пособие / Т.Л. Партика, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. . - Режим доступа: <http://www.znaniy.com/bookread.php?book=420047>
4. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. . - Режим доступа: <http://www.znaniy.com/bookread.php?book=405000>
5. Соловьев Е.Л. Электронный образовательный ресурс "Алгоритмические основы медиа технологий" [Электронный ресурс] 2013 - . - Режим доступа: <http://zilant.kpfu.ru/course/view.php?id=17362>
6. Соловьев Е.Л., Нигматуллин Р.Р. Электронный образовательный ресурс "Компьютерное зрение" [Электронный ресурс] 2014 - режим доступа: <http://zilant.kpfu.ru/course/view.php?id=17266>

## **7.2. Дополнительная литература:**

- 1.Иванов М.А. Защита информации в электронных платежных системах [Электронный ресурс] : электронный учебник / М. А. Иванов, Д. М. Михайлов, И. В. Чугунков . ? Электрон. дан. и прогр. (695 Мб) . ? Москва : Кнорус, 2011 . ? 1 электрон. опт. диск (CD-ROM)
- 2.Петровский, Владимир Ильич. Комплексная защита информации на предприятии : организационная защита информации : учебное пособие / В. И. Петровский, В. В. Петровский, В. И. Глова ; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Казан. нац. исслед. техн. ун-т им. А. Н. Туполева-КАИ" . ? Казань : [Изд-во Казанского государственного технического университета], 2012 . ? ; 20 . ? ISBN 978-5-7579-1656-9 ((в обл.)) , 100. Т. 1 . ? 2012 . ? 438 с
- 3.Петровский, Владимир Ильич. Комплексная защита информации на предприятии : организационная защита информации : учебное пособие / В. И. Петровский, В. В. Петровский, В. И. Глова ; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Казан. нац. исслед. техн. ун-т им. А. Н. Туполева-КАИ" . ? Казань : [Изд-во Казанского государственного технического университета], 2012 . ? ; 20 . ? ISBN 978-5-7579-1656-9 ((в обл.)) , 100. Т. 2 . ? 2012 . ? 509 с.
4. Информационные технологии в науке и образовании[Электронный ресурс]: Учебное пособие / Е.Л. Федотова, А.А. Федотов. - М.: ИД ФОРУМ: ИНФРА-М, 2011. - 336 с. . - Режим доступа: <http://www.znaniy.com/bookread.php?book=251095>
5. Прикладные информационные технологии[Электронный ресурс]: Учебное пособие / Е.Л. Федотова, Е.М. Портнов. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 336 с. . - Режим доступа: <http://www.znaniy.com/bookread.php?book=392462>
6. Информационные технологии: разработка информационных моделей и систем[Электронный ресурс]: Учеб. пос. / А.В.Затонский - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014 - 344 с. . - Режим доступа: <http://www.znaniy.com/bookread.php?book=400563>

### **7.3. Интернет-ресурсы:**

Интернет-портал образовательных ресурсов по ИТ - <http://www.intuit.ru>

Интернет-портал ресурсов по математическим наукам - <http://www.math.ru/>

Интернет-портал с ресурсами по математическим наукам - <http://www.mathnet.ru>

Интернет-портал со статьями по алгоритмике и программированию - <http://algolist.manual.ru/>

Электронная библиотека по техническим наукам - <http://techlibrary.ru>

### **8. Материально-техническое обеспечение дисциплины(модуля)**

Освоение дисциплины "Научно-исследовательская работа" предполагает использование следующего материально-технического обеспечения:

Компьютеры, доступ в интернет, мультимедийное оборудование

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 02.04.02 "Фундаментальная информатика и информационные технологии" и магистерской программе Математические основы и программное обеспечение информационной безопасности и защиты информации .

Автор(ы):

Хабибуллин Р.Ф. \_\_\_\_\_

Андрианова А.А. \_\_\_\_\_

"\_\_" 201 \_\_ г.

Рецензент(ы):

Латыпов Р.Х. \_\_\_\_\_

"\_\_" 201 \_\_ г.