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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____
"___"_____20___ г.

Программа дисциплины

Курсовая работа по направлению Б1.Б.40

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Андрианова А.А. , Ишмухаметов Ш.Т.

Рецензент(ы):
Тагиров Р.Р.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань
2017

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 ; профессор, д.н. (доцент) Ишмухаметов Ш.Т. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Shamil.Ishmukhametov@kpfu.ru

1. Цели освоения дисциплины

Целью является написание курсовой работы по направлению подготовки "Информационная безопасность". Тема курсовой работы может иметь как научный (разработка и исследования основных и вспомогательных алгоритмов криптографии, разработка средств и протоколов защищенной передачи информации по сети, разработка средств сокрытия информации и т.д.), так и прикладной (разработку информационных систем с подсистемами защиты информации). Курсовая работа включает в себя обязательную разработку программного продукта за исключением случаев, когда тема предполагает серьезные научные исследование, 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 " Б1.Б.40 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к базовой (общепрофессиональной) части. Осваивается на курсах, семестры.

Дисциплина "Курсовая работа" относится к профессиональному циклу. Данная дисциплина основывается на результатах изучения предшествующих дисциплин учебного плана и имеет целью агрегацию полученных знаний и самостоятельное выполнение комплексной законченной работы в рамках направления "Информационная безопасность".

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-1 (профессиональные компетенции)	способность анализировать физические явления и процессы для решения профессиональных задач
ОПК-2 (профессиональные компетенции)	способность применять соответствующий математический аппарат для решения профессиональных задач
ОПК-3 (профессиональные компетенции)	способность применять положения в области электротехники, электроники и схемотехники для решения профессиональных задач
ОПК-4 (профессиональные компетенции)	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
ОПК-5 (профессиональные компетенции)	способность использовать нормативные правовые акты в профессиональной деятельности

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-6 (профессиональные компетенции)	способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности
ОПК-7 (профессиональные компетенции)	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

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 курсовой 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:

- грамотно и профессиональным языков излагать результаты своей работы;
- самостоятельно разрабатывать сложные программные приложения.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины .

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. Работа с научным руководителем: обсуждение темы курсовой работы, цели исследования, способов и методов с помощью которых можно ее достичь, анализ необходимых пакетов прикладных программ, наличие необходимого мультимедийного и сетевого оборудования, конкретная детализация этапов работы.	5		0	0	0	Творческое задание
2.	Тема 2. Сбор материала необходимого для курсовой работы, анализ и работа над материалом, работа над проектом или доказательство теоретических положений, в зависимости от тематики курсовой работы, создание программного продукта, проверка программного продукта на тестовых задачах, исправление замечаний, высказанных научным руководителем, оформление работы в соответствии с установленными требованиями, подготовка презентации для выступления перед комиссией.	6		0	0	0	Творческое задание
.	Тема . Итоговая форма контроля	6		0	0	0	Зачет
	Итого			0	0	0	

4.2 Содержание дисциплины

Аудиторная нагрузка по учебному плану не предусмотрена

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. Работа с научным руководителем: обсуждение темы курсовой работы, цели исследования, способов и методов с помощью которых можно ее достичь, анализ необходимых пакетов прикладных программ, наличие необходимого мультимедийного и сетевого оборудования, конкретная детализация этапов работы.	5		подготовка к творческому экзамену	13	творческое задание
2.	Тема 2. Сбор материала необходимого для курсовой работы, анализ и работа над материалом, работа над проектом или доказательство теоретических положений, в зависимости от тематики курсовой работы, создание программного продукта, проверка программного продукта на тестовых задачах, исправление замечаний, высказанных научным руководителем, оформление работы в соответствии с установленными требованиями, подготовка презентации для выступления перед комиссией.	6		подготовка к творческому заданию	49	творческое задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
	Итого				62	

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 (контроль самостоятельной работы) 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. Работа с научным руководителем: обсуждение темы курсовой работы, цели исследования, способов и методов с помощью которых можно ее достичь, анализ необходимых пакетов прикладных программ, наличие необходимого мультимедийного и сетевого оборудования, конкретная детализация этапов работы.

творческое задание , примерные вопросы:

Обсуждение темы курсовой работы, цели исследования, способов и методов с помощью которых можно ее достичь, анализ необходимых пакетов прикладных программ, наличие необходимого мультимедийного и сетевого оборудования, конкретная детализация этапов работы.

Тема 2. Сбор материала необходимого для курсовой работы, анализ и работа над материалом, работа над проектом или доказательство теоретических положений, в зависимости от тематики курсовой работы, создание программного продукта, проверка программного продукта на тестовых задачах, исправление замечаний, высказанных научным руководителем, оформление работы в соответствии с установленными требованиями, подготовка презентации для выступления перед комиссией.

творческое задание , примерные вопросы:

Демонстрация этапов выполнения курсовой работы. демонстрация готового проекта, анализ пояснительной записки к курсовой работе, тестирование готового программного продукта на соответствие поставленным целям и задачам.

Тема . Итоговая форма контроля

Примерные вопросы к :

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

Примерные темы курсовых работ.

1. Реализация на компьютере и исследование эффективности процедуры факторизации натуральных чисел (разложения на простые множители) ро-методом Полларда. Разложение специальных чисел вида .

2. Реализация на компьютере и исследование эффективности факторизации натуральных чисел (p-1) - методом Полларда. Разложение чисел вида .

3. Программирование системы шифрования на эллиптических кривых.

4. Реализация на компьютере генерации простых чисел на основе метода Миллера-Рабина. Построение простых чисел, удовлетворяющих требованиям RSA.

5. Реализация на компьютере и исследование эффективности арифметических операций на эллиптических кривых.

6. Реализация на компьютере и исследование эффективности факторизации натуральных чисел методом Шенкса непрерывных дробей и сравнение с ро-методом Полларда.

7. Реализация на компьютере метода факторизации на эллиптических кривых. Исследование его эффективности. Разложение чисел специального вида.

8. Сравнительное изучение и реализация на компьютере алгоритма вычисления дискретного логарифма в конечных полях.

9. Программирование процедуры факторизации на основе метода квадратичных форм.

10. Реализация на компьютере алгоритма Шенкса-Тоннелли извлечения квадратного корня в конечных полях.

11. Изучение и реализация на компьютере метода вычисления составных псевдопростых чисел для различных баз.

Примечание: Данная тема представляет собой открытую научную проблему.

12. Реализация и исследование теста простоты BPSW.

13. Изучение преобразования Тейта и его использования в криптографии.

14. Разработка автоматизированной системы оценки реккурентных алгоритмов на основе производящих функций.

15. Реализация и изучение бинарного алгоритма Евклида. Сравнение с классическим алгоритмом Евклида.

16. Реализация и изучение k-арного алгоритма Евклида. Сравнение с классическим алгоритмом Евклида.

17. Изучение числовых рядов Дирихле и использование для оценки алгоритмов.

18. Исследование эффективности реализации операции модульной арифметики на многоядерных видеопроцессорах (система программирования CUDA).

19. Реализация метода Ленстры процедуры факторизации на эллиптических кривых с использованием кривых Монтгомери.

20. Реализация и исследования преобразований Вейля. MOV-атака на системы шифрования на эллиптических кривых.

21. Реализация на компьютере метода факторизации на эллиптических кривых с использованием кривых Эдварда.

22. Реализация алгоритма построения слепой и короткой подписи на основе пре-образования Тейта.

23. Реализация на компьютере метода факторизации на эллиптических кривых с использованием кривых Эдварда. Сравнение эффективности метода с простой процедурой факторизации.

7.1. Основная литература:

1. Расторгуев, С. П. Основы информационной безопасности: учебное пособие / С.П. Расторгуев.?Москва: Академия, 2007.?186 с.

2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: http://znanium.com/bookread.php?book=335362

3. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. URL: http://znanium.com/bookread.php?book=402686

4. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. URL: http://znanium.com/bookread.php?book=405000

7.2. Дополнительная литература:

1. Партыка, Т. Л. Информационная безопасность: учеб. пособие / Т.Л. Партыка, И.И. Попов.?Изд. 2-е, испр. и доп..?Москва: ФОРУМ: ИНФРА-М, 2007.?367 с

2. Бабаш, А. В. Информационная безопасность: лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников.?Москва: КноРус, 2012.?131 с

7.3. Интернет-ресурсы:

Википедия - http://ru.wikipedia.org

Интернет-портал образовательных ресурсов КФУ - http://tulpar.kfu-elearning.ru

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

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

положение по курсовым работам - http://ksu.ru/umu/index.php?id=3&idm=7&num=2

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Курсовая работа по направлению" предполагает использование следующего материально-технического обеспечения:

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Компьютеры, доступ в интернет, мультимедийное оборудование

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность компьютерных систем .

Автор(ы):
Андрианова А.А. _____
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

Рецензент(ы):
Тагиров Р.Р. _____
"__" _____ 201 __ г.