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

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

*подписано электронно-цифровой подписью*

# Программа дисциплины

Математические методы в криптографии

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Математические методы и программные технологии защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

**Содержание**

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Салимов Ф.И. (кафедра теоретической кибернетики, отделение фундаментальной информатики и информационных технологий), Farid.Salimov@kpfu.ru

**1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО**

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

| Шифр компетенции | Расшифровка приобретаемой компетенции |
|---|---|
| ОК-1 | способность к абстрактному мышлению, анализу, синтезу |
| ОПК-1 | способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности |
| ПК-1 | способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты |
| ПК-2 | способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности |
| ПК-3 | способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов |
| ПК-5 | способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества |

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- базовые принципы построения криптографических систем с симметричным и асимметричным ключом,
- принципы построения шифров и криптографических протоколов;
- математические методы расчета надежности криптографических систем;
- методы построения математических моделей защищаемой информации, шифров, криптографических систем и криптографических протоколов;
- методы решения конкретных алгебраических, теоретико-числовых и алгоритмических задач криптографического анализа и синтеза

криптографических систем и криптографических протоколов;

Должен уметь:

- использовать ЭВМ в решении криптографических задач;
- использовать методы дискретной математики при решении практических задач криптографии;
- использовать типовые методы криптографического анализа;
- практически решать задачи защиты программ и данных.

Должен владеть:

- математическими знаниями построения криптографических систем;
- применять системный подход к обеспечению информационной безопасности телекоммуникационных систем;

Должен демонстрировать способность и готовность:

- практического применения криптографических методов в современных приложениях
- практического освоения криптографических технологий на реальных задачах обеспечения конфиденциальности и аутентификации.

**2. Место дисциплины (модуля) в структуре ОПОП ВО**

Данная дисциплина (модуль) включена в раздел "Б1.В.ОД.12 Дисциплины (модули)" основной профессиональной образовательной программы 10.04.01 "Информационная безопасность (Математические методы и программные технологии защиты информации)" и относится к обязательным дисциплинам.
Осваивается на 1 курсе в 1 семестре.

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

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

Контактная работа - 36 часа(ов), в том числе лекции - 18 часа(ов), практические занятия - 18 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 36 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 1 семестре.

**4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)**

| N | Разделы дисциплины / модуля | Семестр | Виды и часы контактной работы, их трудоемкость (в часах) | | | Самостоятельная работа |
|---|---|---|---|---|---|---|
| | | | Лекции | Практические занятия | Лабораторные работы | |
| 1. | Тема 1. Значение криптографии в информационном обществе | 1 | 2 | 0 | 0 | |
| 2. | Тема 2. Теория делимости, сравнения | 1 | 2 | 4 | 0 | 8 |
| 3. | Тема 3. Криптосистемы на основе модулярной арифметики | 1 | 4 | 2 | 0 | 6 |
| 4. | Тема 4. Элементы высшей алгебры | 1 | 4 | 6 | 0 | 10 |
| 5. | Тема 5. Элементы алгебраической геометрии | 1 | 4 | 2 | 0 | 8 |
| 6. | Тема 6. Методы криптоанализа. | 1 | 2 | 4 | 0 | 4 |
| | Итого | | 18 | 18 | 0 | 36 |

**4.2 Содержание дисциплины (модуля)**

**Тема 1. Значение криптографии в информационном обществе**

Предмет и содержание курса, взаимосвязь курса со смежными дисциплинами. Значение криптографии в информационном обществе. Проблематика криптографии. История возникновения криптографии. Основные определения. Задачи и современные приложения криптографии. Особенности применения криптографических методов в информационных системах. Классификация криптографических систем. Основные определения.

**Тема 2. Теория делимости, сравнения**

Нахождение НОД, НОК, коэффициентов Безу. Свойства сравнений.

Классы вычетов. Полная и приведенная системы вычетов.

Использование малой теоремы Ферма и Эйлера.

Китайская теорема об остатках. Сравнения любой степени по простому и составному модулю. .

Символ Лежандра и Якоби. Первообразные корни, индексы и характеры по модулю.

**Тема 3. Криптосистемы на основе модулярной арифметики**

Криптосистема RSA. Атаки на RSA. Система Рабина. Задача о рюкзаке. Признаки простоты и алгоритмы генерации простых чисел. Электронные цифровые подписи: Рабина, Диффи-Лампорта, DSS, Эль-Гамаля, Российского стандарта. Задача дискретного логарифмирования.

Хеш-функции

**Тема 4. Элементы высшей алгебры**

Группы и подгруппы. Гомоморфизмы групп. Группы подстановок.

Кольца и поля. Простые и максимальные идеалы. Поля Галуа.

Поля Галуа. Конечные расширения полей. Неприводимые многочлены и их порядки.

Линейные рекуррентные последовательности. Поточные криптосистемы.

**Тема 5. Элементы алгебраической геометрии**

Эллиптические кривые. Сложение точек эллиптической кривой.

Кривые над незамкнутым полем. Эллиптические кривые над конечными полями.

Порядок эллиптической кривой. Скалярное умножение на эллиптической кривой.

Генерация и проверка цифровой подписи на эллиптической кривой.

**Тема 6. Методы криптоанализа.**

Корреляционный криптоанализ поточной криптосистемы.

Криптоанализ на основе теории статистических решений.

Разностный криптоанализ.

## 5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

## 6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);

- критерии оценивания сформированности компетенций;

- механизм формирования оценки по дисциплине (модулю);

- описание порядка применения и процедуры оценивания для каждого оценочного средства;

- критерии оценивания для каждого оценочного средства;

- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

## 7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;

- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

**8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)**

Материалы онлайн-курсов Массачусетского Технологического Института - http://ocw.mit.edu/index.htm

Онлайн-курсы лучших университетов мира - https://www.udacity.com

Онлайн-курсы Стенфордского Университета - http://online.stanford.edu

**9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Самостоятельная работа студента по курсу 'Математические методы в криптографии' заключается в выполнении лабораторных и контрольных работ, подготовке и защите научного доклада. Курс заканчивается подготовкой к зачёту.

Темы и сроки сдачи лабораторных работы определяются преподавателем. Лабораторная робота заключается в построении псевдослучайной перестановки. В работе должна быть описана

перестановка, написана программа реализующий этот метод, приведены результаты на тестовых данных. Порядок выполнении работы описан в методическом пособии.

Научный доклад подготавливается студентом по теме заданной преподавателем. Далее докладывается на занятии перед аудиторией. Для подготовки доклада необходимо использовать методическое пособие, литературу из списка данного в программе, а также информацию из интернет источников. Время доклада ограничено, поэтому студент должен выделить только основные моменты. Доклад должен оставлять целостное впечатление.

Подготовка студента к контрольной работе заключается в решение задач на тему Вычисление корней многочленов второй, третьей и четвертой степеней над конечным полем характеристики 2. Необходимо рассмотреть задачи решенные на практическом занятии, изучить примеры данные в методическом пособии, попробовать решить задачи данные для самостоятельной работы.

Заключительная часть самостоятельной работы заключается в подготовке к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно

по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Необходимо изучить весь лекционный материал, просмотреть ссылки на другие источники информации.

Необходимо также просмотреть все виды практических заданий и их решения. При необходимости доделать домашние задания. Зачёт заключается в ответе на теоретический вопрос и решении практической задачи.

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

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

**11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)**

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

**12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья**

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.04.01 "Информационная безопасность" и магистерской программе "Математические методы и программные технологии защиты информации".

*Приложение 2*
*к рабочей программе дисциплины (модуля)*
*Б1.В.ОД.12 Математические методы в криптографии*

**Перечень литературы, необходимой для освоения дисциплины (модуля)**

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Математические методы и программные технологии защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

**Основная литература:**

1.Кнауб Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю.А. Шитов. -
Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5- 7638-2113- 7.
http://znanium.com/bookread2.php?book=441493

2 Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6, 500 экз.
http://znanium.com/bookread2.php?book=474838

3. Марченков, С.С. Основы теории булевых функций. [Электронный ресурс] ? Электрон. дан. ? М. : Физматлит, 2014. ? 136 с. ? Режим доступа:
http://e.lanbook.com/book/59714

**Дополнительная литература:**

1.Криптографические методы защиты информации [Электронный ресурс] : Учебное пособие для вузов / Рябко Б.Я., Фионов А.Н. - 2-е издание, стереотип. - М. : Горячая линия - Телеком, 2012. -
http://www.studentlibrary.ru/book/ISBN9785991202862.html

2.Сидельников, В. М. Теория кодирования [Электронный ресурс] / В. М. Сидельников. - М.: ФИЗМАТЛИТ, 2008. - 324 с. - ISBN 978-5-9221-0943-7. http://znanium.com/bookread2.php?book=544713

3. Музыкантский, А.И. Лекции по криптографии [Электронный ресурс] : учеб. пособие / А.И. Музыкантский, В.В. Фурин. ? Электрон. дан. ? Москва : МЦНМО, 2013. ? 68 с. ? Режим доступа: https://e.lanbook.com/book/56408.

*Приложение 3*
*к рабочей программе дисциплины (модуля)*
*Б1.В.ОД.12 Математические методы в криптографии*

**Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем**

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Математические методы и программные технологии защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. 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, учебно-методические комплексы, 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 образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.