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

Модульные вычисления и основы криптографии

Направление подготовки: 09.03.02 - Информационные системы и технологии
Профиль подготовки: Информационные системы в образовании
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

Содержание

Программу дисциплины разработал(а)(и) заведующий кафедрой, к.н. (доцент) Гафаров Ф.М. (Кафедра информационных систем, отделение фундаментальной информатики и информационных технологий), Fail.Gafarov@kpfu.ru ; старший преподаватель, б/с Гилемзянов А.Ф. (Кафедра информационных систем, отделение фундаментальной информатики и информационных технологий), AIFGilemzyanov@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
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности
ПК-2	Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

Основы работы с современными вычислительными системами, математические алгоритмы

Должен уметь:

Использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем

Должен владеть:

Способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем

Должен демонстрировать способность и готовность:

Использовать методы математического, алгоритмического моделирования и криптографические методы при решении теоретических и прикладных задач в области шифрования данных.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.04.03 Дисциплины (модули)" основной профессиональной образовательной программы 09.03.02 "Информационные системы и технологии (Информационные системы в образовании)" и относится к дисциплинам по выбору.

Осваивается на 4 курсе в 7 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 - 0 часа(ов), лабораторные работы - 18 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 18 часа(ов).

Контроль (зачёт / экзамен) - 18 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 7 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. Введение в криптографию.	7	2	0	2	2
2.	Тема 2. Методы симметричных систем защиты информации.	7	4	0	4	4
3.	Тема 3. Асимметричные системы защиты информации.	7	4	0	4	5
4.	Тема 4. Криптография на эллиптических кривых.	7	6	0	6	5
5.	Тема 5. Методы установления подлинности и целостности данных.	7	2	0	2	2
Итого			18	0	18	18

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	

4.2 Содержание дисциплины (модуля)

Тема 1. Введение в криптографию.

Основные понятия, обозначения и задачи криптографии. Основные принципы криптографической защиты информации. Исторические примеры криптосистем. Алгоритм создания и общепринятые требования для любой криптосистемы. Функции шифрования. Односторонние функции. Простейшие шифры и их классификация. Примеры. Методы криптоанализа. Частотный анализ текста. Криптостойкость алгоритма шифрования.

Абсолютно стойкие (совершенные) шифры. Модульная арифметика в криптографии.

Решение сравнений. Возведение в большую степень по модулю.

Тема 2. Методы симметричных систем защиты информации.

Особенности и типы симметричных криптосистем. Шифры замены. Квадрат Полибия. Шифр Виженера. Двоичный шифр Бэкона. Аффинные криптосистемы. Реализация однобуквенных, биграммных и триграммных преобразований. Возможности усложнения. Шифры перестановки. Столбцевая перестановка. Двойная перестановка. Решетка Кардано. Композиция шифров. Способы усложнения шифров.

28147-89.

Тема 3. Асимметричные системы защиты информации.

Системы защиты с открытым ключом. Необходимые сведения из алгебры для криптосистемы RSA. Криптосистема RSA. Варианты реализации: простой, биграммный, блочный. Неудачный выбор параметров криптосистемы. Атаки на алгоритм RSA. Аутентификация на основе алгоритма RSA. Необходимые сведения из алгебры для криптосистемы RSA. Выбор параметров криптосистемы

Тема 4. Криптография на эллиптических кривых.

Основные свойства эллиптических кривых. Абелева группа точек эллиптической кривой. Криптосистемы на эллиптических кривых. Ключевой обмен и шифрование Эль-Гамаля с

использованием точек эллиптических кривых. Системы защиты Диффи-Хеллмана и МэссиОмуры с использованием точек эллиптических кривых. Критерий простоты, использующий эллиптические кривые. Разложение на множители при помощи эллиптических кривых.

Тема 5. Методы установления подлинности и целостности данных.

Аутентификация данных. Электронная цифровая подпись. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля. Асимметричное шифрование алгоритмом Рабина. ЭЦП Рабина. Необратимые операции в блочном шифровании. Шифры перестановки. Квадрат "Кардана". MARS структура: образующая функция, схемы входного и выходного

перемешивания.

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)

Научно-информационный ресурс - http://www.cryptography.ru/

Научно-информационный ресурс по криптографии и теории кодирования - http://gouspo.ru/

Сайт, содержащий необходимые дистрибутивы и полную информацию для языка программирования Python - https://www.python.org/

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

Вид работ	Методические рекомендации
лекции	Студенты для лучшего восприятия лекционного материала готовятся к лекциям заблаговременно. Преподаватель сообщает на первом занятии тематику предстоящих лекций. Студенты актуализируют имеющиеся у них по данной теме знания, прорабатывают учебную литературу. Во время лекции при возникновении неясных моментов студенты из фиксируют и в конце лекции задают преподавателю.
лабораторные работы	Темы для конкретных работ предлагаются преподавателем. Однако, студенты имеют право выбора тем из предложенных. Поэтому студентам заранее предлагается список выбора тем, они его изучают, готовятся, прорабатывают учебную литературу. Это дает возможность сделать выбор темы осознанно. Темы могут обсуждаться с преподавателем. Инструментарий зависит от имеющегося программного обеспечения.
самостоя-тельная работа	Самостоятельная работа включает в себя работу с лекционным материалом, подготовку к лекциям, лабораторным работам и выполнение лабораторных работ вне аудитории, а аткже изучение нового материала. Изучение нового материала по теме должно обязательно сопровождаться ознакомлением с новейшими достижениями, так как данная сфера относитсыя к быстро развивающимся областям.
экзамен	Экзамен проводится по известным заранее студентам вопросам. Это дает возможность студентам заранее подготовиться и разобрать непонятные моменты с преподавателем. При ответе на вопросы билета необходимо продемонстрировать развернутые знания в данной области, а также отразить новейшие достижения по указанному вопросу.

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.

Компьютерный класс.

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 09.03.02 "Информационные системы и технологии" и профилю подготовки "Информационные системы в образовании".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.04.03 Модульные вычисления и основы криптографии

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 09.03.02 - Информационные системы и технологии
Профиль подготовки: Информационные системы в образовании
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

Основная литература:

1.Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - Санкт-Петербург : Лань, 2011. - 400 с. - ISBN 978-5-8114-1116-0. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/68466 (дата обращения: 02.03.2020). - Режим доступа: для авториз. пользователей.

2.Торстейнсон, П. Криптография и безопасность в технологии. NET / П. Торстейнсон, Г. А. Ганеш ; под редакцией С. М. Молявко ; перевод с английского В. Д. Хорева. - 3-е изд. (эл.). - Москва : Лаборатория знаний, 2015. - 428 с. - ISBN 978-5-9963-2952-6. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/70724 (дата обращения: 02.03.2020). - Режим доступа: для авториз. пользователей.

3. Стефанова, И. А. Обработка данных и компьютерное моделирование : учебное пособие / И. А. Стефанова. - Санкт-Петербург : Лань, 2020. - 112 с. - ISBN 978-5-8114-4010-8. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/126939 (дата обращения: 02.03.2020). - Режим доступа: для авториз. пользователей.

4. Информационный мир XXI века. Криптография - основа информационной безопасности : методическое руководство / под ред. Э. А. Болелова ; Московский государственный технический университет гражданской авиации. - 4-е изд. - Москва : Издательско-торговая корпорация 'Дашков и К-', 2020. - 126 с. - ISBN 978-5-394-03777-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1081675 (дата обращения: 02.03.2020). - Режим доступа: по подписке.

Дополнительная литература:

1. Белугина, С. В. Разработка программных модулей программного обеспечения для компьютерных систем. Прикладное программирование : учебное пособие / С. В. Белугина. - Санкт-Петербург : Лань, 2020. - 312 с. - ISBN 978-5-8114-4496-0. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/133920 (дата обращения: 02.03.2020). - Режим доступа: для авториз. пользователей.

2. Применение искусственных нейронных сетей и системы остаточных классов в криптографии : монография / Н. И. Червяков, А. А. Евдокимов, А. И. Галушкин, И. Н. Лавриненко. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. - ISBN 978-5-9221-1386-1. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/5300 (дата обращения: 02.03.2020). - Режим доступа: для авториз. пользователей.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.04.03 Модульные вычисления и основы криптографии

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

Направление подготовки: 09.03.02 - Информационные системы и технологии
Профиль подготовки: Информационные системы в образовании
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

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 Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

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.