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

подписано электронно-цифровой подписью

Программа дисциплины

Основы криптографии

Направление подготовки: 01.03.02 - Прикладная математика и информатика
Профиль подготовки: Прикладная математика и информатика
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

Содержание

Программу дисциплины разработал(а)(и): старший преподаватель, б/с Хайруллин А.Ф. (кафедра теоретической кибернетики, отделение фундаментальной информатики и информационных технологий), Alfred.Khairoullin@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
ПК-1	Способен осуществлять проведение работ по обработке, анализу научно-технической информации и результатов исследований

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

необходимость обеспечения комплексной информационной безопасности любых объектов;

Должен уметь:

ориентироваться в существующих системах криптографической защиты информации;

Должен владеть:

теоретическими знаниями о методах криптографической защиты информации;

Должен демонстрировать способность и готовность:

приобрести навыки простейшей организации защиты информационных систем.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.04.01 Дисциплины (модули)" основной профессиональной образовательной программы 01.03.02 "Прикладная математика и информатика (Прикладная математика и информатика)" и относится к дисциплинам по выбору части ОПОП ВО, формируемой участниками образовательных отношений.

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 5 зачетных(ые) единиц(ы) на 180 часа(ов).

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

Самостоятельная работа - 144 часа(ов).

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

Форма промежуточного контроля дисциплины: зачет 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, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабораторные работы, всего	Лабораторные в эл. форме	
1.	Тема 1. Введение. Информационная безопасность компьютерных систем.	7	0	0	0	0	6	0	44

N	Разделы дисциплины / модуля	Се-местр	Виды и часы контактной работы, их трудоемкость (в часах)						Самостоятельная работа
			Лекции, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабораторные работы, всего	Лабораторные в эл. форме	
2.	Тема 2. Формальные модели криптосистем. Классические симметричные криптосистемы. Современные симметричные криптосистемы (блочные системы шифрования). Поточные шифры. Асимметрические криптосистемы (системы шифрования с открытым ключом).	7	0	0	0	0	16	0	52
3.	Тема 3. Идентификация и проверка подлинности. Аутентификация сообщений и функции хэширования. Управление криптографическими ключами. Цифровая подпись. Протоколы распределения ключей. Практические аспекты применения криптосистем.	7	0	0	0	0	14	0	48
	Итого		0	0	0	0	36	0	144

4.2 Содержание дисциплины (модуля)

Тема 1. Введение. Информационная безопасность компьютерных систем.

Цель и задачи курса. Структура курса и его связь с другими дисциплинами. Краткий исторический очерк о развитии систем защиты информации в России и за рубежом. Основные понятия и определения. Основные угрозы безопасности автоматизированных систем обработки информации (АСОИ). Обеспечение безопасности АСОИ. Принципы криптографической защиты информации. Основные приложения современной криптографии. Аппаратные и программные средства защиты информации.

Тема 2. Формальные модели криптосистем. Классические симметричные криптосистемы. Современные симметричные криптосистемы (блочные системы шифрования). Поточные шифры. Асимметрические криптосистемы (системы шифрования с открытым ключом).

Надежность шифров. Теоретическая и практическая стойкость шифров. Классификация шифров по различным признакам. Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр. Принципы построения блочных шифров. Прин-цип итерирования. Схема Фейстеля. Стандарты блочного шифрования. Федеральный стандарт США DES. Российский стандарт шифрования данных ГОСТ-28147-89. Известные блочные шифры: IDEA, RC-5, BlowFish, CAST-128 и т.п.. Новые стандарты криптографической защиты информации: шифр Rijndael и др. Режимы ис-пользования блочных шифров: ECB, CBC, CFB, OFB. Режимы шифрования данных российского стандарта. Комбинирование алгоритмов блочного шифрования. Криптосистемы с депонированием ключей. Криптоалгоритм Skipjack. Стандарт криптографической защиты AES. Атаки на блочные шифры.Принципы построения поточных шифров. Примеры поточных криптосистем (RC4, A5, Panama и др.). Генераторы псевдослучайных последовательностей. Принципы построения асимметрических криптосистем. Теоретико-числовой и алгебраический аппарат, используемый при построении асимметрических криптосистем. Криптоалгоритмы RSA и Эль-Гамаля; криптография на основе эллиптических кривых над конечными полями.

Тема 3. Идентификация и проверка подлинности. Аутентификация сообщений и функции хэширования. Управление криптографическими ключами. Цифровая подпись. Протоколы распределения ключей. Практические аспекты применения криптосистем.

Основные понятия и концепции. Идентификация и аутентификация. Особенности применения паролей для идентификации пользователя. Взаимная проверка пользователей. Протоколы идентификации. Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы создания электронной цифровой подписи (RSA, EGSA, ECDSA). Стандарты цифровой подписи. Алгоритм цифровой подписи DSA. Российский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функциональными возможностями: схема слепой цифровой подписи, схема неоспоримой подписи. Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей. Передача ключей с использование симметричного шифрования. Двусторонние и трехсторонние протоколы. Передача ключей с использованием асимметричных систем шифрования. Протоколы без использования и с использованием цифровой подписи. Протокол Kerberos. Требования к криптосистемам. Длина ключа и стойкость. Шифрование и архивирование. Шифрование и кодирование. Стандартизация алгоритмов шифрования.

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 науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

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

М. Анохин, Блочные криптографические алгоритмы. - Отличный краткий обзор современного состояния криптоанализа на русском языке. - http://www.cryptography.ru/db/msg.html?mid=1162999&uri=node4.html

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

Портал математических интернет-ресурсов - http://www.math.ru/

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)

Википедия - http://ru.wikipedia.org/

Интернет-портал математических образовательных ресурсов - http://www.math.ru/

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

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

Компьютерная энциклопедия - http://www.computer-encyclopedia.ru

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

Вид работ	Методические рекомендации
лабораторные работы	Лабораторные работы проводятся в аудиторные часы, и с использованием материала, преподаваемого в аудитории. Дополнительного изучения материала вне аудитории не требуется. Необходимо понимание организации процесса разработки программного обеспечения. Базовые знания разработки ПО (стадии, базовое понимание разработки архитектуры ПО).
самостоя-тельная работа	Самостоятельные работы проводятся вне аудиторных часов в группах, на которые студенты делятся самостоятельно. Результат работы группы оценивается совокупно, а не по вкладу каждого отдельного ее участника. При выполнении заданий по самостоятельной работе рекомендуется активно изучать открытые интернет-ресурсы проводить совместные обсуждения для решения поставленной задачи.
зачет	Для подготовки к зачету следует повторить все письменные записи, изучить основную и дополнительную литературу, рекомендованные интернет-ресурсы. Приветствуется самостоятельное изучение дополнительного материала по теме. Оценивается владение материалом, способность оперировать изученными терминами и определениями. Возникшие вопросы студент должен задать в течении курса и во время консультации.

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.

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 01.03.02 "Прикладная математика и информатика" и профилю подготовки "Прикладная математика и информатика".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.04.01 Основы криптографии

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.03.02 - Прикладная математика и информатика

Профиль подготовки: Прикладная математика и информатика

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2024

Основная литература:

1.Теоретические основы информатики / Царев Р.Ю., Пупков А.Н., Самарин В.В. - Краснояр.:СФУ, 2015. - 176 с.: ISBN - Режим доступа: http://znanium.com/catalog/product/549801

2.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. Режим доступа: http://znanium.com/catalog.php?bookinfo=441493

3.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. Режим доступа: http://znanium.com/bookread.php?book=405000

4. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие. - Казань: Казанский университет, 2012. - 138 с. - Режим доступа: http://kpfu.ru/docs/F366166681/mzi.pdf

Дополнительная литература:

1.Рябко Б.Я., 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. - 229 с. - ISBN 978-5-9912-0286-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202862.html

2. Петров А.А., Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / Петров А.А. - М. : ДМК Пресс, 2008. - 448 с. - ISBN 5-89818-064-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN5898180648.html

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.04.01 Основы криптографии

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

Направление подготовки: 01.03.02 - Прикладная математика и информатика

Профиль подготовки: Прикладная математика и информатика

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2024

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.