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

Криптографические методы защиты информации

Направление подготовки: 02.03.02 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Системный анализ и информационные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), Shamil.Ishmukhametov@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	Способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям
ПК-2	Способность понимать, совершенствовать и применять современный математический аппарат, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- основные результаты теории чисел и алгебры, понимать проблемы сложности алгоритмов.

Должен уметь:

- использовать на практике полученные знания.

Должен владеть:

- знаниями по основным разделам теории кодирования и криптографии.

Должен демонстрировать способность и готовность:

- знаниями по основным разделам теории кодирования и криптографии.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.11 Дисциплины (модули)" основной профессиональной образовательной программы 02.03.02 "Фундаментальная информатика и информационные технологии (Системный анализ и информационные технологии)" и относится к дисциплинам по выбору.
Осваивается на 4 курсе в 8 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 4 зачетных(ые) единиц(ы) на 144 часа(ов).

Контактная работа - 56 часа(ов), в том числе лекции - 28 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 28 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 52 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 8 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. Сложность алгоритмов	8	2	0	0	5
2.	Тема 2. Сведения из теории чисел	8	2	0	0	5

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Алгебраические структуры, конечные поля	8	2	0	2	5
4.	Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.	8	2	0	2	5
5.	Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.	8	2	0	4	6
6.	Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.	8	2	0	4	5
7.	Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	8	4	0	4	5
8.	Тема 8. Симметричное шифрование: докомпьютерные шифры.	8	4	0	4	5
9.	Тема 9. Обзор результатов Клода Шеннона	8	4	0	4	5
10.	Тема 10. Симметричное шифрование: обзор современных шифров.	8	4	0	4	6
	Итого		28	0	28	52

4.2 Содержание дисциплины (модуля)

Тема 1. Сложность алгоритмов

Понятие сложности алгоритмов. Верхние и нижние оценки. Приемы построения оценок. Классы сложности. Классы P и NP. Полиномиальная сводимость. NP-трудные проблемы. Вычислительная сложность сортировки массива, поиска в базе данных, факторизации натуральных чисел. NP-полные проблемы. NP-полнота проблемы выполнимости произвольной булевой формулы.

Тема 2. Сведения из теории чисел

Кольцо вычетов Zn. Полная и приведенные системы вычетов. Функция Эйлера. Теорема Эйлера. Мультипликативность функции Эйлера. Решений сравнений 1 и 2-о порядка. Символ Лежандра и его определение. Правила вычисления символа Лежандра. Закон квадратичной взаимности Гаусса. Пример вычисления символа Лежандра.

Тема 3. Алгебраические структуры, конечные поля

Алгебраические структуры: группы, кольца, поля. Конечные поля простой характеристики. Расширений конечных полей. Вычисления в конечных полях. Вычисление обратных элементов с использование расширенного алгоритма Евклида. Расширения конечных полей. Неприводимые многочлены. Критерий неприводимости многочлена.

Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.

Общая задача построения кодов. Избыточные и неизбыточные коды. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга. Использование избыточных кодов в криптографии. Псевдослучайные последовательности. Генерация псевдослучайных последовательностей. Алгоритм RC4 и оценка его криптографической стойкости.

Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.

Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ. Матричное задание кодов. Задание циклического кода порождающей и проверочной матрицами. Построение матрицы кодов для несистематического циклического кода циклическим сдвигом порождающего и проверочного многочленов, т.е. путем их умножения на переменную.

Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.

Ввендение в мажоритарное декодирование. Коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона. Использование кодов Рида-Маллера в криптографии.

Основные стратегий борьбы с ошибками в системах связи:

1. обнаружение ошибок в блоках данных и автоматический запрос повторной передачи поврежденных блоков;

2. обнаружение ошибок в блоках данных и отбрасывание поврежденных блоков;

3. исправление ошибок (англ. forward error correction) на физическом уровне.

Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.

Аспекты безопасности, основные угрозы. Стандарты и законодательство в области информационной безопасности. Федеральные законы и постановления Российской Федерации об электронной подписи, о защите персональных данных, авторского права. Серия стандартов информационной безопасности 27000. Теория оценки рисков.

Тема 8. Симметричное шифрование: докомпьютерные шифры.

Разработка алгоритмов симметричного шифрования. Хеш-функции. Блочные и потоковые методы. Примеры. Криптографические примитивы. Примеры использования криптографических примитивов. Сдвиги, перемешивания, перестановки. Недостатки отдельных криптографических примитивов. Взлом компьютерных шифров. Шифры Фейстеля.

Тема 9. Обзор результатов Клода Шеннона

Прямая и обратная теоремы Шеннона для источника общего вида о связи энтропии источника и средней длины сообщений.Прямая и обратная теоремы Шеннона для источника без памяти о связи энтропии источника и достижимой степени сжатия с помощью кодирования с потерями и последующего неоднозначного декодирования.

Тема 10. Симметричное шифрование: обзор современных шифров.

Симметричное шифрование: методы DES, AES, RC4. Их свойства и особенности применения. Достоинства и недостатки алгоритма DES. Усиление алгоритма DES, алгроитм 3DES. Конкурс на замещение национального криптографического стандарта США. Современные алгоритмы шифрования в США, Европе и России. Федеральный закон РФ об электронной подписи 2012 года.

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)

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

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

Интернет--портал ресурсов по математическим наукам - http://www.mathnet.ru

Интернет--портал ресурсов по математическим наукам - http://www.allmath.com/

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

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

Вид работ	Методические рекомендации
лекции	Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.
лабораторные работы	Лабораторные занятия призваны дать такой практический навык, а также навыки программирования криптографических алгоритмов и их внедрения в информационные системы. В ходе выполнения работ происходит отработка знаний студентов по программированию криптографических алгоритмов, изучаются специальных разделы программирования комплексных систем информационной безопасности.
самостоя-тельная работа	Самостоятельная работа предполагает выполнение домашних работ при подготовке к контрольной работе и выполнении компьютерной программы. Самостоятельная работа выполняется в несколько этапов. Сначала предполагается изучение теоретического материала. Также рекомендуется каждый раздел программы сопровождать практической работой, выполняя лабораторные занятия.

Вид работ	Методические рекомендации
экзамен	При подготовке к экзамену рекомендуется разбить материал на смысловые блоки и изучать его, выписывая краткое содержание блока. По каждому блоку надо составить контрольные вопросы и самостоятельно составить краткие ответы по вопросам. Прочитав лекции, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

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 02.03.02 "Фундаментальная информатика и информационные технологии" и профилю подготовки "Системный анализ и информационные технологии".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.11 Криптографические методы защиты информации

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 02.03.02 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Системный анализ и информационные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016

Основная литература:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. - 416 с. Режим доступа: http://znanium.com/bookread2.php?book=775200

2. Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. Пособие / Е.В. Глинская, Н.В. Чичварин. - М. : ИНФРА-М, 2018. Режим доступа: http://znanium.com/bookread2.php?book=925825

3. Партыка Т. Л. Информационная безопасность : учеб. Пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. И доп. - М. : ФОРУМ : ИНФРА-М, 2018. - 432 с. Режим доступа: http://znanium.com/bookread2.php?book=915902

4. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. Режим доступа: http://znanium.com/bookread2.php?book=495249

5. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие. - Электрон. Дан. - СПб. : Лань, 2016. - 324 с. - Режим доступа: http://e.lanbook.com/book/75515

6. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. - Режим доступа: http://znanium.com/bookread2.php?book=405313

Дополнительная литература:

1.Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - 465 с. - Режим доступа: http://znanium.com/catalog/product/944503

2. Жук А. П. 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. - Режим доступа: http://znanium.com/bookread.php?book=474838

3. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://znanium.com/bookread.php?book=503511

4. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - Режим доступа: http://znanium.com/bookread.php?book=491597

5. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с. - Режим доступа: http://znanium.com/bookread.php?book=169345

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.11 Криптографические методы защиты информации

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

Направление подготовки: 02.03.02 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Системный анализ и информационные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016

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.