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

Программирование криптографических алгоритмов Б1.В.ДВ.3

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2019
Автор(ы): Ишмухаметов Ш.Т.
Рецензент(ы): Разинков Е.В.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 20__г.
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No _____ от "____" _____ 20__г.

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

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

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)

4.2. Содержание дисциплины

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

6. Фонд оценочных средств по дисциплине (модулю)

6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1. Основная литература

7.2. Дополнительная литература

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

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

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

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

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

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 образовательной программы

Выпускник, освоивший дисциплину, должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

Выпускник, освоивший дисциплину:

Должен знать:

Базовые алгоритмы шифрования и электронной подписи

Должен уметь:

Использовать современные технические устройства для защиты информации

Должен владеть:

Знаниями в области современных методов защиты информации

Должен демонстрировать способность и готовность:

1. Работать с использованием знаний по основным разделам информационной безопасности и криптографии.

2. Владеть базовыми знаниями по алгоритмам шифрования, построения электронной подписи.

3. Владеть основными правовыми постановлениями и законами в области информационной безопасности.

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Данная учебная дисциплина включена в раздел "Б1.В.ДВ.3 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к дисциплинам по выбору.
Осваивается на 3 курсе в 6 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 - 72 часа(ов), в том числе лекции - 36 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 36 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 36 часа(ов).

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

Форма промежуточного контроля дисциплины: экзамен в 6 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	
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 теорию сложности алгоритмов. Получение верхних оценок сложности.	6	4	0	2	4
2.	Тема 2. Потоковые и блочные шифры. Криптографические примитивы: подстановки, перестановки, гаммирование. Метод DES.	6	4	0	4	4
3.	Тема 3. Методы шифрования с двумя ключами. Метод RSA.	6	4	0	4	4
4.	Тема 4. Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля.	6	4	0	4	4
5.	Тема 5. Контрольная работа по RSA.	6	0	0	2	4
6.	Тема 6. Вычисления в конечных полях. Задача вычисления дискретного логарифма. Метод Шенкса. Оценки сложности для задачи дискретного логарифмирования.	6	4	0	4	4
7.	Тема 7. Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами. Контрольная работа по теме.	6	4	0	8	4
8.	Тема 8. Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера.	6	4	0	4	4
9.	Тема 9. Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита.	6	6	0	4	4
	Итого		36	0	36	36

4.2 Содержание дисциплины

Тема 1. Введение в теорию сложности алгоритмов. Получение верхних оценок сложности.

Основные понятия теории сложности алгоритмов. Верхние и нижние оценки. Классы сложности алгоритмов. Полиномиальные и экспоненциальные алгоритмы.

Полиномиальная сводимость. Классы сложности. NP-трудные задачи. Примеры NP-трудных задач. Проблема P=NP и её анализ. Полнота задачи проверки выполнимости булевой формулы.

Тема 2. Потоковые и блочные шифры. Криптографические примитивы: подстановки, перестановки, гаммирование. Метод DES.

Потоковые и блочные шифры. Криптографические примитивы: подстановки, перестановки, гаммирование. Метод DES. Слабости и уязвимости алгоритма DES. Переход к новым криптографическими стандартам. Алгоритм AES и его краткое описание. Сочетание линейных и нелинейных преобразований. Проблема передачи ключа шифрования.

Тема 3. Методы шифрования с двумя ключами. Метод RSA.

Методы шифрования с двумя ключами. Метод RSA.

Основные вычислительные алгоритмы, используемые в RSA. Поиск обратных по модулю элементов. Алгоритм быстрого возведения в степень. Генерация ключей RSA. Алгоритмы факторизации. Ро-метод Полларда и оценка его сходимости. Метод факторизации Ферма. Примеры.

Тема 4. Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля.

Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля. Шифрование и создание электронной подписи на основе метода Эль-Гамаля.

Юридическая значимость электронной цифровой подписи. Российское законодательство в в области защиты информации. Федеральный закон 2012 года Об электронной подписи. Его основные положения.

Тема 5. Контрольная работа по RSA.

Контрольная работа по RSA.

1. Проверить заданное число на простоту, используя вероятностный алгоритм Миллера-Рабина.
2. Генерировать два случайных простых числа из заданного интервала.
3. Построить открытый и секретные ключи RSA и и выполните их проверку на устойчивость.
4. Зашифровать заданное сообщение и выполнить его проверку дальше сделать обратное преобразование

Тема 6. Вычисления в конечных полях. Задача вычисления дискретного логарифма. Метод Шенкса. Оценки сложности для задачи дискретного логарифмирования.

Вычисления в конечных полях. Задача вычисления дискретного логарифма. Метод Шенкса. Оценки сложности для задачи дискретного логарифмирования.

Конечные поля. Вычисления в конечных полях.Решение уравнения Безу и поиск обратных элементов. Порядок элемента. Примитивные элементы конечного поля. Теорема о примитивных элементах.

Тема 7. Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами. Контрольная работа по теме.

Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами.

Формулы для вычисления суммы точек эллиптических кривых, их геометрическая интерпретация. Перевод формул в другие координаты. Афинные и проективных координаты, их связь. Вычисление кратного заданной точки.

Тема 8. Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера.

Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера.

Алгоритм сведения задачи дискретного логарифмирования на эллиптических кривых к задаче вычисления дискретного логарифма в конечных полях. Особые кривые. Использование преобразования Вейля-Тейта в криптографии. Реализация алгоритма Миллера.

Тема 9. Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита.

Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита.

Особенности удаленной аутентификации в локальных сетях. Аутентификация в сетях Интернет. Угрозы информационной безопасности в сетях. Использование криптографических примитивов в программировании сетевых приложений. Объектно-ориентированное программирование.

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".

Положение от 29 декабря 2018 г. № 0.1.1.67-08/328 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет".

Положение № 0.1.1.67-06/241/15 от 14 декабря 2015 г. "О формировании фонда оценочных средств для проведения текущей, промежуточной и итоговой аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"".

Положение № 0.1.1.56-06/54/11 от 26 октября 2011 г. "Об электронных образовательных ресурсах федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/66/16 от 30 марта 2016 г. "Разработки, регистрации, подготовки к использованию в учебном процессе и удаления электронных образовательных ресурсов в системе электронного обучения федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/11/16 от 25 января 2016 г. "О балльно-рейтинговой системе оценки знаний обучающихся в федеральном государственном автономном образовательном учреждении высшего образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/91/13 от 21 июня 2013 г. "О порядке разработки и выпуска учебных изданий в федеральном государственном автономном образовательном учреждении высшего профессионального образования "Казанский (Приволжский) федеральный университет"".

6. Фонд оценочных средств по дисциплине (модулю)

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
Семестр 6			
	Текущий контроль		
1	Контрольная работа	ОПК-2 , ОПК-4 , ОПК-7 , ПК-1 , ПК-10 , ПК-11	4. Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля.
2	Контрольная работа	ОПК-2 , ОПК-4 , ОПК-7 , ПК-1 , ПК-10 , ПК-11	9. Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита.
3	Компьютерная программа	ОПК-2 , ОПК-4 , ОПК-7 , ПК-1 , ПК-10 , ПК-11	7. Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами. Контрольная работа по теме.
	Экзамен	ОПК-2, ПК-10, ПК-11	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Семестр 6					
Текущий контроль					
Контрольная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.	1 2
Компьютерная программа	Высокий уровень умений и навыков программирования, в том числе моделирования, алгоритмизации, использования языка программирования. Поставленная задача полностью решена.	Хороший уровень умений и навыков программирования, в том числе моделирования, алгоритмизации, использования языка программирования. Поставленная задача в основном решена.	Удовлетворительный уровень умений и навыков программирования, в том числе моделирования, алгоритмизации, использования языка программирования. Поставленная задача решена частично.	Недостаточный уровень умений и навыков программирования, в том числе моделирования, алгоритмизации, использования языка программирования. Поставленная задача не решена.	3

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Экзамен	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании, изложении и использовании учебно-программного материала.	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.	

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Семестр 6

Текущий контроль

1. Контрольная работа

Тема 4

1. Проверить число n=57 на простоту, используя одну итерацию теста Миллера-Рабина с базой a=2.
2. Используя заданные значения p, q и e, вычислить остальные параметры RSA и расшифровать число m. Для вычисления d использовать расширенный алгоритм Евклида: p=17, q=29, e=239, m=24.
3. Выполнить шифрование текста на основе методов перестановки, подстановок и гаммирования.

Варианты контрольной работы отличаются числовыми данными.

2. Контрольная работа

Тема 9

1. Решить уравнение 2-й степени в конечном поле.
2. Вычислить символ Лежандра для заданного элемента в кольце вычетов.
3. Решить реккурентное уравнение с использованием производящих функций.

Варианты контрольной работы отличаются исходным данными.

3. Компьютерная программа

Тема 7

Разработать комплекс программ для компьютера, реализующих криптографические примитивы.

На основе них разработать пользовательский интерфейс и программу, осуществляющая решение задач защиты информации в компьютерных сетях.
Реализовать алгоритм построения электронной подписи.

Экзамен

Вопросы к экзамену:
1. Основные принципы организации и задачи сетевой безопасности.
2. Описание модели OSI межсетевых взаимодействий.
3. Общая характеристика TCP/IP
4. Протоколы IPv4.
5. Односторонние функции. Хеш-функции. Алгоритм HMAC
6. Метод RC4.
7. Метод RSA.
8 Алгоритм шифрования Эль-Гамаля.
9. Метод выработки секретного ключа Диффи-Хелмана.
10 Электронно-цифровая подпись. Ее свойства и правовые основы. Алгоритм создание ЭЦП.
11 Эллиптические кривые. Операции сложения и удвоения на множестве точек ЭК.
12 Криптографические протоколы на эллиптических кривых.
13 Разработка клиент-серверных приложений в C++.
14 Стандарт сертификации X.509. Состав сертификата.
15 Организация защиты данных в сетях. Протокол IPsec.
11. Защита Web. Архитектура SSL. Протокол квитирования SSL.
12. Протокол SET. Сравнительные характеристики протоколов SSL и SET.
13. Организация сетей GSM .
14. Защита сетей GSM.
15. Алгоритм проверки простоты целых чисел Ферма.
16. Алгоритм проверки простоты целых чисел Рабина-Миллера.
17. Методы факторизации целых чисел. Ро-метод Полларда.
18. Методы факторизации целых чисел. (p-1)-метод Полларда.
19. Факторизация на основе эллиптических кривых.
20. Метод факторизации квадратичного решета.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В КФУ действует балльно-рейтинговая система оценки знаний обучающихся. Суммарно по дисциплине (модулю) можно получить максимум 100 баллов за семестр, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов.

Для зачёта:

56 баллов и более - "зачтено".

55 баллов и менее - "не зачтено".

Для экзамена:

86 баллов и более - "отлично".

71-85 баллов - "хорошо".

56-70 баллов - "удовлетворительно".

55 баллов и менее - "неудовлетворительно".

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Семестр 6			

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Текущий контроль			
Контрольная работа	Контрольная работа проводится в часы аудиторной работы. Обучающиеся получают задания для проверки усвоения пройденного материала. Работа выполняется в письменном виде и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	1 2	15 15
Компьютерная программа	Обучающиеся самостоятельно составляют программу на определённом языке программирования в соответствии с заданием. Программа сдаётся преподавателю в электронном виде. Оценивается реализация алгоритмов на языке программирования, достижение заданного результата.	3	20
Экзамен	Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература:

1.Шаньгин В.Ф., Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785940747680.html

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/bookread2.php?book=474838

3. 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

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

5. Девянин П.Н., Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - 2-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203289.html

7.2. Дополнительная литература:

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

2. Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. Пособие / Е.В. Глинская, Н.В. Чичварин. - М. : ИНФРА-М, 2018. - 118 с. - Режим доступа: http://znanium.com/bookread2.php?book=925825

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/bookread2.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/bookread2.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/bookread2.php?book=169345

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 ресурсов по программированию - http://algolist.manual.ru/

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

Вид работ	Методические рекомендации
лекции	Теоретический курса материал излагается на лекциях. Конспект лекций, который остается у студента в результате прослушивания лекции содержит базовый материал, но 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, изучение специальных разделов программирования алгоритмов криптографии.
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.
контрольная работа	Текущий контроль успеваемости студентов осуществляется с помощью контрольной работы, которая призвана показать основные практические навыки решения задач, связанных с математическим обеспечением задач информационной безопасности. При подготовке к контрольной работе рекомендуется обращаться внимание на основные задачи, решенные в течение семестра, периодически решать аналогичные задачи, программировать основные вычислительные алгоритмы, чтобы лучше понять их тонкости.
компьютерная программа	Разработать комплекс компьютерных программ для удаленной аутентификаци клиентов и серверов, защиты данных с помощью шифрования и защиты целостности данных на основе алгоритмов электронной цифровой подписи. Разработать удобный интерфейс пользователя, представление данных в оконном и консолтном вариантах.
экзамен	При подготовке к экзамену рекомендуется разбивать 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)

Освоение дисциплины "Программирование криптографических алгоритмов" предполагает использование следующего программного обеспечения и информационно-справочных систем:

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.

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

Освоение дисциплины "Программирование криптографических алгоритмов" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

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 10.03.01 "Информационная безопасность" и профилю подготовки "Безопасность компьютерных систем".