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: 01.04.04 - Прикладная математика
Профиль подготовки: Классические и квантовые методы обработки информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Кугураков В.С. (кафедра теоретической кибернетики, отделение фундаментальной информатики и информационных технологий), Vladimir.Kugurakov@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-3	Способен применять знания и методы дисциплин естественно-научного и математического цикла при проведении научных исследований, в том числе математического и компьютерного моделирования и высокопроизводительных вычислений
ПК-4	Разработка, отладка, рефакторинг программного кода, баз данных, информационных ресурсов; проектирование и интеграция программного обеспечения, управление проектами в области ИТ

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- основные понятия криптологии;
- примеры секретных систем;
- алгебраическую и логическую структуру секретных систем;
- основные свойства чистых и смешанных шифров;
- понятия энтропии и надежности (и ненадежности);
- понятия однонаправленной и односторонней функций;
- основные идеи построения симметричных и асимметричных криптосистем

Должен уметь:

- применять методы алгебры, теории вероятностей и теории чисел для описания и анализа криптосистем;
- применять методы криптоанализа для простейших шифров;
- использовать на практике простейшие криптографические протоколы;

Должен владеть:

- терминологией криптологии;
- методикой использования простейших методов криптоанализа.
- методикой построения простейших криптографических систем.

Должен демонстрировать способность и готовность:

осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок

обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

проводить аттестацию объектов информатизации по требованиям безопасности информации

организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России

разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.06 Дисциплины (модули)" основной профессиональной образовательной программы 01.04.04 "Прикладная математика (Классические и квантовые методы обработки информации)" и относится к вариативной части.

Осваивается на 2 курсе в 3 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 3 зачетных(ые) единиц(ы) на 108 часа(ов).

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

Самостоятельная работа - 72 часа(ов).

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

Форма промежуточного контроля дисциплины: зачет в 3 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. Цель и задачи курса. Структура курса и его связь с другими дисциплинами. Краткий исто-рический очерк о развитии систем защиты инфор-мации в России и за рубежом.	3	3	0	0	6
2.	Тема 2. Информационная безопасность компьютер-ных систем. Основные понятия и определения. Основные угрозы безопасности автоматизирован-ных систем обработки информации (АСОИ). Обес-печение безопасности АСОИ. Принципы крипто-графической защиты информации. Основные при-ложения современной криптографии. Аппаратные и программные средства защиты информации.	3	3	0	0	6
3.	Тема 3. Формальные модели криптосистем. Надежность шифров. Теоретическая и практиче-ская стойкость шифров. Классификация шифров по различным признакам.	3	3	0	0	6
4.	Тема 4. Классические симметричные криптосистемы. Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр.	3	3	0	0	8

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
5.	Тема 5. Современные симметричные криптосистемы (блочные системы шифрования). Принципы построения блочных шифров. Принцип 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 использования 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.	3	3	0	0	8
6.	Тема 6. Поточные шифры. Принципы построения поточных шифров. Примеры поточных криптосистем (RC4, A5, Panama и др.). Генераторы псевдослучайных последовательностей.	3	4	0	0	8
7.	Тема 7. Асимметрические криптосистемы (системы шифрования с открытым ключом). 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.	3	4	0	0	6
8.	Тема 8. Идентификация и проверка подлинности. Основные понятия и концепции. Идентификация и аутентификация. Особенности применения паролей для идентификации пользователя. Взаимная проверка пользователей. Протоколы идентификации.	3	2	0	0	6

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
9.	Тема 9. Аутентификация сообщений и функции хэширования. Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94, ГОСТ Р.34.11-2013.	3	2	0	0	6
10.	Тема 10. Цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись. Алго-ритмы создания электронной цифровой подписи (RSA, EGSA, ECDSA). Стандарты цифровой под-писи. Алгоритм цифровой подписи DSA. Россий-ский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функцио-нальными возможностями: схема слепой цифро-вой подписи, схема неоспоримой подписи.	3	3	0	0	6
11.	Тема 11. Управление криптографическими ключами. Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей.	3	3	0	0	6
12.	Тема 12. Протоколы распределения 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.	3	3	0	0	0
	Итого		36	0	0	72

4.2 Содержание дисциплины (модуля)

Тема 1. Введение. Цель и задачи курса. Структура курса и его связь с другими дисциплинами. Краткий исто-рический очерк о развитии систем защиты инфор-мации в России и за рубежом.

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.

Шифр простой подстановки. Шифр многоалфавитной подстановки.

Шифр простой перестановки.

Шифр простой подстановки.

Метод гаммирования.

Линейные преобразования.

Тема 2. Информационная безопасность компьютер-ных систем. Основные понятия и определения. Основные угрозы безопасности автоматизирован-ных систем обработки информации (АСОИ). Обес-печение безопасности АСОИ. Принципы крипто-графической защиты информации. Основные при-ложения современной криптографии. Аппаратные и программные средства защиты информации.

Основные угрозы безопасности автоматизированных систем обработки информации. (АСОИ). Пассивные и активные угрозы.

Обеспечение безопасности автоматизированных систем обработки информации

Принципы криптографической защиты информации.

Основные приложения современной криптографии.

Аппаратные и программные средства защиты информации.

Тема 3. Формальные модели криптосистем. Надежность шифров. Теоретическая и практиче-ская стойкость шифров. Классификация шифров по различным признакам.

Формальные модели криптосистем.

Надежность шифров.

Теоретическая и практическая стойкость шифров.

Композиционные и итеративные шифры. Схема Фейстеля и SP-сети

Классификация шифров по различным признакам.

Закрытые (симметричные) и открытые (асимметричные) системы шифрования информации.

Блочные и поточные шифры.

Тема 4. Классические симметричные криптосистемы. Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр.

Шифры-перестановки.

Блочные и поточные шифры простой замены.

Многоалфавитные шифры замены.

Шифрование методом гаммирования.

Ленейные нелинейные преобразования, используемые при разработке шифров. Инволютивные преобразования. Методы построения инволютивных преобразований (иатриц и подстановок).

Абсолютно стойкий шифр.

Тема 5. Современные симметричные криптосистемы (блочные системы шифрования). Принципы построения блочных шифров. Принцип 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 использования 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 блочных шифров. Принцип 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 блочного шифрования.

Атаки на блочные шифры.

Тема 6. Поточные шифры. Принципы построения поточных шифров. Примеры поточных криптосистем (RC4, A5, Panama и др.). Генераторы псевдослучайных последовательностей.

Принципы построения поточных шифров.

Шифрование методом гаммирования.

Примеры поточных криптосистем (RC4, A5, Panama, SNOW и др.).

Генераторы псевдослучайных последовательностей.

Линейные и нелинейные регистры сдвига. Последовательности максимальной длины и методы их построения.

Алгоритм Берлекэмпа-Мессти.

Тема 7. Асимметрические криптосистемы (системы шифрования с открытым ключом). 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.

Принципы построения асимметрических криптосистем.

Теоретико-числовой и алгебраический аппарат, используемый при построении асимметрических криптосистем. Алгоритмы факторизации чисел и тестирования чисел на простоту.

Криптоалгоритм RSA.

Дискретное логарифмирование в конечных полях и криптоалгоритм Эль-Гамаля;

Криптография на основе эллиптических кривых над конечными полями.

Тема 8. Идентификация и проверка подлинности. Основные понятия и концепции. Идентификация и аутентификация. Особенности применения паролей для идентификации пользователя. Взаимная проверка пользователей. Протоколы идентификации.

Идентификация и аутентификация.

Фиксированные пароли (слабая идентификация).

Правила составления паролей.

Атаки на фиксированые пароли.

Усложнение процедуры проверки паролей. Протоколы идентификации.

Особенности применения паролей для идентификации пользователя.

Взаимная проверка пользователей.

Протоколы идентификации.

Личные идентификационные номера.

Запрос-ответ - сильная идентификация.

Тема 9. Аутентификация сообщений и функции хэширования. Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94, ГОСТ Р.34.11-2013.

Функции хэширования и целостность данных.

Ключевые функции хэширования.

Имитовставка ГОСТ 28147-89 как способ проверки целостности сообщения.

Бесключевые функции хэширования. Построение

Построение бесключевой функции хэширования на основе блочного шифра.

Примеры хэш-функций.

Российский стандарт хэш-функций ГОСТ Р.34.11-94, ГОСТ Р.34.11-2013.

Тема 10. Цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись. Алго-ритмы создания электронной цифровой подписи (RSA, EGSA, ECDSA). Стандарты цифровой под-писи. Алгоритм цифровой подписи DSA. Россий-ский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функцио-нальными возможностями: схема слепой цифро-вой подписи, схема неоспоримой подписи.

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 функцио-нальными возможностями: схема слепой цифро-вой подписи, схема неоспоримой подписи.

Тема 11. Управление криптографическими ключами. Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей.

Управление криптографическими ключами.

Генерация ключей.

Хранение ключей.

Концепция ключевого пространства и иерархия ключей.

Распределение ключей. Протоколы распределения ключей.

открытое распределение ключей.

Протокол Диффи-Хеллмана и его уязвимость перед атакой "Встреча по середине".

Протокол MTI и др..

Тема 12. Протоколы распределения 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.

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.

Предварительное распределение ключей.

Установление ключей для конференц-связи.

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)

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

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

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

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

Вид работ	Методические рекомендации
лекции	Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля (4-5 см) для дополнительных записей. Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры. Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий. Остальное должно быть записано своими словами. Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий. В конспект следует заносить все, что преподаватель пишет на доске, также рекомендуемые схемы, таблицы, диаграммы и т.д.
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 ра-боте рекомендуется активно изучать открытые интернет-ресурсы проводить совместные об-суждения для решения поставленной задачи.
зачет	Обучающийся представляет текст выполненных заданий в сброшюрованном виде и защищает её в форме устного доклада с последующими ответами на вопросы. Оцениваются: актуальность, теоретическая и/или практическая значимость тем исследования, её соответ-ствие направлению подготовки (специальности); своевременность выполнения этапов рабо-ты; владение материалом по теме исследования; методы; структура работы; полнота раскры-тия темы; самостоятельность работы; наличие результатов, обладающих новизной; язык из-ложения; оформление текста работы; навыки публичного выступления; способность отве-чать на вопросы по теме курсовой.

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.

Специализированная лаборатория.

Специализированная лаборатория.

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 01.04.04 "Прикладная математика" и магистерской программе "Классические и квантовые методы обработки информации".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.06 Криптографические методы защиты информации

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.04.04 - Прикладная математика

Профиль подготовки: Классические и квантовые методы обработки информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2020

Основная литература:

Теоретические основы информатики / Царев Р.Ю., Пупков А.Н., Самарин В.В [и др.]. - Краснояр.:СФУ, 2015. - 176 с.: ISBN 978-5-7638-3192-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/549801 (дата обращения: 10.03.2020). - Режим доступа: по подписке.

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. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/441493 (дата обращения: 10.03.2020). - Режим доступа: по подписке.

3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 10.03.2020). - Режим доступа: по подписке.

4. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. - 4-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2020. - 336 с. - (Высшее образование). - DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1114032

(дата обращения: 10.03.2020). - Режим доступа: по подписке.

5. Ишмухаметов, Ш.Т. Математические основы защиты информации: учебное пособие / Ш.Т. Ишмухаметов. - Казань: Казанский университет, 2012. - 138 с. - URL: http://kpfu.ru/docs/F366166681/mzi.pdf (дата обращения: 10.03.2020).

Дополнительная литература:

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. - Москва : ИД 'ФОРУМ' : ИНФРА-М, 2020. - 592 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093695 (дата обращения: 10.03.2020). - Режим доступа: по подписке.

2. Рябко Б.Я., Криптографические методы защиты информации : 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 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991202862.html (дата обращения: 10.03.2020). - Режим доступа : по подписке.

3. Петров А.А., Компьютерная безопасность. Криптографические методы защиты / Петров А.А. - М. : ДМК Пресс, 2008. - 448 с. - ISBN 5-89818-064-8 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN5898180648.html (дата обращения: 10.03.2020). - Режим доступа : по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.06 Криптографические методы защиты информации

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

Направление подготовки: 01.04.04 - Прикладная математика
Профиль подготовки: Классические и квантовые методы обработки информации
Квалификация выпускника: магистр
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.