

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



подписано электронно-цифровой подписью

**Программа дисциплины**  
**Введение в криптографию Б2.ДВ.1**

Направление подготовки: 010400.62 - Прикладная математика и информатика

Профиль подготовки: Математическое и программное обеспечение вычислительных машин и сетей

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

**Автор(ы):**

Кугураков В.С.

**Рецензент(ы):**

Гайнутдинова А.Ф.

**СОГЛАСОВАНО:**

Заведующий(ая) кафедрой: Аблаев Ф. М.

Протокол заседания кафедры No \_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 201\_\_г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:

Протокол заседания УМК No \_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 201\_\_г

Регистрационный No 969314

Казань  
2014

## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

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. Цели освоения дисциплины

Основная цель дисциплины - научить пониманию необходимости обеспечения комплексной безопасности информационных систем, получить практические знания и навыки для простейшей организации криптографически защищенной системы.

### 2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б2.ДВ.1 Общепрофессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 2 курсе, 4 семестр.

Данная дисциплина относится к общепрофессиональным дисциплинам.

Читается на 2 курсе 4 семестре для студентов, обучающихся по направлению "Прикладная математика и информатика".

### 3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-11 (профессиональные компетенции)	способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций
ПК-3 (профессиональные компетенции)	способность разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий; способность разработки проектной и программной документации, удовлетворяющей нормативным требованиям
ПК-4 (профессиональные компетенции)	способность понимать и применять в исследовательской и прикладной деятельности современный математический аппарат, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий, способность использовать современные инструментальные и вычислительные средства (в соответствии с профилем подготовки)

В результате освоения дисциплины студент:

1. должен знать:

необходимость обеспечения комплексной информационной безопасности любых объектов;

2. должен уметь:

ориентироваться в существующих системах криптографической защиты информации;

3. должен владеть:

теоретическими знаниями о методах криптографической защиты информации;

4. должен демонстрировать способность и готовность:

приобрести навыки простейшей организации защиты информационных систем.

#### 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 4 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

#### 4.1 Структура и содержание аудиторной работы по дисциплине/ модулю Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение	4		1	0	0	
2.	Тема 2. Информационная безопасность компьютерных систем.	4		1	0	3	домашнее задание
3.	Тема 3. Формальные модели криптосистем.	4		1	0	3	домашнее задание
4.	Тема 4. Классические симметричные криптосистемы.	4		1	0	3	домашнее задание
5.	Тема 5. Современные симметричные криптосистемы (блочные системы шифрования).	4		2	0	3	домашнее задание
6.	Тема 6. Поточные шифры.	4		1	0	3	домашнее задание
7.	Тема 7. Асимметричные криптосистемы (системы шифрования с открытым ключом).	4		2	0	3	контрольная работа

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
8.	Тема 8. Идентификация и проверка подлинности.	4		1	0	3	домашнее задание
9.	Тема 9. Аутентификация сообщений и функции хэширования.	4		2	0	3	домашнее задание
10.	Тема 10. Цифровая подпись.	4		2	0	3	домашнее задание
11.	Тема 11. Управление криптографическими ключами.	4		1	0	3	контрольная работа
12.	Тема 12. Протоколы распределения ключей.	4		1	0	2	домашнее задание
13.	Тема 13. Практические аспекты применения криптосистем.	4		1	0	2	домашнее задание
	Тема . Итоговая форма контроля	4		0	0	0	экзамен
	Итого			17	0	34	

## 4.2 Содержание дисциплины

### Тема 1. Введение

#### **лекционное занятие (1 часа(ов)):**

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.

### Тема 2. Информационная безопасность компьютерных систем.

#### **лекционное занятие (1 часа(ов)):**

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.

#### **лабораторная работа (3 часа(ов)):**

Примеры реализации простейших шифров.

### Тема 3. Формальные модели криптосистем.

#### **лекционное занятие (1 часа(ов)):**

Надежность шифров. Теоретическая и практическая стойкость шифров. Классификация шифров по различным признакам.

#### **лабораторная работа (3 часа(ов)):**

Примеры оценки сложности построения и взлома шифров.

### Тема 4. Классические симметричные криптосистемы.

#### **лекционное занятие (1 часа(ов)):**

Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр.

**лабораторная работа (3 часа(ов)):**

Примеры программной реализации классических симметричных шифров.

**Тема 5. Современные симметричные криптосистемы (блочные системы шифрования).**

**лекционное занятие (2 часа(ов)):**

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.

**лабораторная работа (3 часа(ов)):**

Примеры программной реализации блочных шифров.

**Тема 6. Поточные шифры.**

**лекционное занятие (1 часа(ов)):**

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

**лабораторная работа (3 часа(ов)):**

Примеры программной реализации поточных шифров.

**Тема 7. Асимметричные криптосистемы (системы шифрования с открытым ключом).**

**лекционное занятие (2 часа(ов)):**

Принципы построения асимметричных криптосистем. Теоретико-числовой и алгебраический аппарат, используемый при построении асимметричных криптосистем. Криптоалгоритмы RSA и Эль-Гамала; криптография на основе эллиптических кривых над конечными полями.

**лабораторная работа (3 часа(ов)):**

Примеры программной реализации асимметричных шифров.

**Тема 8. Идентификация и проверка подлинности.**

**лекционное занятие (1 часа(ов)):**

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

**лабораторная работа (3 часа(ов)):**

Примеры программной реализации систем идентификации.

**Тема 9. Аутентификация сообщений и функции хэширования.**

**лекционное занятие (2 часа(ов)):**

Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94.

**лабораторная работа (3 часа(ов)):**

Примеры программной реализации хэширования.

**Тема 10. Цифровая подпись.**

**лекционное занятие (2 часа(ов)):**

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.

**лабораторная работа (3 часа(ов)):**

Примеры программной реализации электронной цифровой подписи.

## Тема 11. Управление криптографическими ключами.

### лекционное занятие (1 часа(ов)):

Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей.

### лабораторная работа (3 часа(ов)):

Примеры программной реализации генерации ключей.

## Тема 12. Протоколы распределения ключей.

### лекционное занятие (1 часа(ов)):

Передача ключей с использованием симметричного шифрования. Двусторонние и трехсторонние протоколы. Передача ключей с использованием асимметричных систем шифрования. Протоколы без использования и с использованием цифровой подписи. Протокол Kerberos.

### лабораторная работа (2 часа(ов)):

Примеры программной реализации протоколов распределения ключей.

## Тема 13. Практические аспекты применения криптосистем.

### лекционное занятие (1 часа(ов)):

Требования к криптосистемам. Длина ключа и стойкость. Шифрование и архивирование. Шифрование и кодирование. Стандартизация алгоритмов шифрования.

### лабораторная работа (2 часа(ов)):

Обсуждение требований к криптосистемам.

## 4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Информационная безопасность компьютерных систем.	4		подготовка домашнего задания	3	домашнее задание
3.	Тема 3. Формальные модели криптосистем.	4		подготовка домашнего задания	4	домашнее задание
4.	Тема 4. Классические симметричные криптосистемы.	4		подготовка домашнего задания	4	домашнее задание
5.	Тема 5. Современные симметричные криптосистемы (блочные системы шифрования).	4		подготовка домашнего задания	4	домашнее задание
6.	Тема 6. Поточные шифры.	4		подготовка домашнего задания	4	домашнее задание
7.	Тема 7. Асимметричные криптосистемы (системы шифрования с открытым ключом).	4		подготовка к контрольной работе	10	контрольная работа



N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
8.	Тема 8. Идентификация и проверка подлинности.	4		подготовка домашнего задания	4	домашнее задание
9.	Тема 9. Аутентификация сообщений и функции хэширования.	4		подготовка домашнего задания	4	домашнее задание
10.	Тема 10. Цифровая подпись.	4		подготовка домашнего задания	4	домашнее задание
11.	Тема 11. Управление криптографическими ключами.	4		подготовка к контрольной работе	10	контрольная работа
12.	Тема 12. Протоколы распределения ключей.	4		подготовка домашнего задания	4	домашнее задание
13.	Тема 13. Практические аспекты применения криптосистем.	4		подготовка домашнего задания	2	домашнее задание
	Итого				57	

## 5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекций, лабораторно-практических занятий, а также самостоятельной работы студентов.

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.

Изучение курса подразумевает овладение теоретическим материалом и получение практических навыков для более глубокого понимания разделов дисциплины "Введение в криптографию" на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени.

## 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов



## **Тема 1. Введение**

## **Тема 2. Информационная безопасность компьютерных систем.**

домашнее задание , примерные вопросы:

Программная реализация простейших шифров.

## **Тема 3. Формальные модели криптосистем.**

домашнее задание , примерные вопросы:

Оценить сложность построения и взлома шифров.

## **Тема 4. Классические симметричные криптосистемы.**

домашнее задание , примерные вопросы:

Программная реализация классических симметричных шифров.

## **Тема 5. Современные симметричные криптосистемы (блочные системы шифрования).**

домашнее задание , примерные вопросы:

Программная реализация современных симметричных шифров.

## **Тема 6. Поточные шифры.**

домашнее задание , примерные вопросы:

Программная реализация поточных шифров.

## **Тема 7. Асимметричные криптосистемы (системы шифрования с открытым ключом).**

контрольная работа , примерные вопросы:

Программная реализация одного из следующих шифров: - Crypton V1.0 - E2 - IDEA - LOKI 91 и 97 - Noekeon - Magenta - Rijndael - SAFER или SAFER++ - Skipjack - ГОСТ 28147-89 - Anubis - Blowfish - Serpent - Camellia - CAST-128 - DFCv2 - Khazad Square

## **Тема 8. Идентификация и проверка подлинности.**

домашнее задание , примерные вопросы:

Программная реализация системы аутентификации и авторизации.

## **Тема 9. Аутентификация сообщений и функции хэширования.**

домашнее задание , примерные вопросы:

Программная реализация хэширования

## **Тема 10. Цифровая подпись.**

домашнее задание , примерные вопросы:

Программная реализация системы цифровой подписи.

## **Тема 11. Управление криптографическими ключами.**

контрольная работа , примерные вопросы:

Программная реализация хэширования и механизма электронной цифровой подписи на основании следующих алгоритмов: - Crypton V1.0 - E2 - IDEA - LOKI 91 и 97 - Noekeon - Magenta - Rijndael - SAFER или SAFER++ - Skipjack - ГОСТ 28147-89 - Anubis - Blowfish - Serpent - Camellia - CAST-128 - DFCv2 - Khazad Square

## **Тема 12. Протоколы распределения ключей.**

домашнее задание , примерные вопросы:

Программная реализация протоколов распределения ключей.

## **Тема 13. Практические аспекты применения криптосистем.**

домашнее задание , примерные вопросы:

Анализ взломостойкости алгоритма от изменение длины ключа.

## **Тема . Итоговая форма контроля**

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение экзамена. Примерные вопросы для экзамена - Приложение10.

**ВОПРОСЫ К ЭКЗАМЕНУ**

## 1. Информационная безопасность компьютерных систем.

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.

## 2. Формальные модели криптосистем.

Надежность шифров. Теоретическая и практическая стойкость шифров. Классификация шифров по различным признакам.

## 3. Классические симметрические криптосистемы.

Шифры перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифры гаммирования. Абсолютно стойкий шифр.

## 4. Современные симметричные криптосистемы (блочные системы шифрования).

Принципы построения блочных шифров. Принцип итерирования. Схема Фейстеля. Стандарты блочного шифрования. Федеральный стандарт США DES. Российский стандарт ГОСТ-28147-89. Известные блочные шифры: IDEA, RC-5, Blowfish, CAST-128. 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. Атаки на блочные шифры.

## 5. Поточные шифры.

Принципы построения поточных шифров. Примеры поточных криптосистем. Генераторы псевдослучайных чисел.

## 6. 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-Гамала. Криптография на основе эллиптических кривых над конечными полями.

## 7. Идентификация и проверка подлинности.

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

## 8. Аутентификация сообщений и функции хэширования.

Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функции ГОСТ Р.34.11-94.

## 9. Цифровая подпись.

Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы создания электронной цифровой подписи. Стандарты цифровой подписи. Российский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функциональными возможностями: схема слепой подписи, схема неоспоримой подписи.

## 10. Управление криптографическими ключами.

Генерация ключей. Хранение ключей. Концепция и иерархия ключей. Распределение ключей.

## 11. Протоколы распределения ключей.

Передача ключей с использованием симметричного шифрования. Двусторонние и трехсторонние протоколы. Передача ключей с использованием асимметричных систем шифрования. Протоколы без использования и с использованием цифровой подписи. Протокол Kerberos.

## 12. Практические аспекты применения криптосистем.

Требования к криптосистемам. Длина ключа и стойкость. Шифрование и архивирование. Шифрование и кодирование. Стандартизация алгоритмов шифрования.

### 7.1. Основная литература:

1. Громкович, Ю. Теоретическая информатика: Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию. - Издание 3 - е. - СПб: БХВ - Петербург, 2010. - 336 с.
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.  
<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.  
<http://znanium.com/bookread.php?book=405000>
4. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: <http://kpfu.ru/docs/F366166681/mzi.pdf>

### 7.2. Дополнительная литература:

1. Применко Э. А. Алгебраические основы криптографии: М.: URSS: [ЛИБРОКОМ, 2013]..283 с
2. Латыпов, Р. Х. Математические основы кодирования информации и криптографии: учеб. Пособие./ Казан. гос. ун - т. - Казань: [КГУ], 2005. - 59 с.
3. Земор, Жиль. Курс криптографии / Жиль Земор; пер. с фр. В.В. Шуликовской. - М.; Ижевск: Ин - т компьютер. исслед.: Регуляр. и хаотич. динамика, 2006. - 255 с
4. Введение в теоретико-числовые методы криптографии : учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090101 "Криптография" / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин .? Санкт-Петербург [и др.] : Лань, 2011 .? 394 с.

### 7.3. Интернет-ресурсы:

- 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://algotlist.manual.ru/>  
Компьютерная энциклопедия - <http://www.computer-encyclopedia.ru>

## 8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Введение в криптографию" предполагает использование следующего материально-технического обеспечения:

Лекционные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером), а так же в специализированных компьютерных кабинетах.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010400.62 "Прикладная математика и информатика" и профилю подготовки Математическое и программное обеспечение вычислительных машин и сетей .

Автор(ы):

Кугураков В.С. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.

Рецензент(ы):

Гайнутдинова А.Ф. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.