

МИНОБРНАУКИ РОССИИ  
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ  
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ  
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)



РАБОЧАЯ ПРОГРАММА  
дисциплины  
«ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ»  
для подготовки аспирантов по направлению  
10.06.01 – «Информационная безопасность»  
по направленности  
«Методы и системы защиты информации,  
информационная безопасность»

Санкт-Петербург

2016

## **СТРУКТУРА ДИСЦИПЛИНЫ**

№№ учебных планов:	6910190, 5910190, 4910190
Обеспечивающий факультет:	ФКТИ
Обеспечивающая кафедра:	Информационная безопасность
Общая трудоемкость (ЗЕТ)	3
Курс	1
Семестр	2

### **Виды занятий**

Лекции (академ. часов)	36
Практические занятия (академ. часов)	0
Лабораторные занятия (академ. часов)	0
Все аудиторные (контактные) занятия (академ. часов)	36
Самостоятельная работа (академ. часов)	72
Всего (академ. часов)	108

### **Вид промежуточной аттестации**

Дифференцированный зачет (семестр)	2
------------------------------------	---

Рабочая программа рассмотрена и одобрена на заседании кафедры «Информационная безопасность» 16 июня 2016, протокол № 4.

Рабочая программа рассмотрена и одобрена учебно-методической комиссией факультета компьютерных технологий и информатики 22 сентября 2016 протокол № 7.

**АННОТАЦИЯ ДИСЦИПЛИНЫ**  
**«ТЕОРЕТИЧЕСКИЕ ОСНОВЫ**  
**КРИПТОГРАФИИ»**

Дисциплина «Теоретические основы криптографии» является одной из дисциплин цикла обучения аспирантов и докторантов по выбору и обеспечивает приобретение знаний, умений и навыков в области криптографической защиты информации в соответствии с государственным образовательным стандартом.

**SUBJECT SUMMARY**

**«APPLIED CRYPTOGRAPHY THEORETICAL BASIS AND ITEMS»**

"Cryptography theoretical basis" is one of a graduate students training cycle disciplines at a choice. It provides acquisition of knowledge, skills in the field of technical information security according to the state educational standard.

## **ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ**

1. Изучение теоретических основ криптографических протоколов: терминологии, стандартов, типовых протоколов и требований к ним, а также знание средств анализа безопасности протоколов.
2. Формирование умения использования криптографических протоколов для решения задач обеспечения информационной безопасности компьютерных и телекоммуникационных систем, умения применять математические методы описания и исследования крипtosистем.
3. Освоение теоретических основ решения задач аутентификации пользователей и информации, распределения ключей, получение навыка обеспечения неотрекаемости и анонимности в современных информационных технологиях электронного документооборота и управления.

Перечень компетенций, в формировании которых участвует дисциплина, приведен в матрице компетенций, прилагаемой к ООП.

Настоящая программа составлена на основе «Программы кандидатских экзаменов по истории и философии науки, иностранному языку и специальным дисциплинам», утвержденной приказом Минобрнауки России от 8 октября 2007 г. № 274 (зарегистрирован Минюстом России 19 октября 2007 г., регистрационный № 10363).

## **МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП**

Дисциплина «Теоретические основы криптографии» относится к вариативной части ООП. Дисциплина изучается на основе ранее освоенной дисциплины учебного плана:

1. Проектирование целеустремленных защищенных технических систем и обеспечивает подготовку выпускной научной квалификационной работы (диссертации).

## **СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

### **Введение ( 8 академ. часа)**

Место современной криптографии в проблематике компьютерной безопасности. Три основные задачи, решаемые криптографией: секретность, аутентификация, анонимность. Основные типы крипtosистем. Теоретическая и практическая стойкость криптографических алгоритмов. Доказуемая стойкость шифров с открытым ключом.

### **Тема 1. Теоретико-числовые основы криптографии с открытым ключом(10 академ. часа).**

Элементарная теория чисел и вычислительные алгоритмы, используемые для построения и анализа криптографических алгоритмов (нахождение обратных значений в кольцах вычетов, быстрый алгоритм возведения в многоразрядную степень, извлечение квадратных корней и корней произвольных степеней).

### **Тема 2. Алгоритмы решения вычислительно сложных задач (10 академ. часа)**

Алгоритмы факторизации трудно разложимых целых чисел. Случайные функции и случайные подстановки.. Алгоритм Флойда для нахождения значения в цикле случайной функции. Алгоритмы дискретного логарифмирования в циклической группе и в конечном поле: алгоритм больших и малых шагов, алгоритм Полларда, метод вычисления индексов.

### **Тема 3. Строгая аутентификация абонентов информационно-телекоммуникационных систем (10 академ. часа)**

Протоколы с нулевым разглашением секрета. Толкование понятия нулевое разглашение секрета. Двухшаговые протоколы с нулевым разглашением на основе 1) алгоритмов открытого шифрования, 2) схем открытого согласования секретного ключа, 3) процесса последовательного возведения в квадрат. Протокол послания в будущее. Трехшаговые протоколы с нулевым разглашением секрета и их преобразование в протоколы электронной цифровой подписи. Вы-

вод алгоритма цифровой подписи Шнорра. Доказуемая стойкость алгоритма подписи Шнорра. Доказательство стойкости крипtosхемы Рабина.

Способ открытого шифрования как генерации квадратных и кубичных сравнений. Потайные каналы, связанные с протоколами цифровой подписи.

#### **Тема 4. Протоколы мультиподписи ( 10 академ. часа )**

Групповая и коллективная подпись. Использование крипtosхемы RSA для построения протоколов мультиподписи. Использование алгоритмов цифровой подписи на основе вычислительной трудности задачи дискретного логарифмирования для построения протоколов мультиподписи. Утверждаемая групповая подпись. Алгоритмы защитного контрольного суммирования. Выбор алгоритма в зависимости от решаемой задачи обеспечения возможности контроля целостности информации. Ключевые и бесключевые хэш-функции. Особенности применения хэш-функций в протоколах цифровой подписи. Протоколы слепой цифровой подписи.

#### **Тема 5. Атаки с принуждением ( 8 академ. часа)**

Понятие атаки с принуждением. Модели принудительных атак. Проблема защиты от принудительных атак. Понятие отрицаемого (оспоримого) шифрования. Типы протоколов отрицаемого шифрования – с открытым ключом, с разделяемым ключом, бесключевые. Псеводвероятностное шифрование как способ эффективной реализации протоколов отрицаемого шифрования.

#### **Тема 6. Эллиптическая криптография (8 академ. часа)**

Аппарат эллиптических кривых и его использование для построения крипtosхем с открытым ключом. Экспоненциальная стойкость крипtosхем, основанных на эллиптических кривых. Построение крипtosхем на основе двух трудных задач.

#### **Тема 7. Блочные шифры и режимы их использования ( 26 академ. часов)**

Шифры на основе управляемых перестановочных и подстановочно-перестановочных сетей. Основные типы архитектур аппаратной реализации блочных шифров в заказных и программируемых СБИС. Режим исправления ошибок. Режим вероятностного шифрования. Режим псевдовероятностного шифрования. Быстрые программные шифры. Коммутативные шифры и бесключевое шифрование. Вероятностные шифры с секретным и открытым ключом. Проблема защиты информации в условиях ограниченности ключевого материала. Протоколы стойкого шифрования с ключом малого размера. Описание операций блочного шифрования с использованием булевых функций. Линейность и нелинейность операций, дифференциальные характеристики операций.

**Тема 8. Российские криптографические стандарты (10 академ. часа)**

ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.

**Заключение ( 8 академ. часа )**

Перспективные направления развития прикладной криптографии

# **УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

## **Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

<b>№</b>	<b>Название, библиографическое описание</b>	<b>Семестр</b>	<b>К-во экз. в библ. (на каф.)</b>
<b>Основная литература</b>			
1	Дернова Е.С., Молдовян Д.Н., Молдовян Н.А. Криптографические протоколы. - СПб., Изд. СПбГЭТУ, 2010. - 100 с.	2	42 (0)
2	Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. – СПб.: БХВ – Петербург, 2010. – 304 с.	2	26 (0)
3	Дернова Е.С., Молдовян Н.А., Молдовян П.А. Элементы теоретических основ криптографии. - СПб., Изд. СПбГЭТУ, 2009. – 92 с.	2	78 (0)
4	Молдовян А.А., Молдовян Н.А., Гуд Н.Д., Изотов Б.В. Криптография. Скоростные шифры. – СПб.: БХВ – Петербург, 2002. – 496 с.	2	25 (0)
5	Столлингс В. Криптография и защита сетей: принципы и практика., 2-е изд.: Пер. с англ. – Изд. Дом «Вильямс», 2001. – 672с.	2	42 (2)
<b>Дополнительная литература</b>			
1	Молдовян Н.А., Молдовян А.А. Введение в криптоисистемы с открытым ключом. – СПб.: БХВ – Петербург, 2005. – 286 с.	2	3(0)
2	Молдовян Н.А. Практикум по криптоисистемам с открытым ключом. – СПб.: БХВ – Петербург, 2007. – 298 с.	2	8(0)

3	Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб., Лань, 2001. – 218 с.	2	19(0)
4	Еремеев М.А., Молдовян Н.А., Молдовян А.А. Криптография. От примитивов к синтезу алгоритмов. – Спб.: БХВ – Петербург, 2004г. - 448с.	2	2(0)
5	Иванов М.А. Криптографические методы защиты информации. – М.: Кудиц-Образ. 2001г. - 368с.	2	8(0)
6	Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2002, -816с.	2	2(0)

Зав. отделом учебной литературы *Киселев* Т.В. Киселева  
10. 11. 17-

Информационные технологии (операционные системы, программное обеспечение общего и специализированного назначения, а также информационные справочные системы) и материально-техническая база, используемые при осуществлении образовательного процесса по дисциплине, соответствуют требованиям федерального государственного образовательного стандарта высшего образования.

Описание информационных технологий и материально-технической базы приведено в УМКД дисциплины.

Конкретные формы и процедуры текущего контроля знаний и промежуточной аттестации, а также методические указания для обучающихся по самостоятельной работе при освоении дисциплин (содержащиеся в ООП) доводятся до сведения обучающихся на первом занятии.

## ЛИСТ СОГЛАСОВАНИЯ

**Разработчик**

д.т.н., проф.



Молдовян Н.А.

**Рецензент**

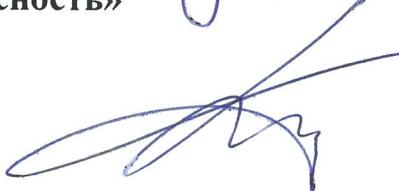
д.т.н., проф.



Воробьев В.И

**Зав. каф. «Информационная безопасность»**

к.т.н., доц.



Воробьев Е.Г.

**Декан ФКТИ**

д.т.н., проф.



Куприянов М.С.

**Согласовано**

**Председатель УМК ФКТИ**

к.т.н., доц.



Михалков В.А.

**Начальник МО**

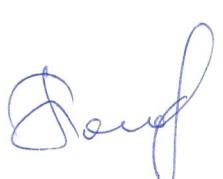
д.т.н., проф.



Грязнов А.Ю.

**Заведующий ОДА**

к.т.н., доцент



Погодин А.А.

## ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№	Дата	Изменение	Дата заседания УМК, № прот-ла	Автор	Нач. МО
1					