

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В.ЛОМОНОСОВА»  
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ



УТВЕРЖДАЮ

Декан факультета ВМК МГУ,

Академик

«14» сентября 2022 г.

*/И.А. Соколов/*

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

### Симметричные криптосистемы Symmetric key cryptosystems

Программа (программы) подготовки научных и научно-педагогических кадров в аспирантуре

---

Рабочая программа дисциплины разработана в соответствии с Приказом Ректора МГУ №1216 от 24 ноября 2021 года «Об утверждении Требований к основным программам подготовки научных и научно-педагогических кадров в аспирантуре, самостоятельно устанавливаемых Московским государственным университетом имени М.В. Ломоносова»

1. Краткая аннотация:

### **Название дисциплины** Симметричные криптосистемы

**Цель** изучения дисциплины – Данный курс посвящен некоторым важным вопросам теории симметричных криптосистем, которые важны как в теоретическом аспекте, так и для приложений. Именно, курс посвящен синтезу и анализу важнейших криптографических свойств криптопримитивов, используемых в современных системах шифрования, ориентированных в первую очередь на реализацию в виде программ на современной компьютерной технике, т.е. на стандартных процессорах и ПЛИС. Эти криптопримитивы описываются на языке детерминированных функций, т.е. функций, реализуемых синхронными автоматами. Класс всех детерминированных функции над конечным алфавитом из  $r$  символов совпадает, как известно, с классом всех функций, удовлетворяющих условию Липшица с константой 1 в  $p$ -адической метрике, что позволяет применять к изучению криптографических свойств соответствующих криптопримитивов методы  $p$ -адического анализа и неархимедовой динамики, что и составляет основное содержание курса. Поскольку  $p$ -адический анализ не относится к числу стандартных курсов, изучаемых даже на математических специальностях университетов, то в начальной части курса «Симметричные криптосистемы» излагаются основы  $p$ -адического анализа и  $p$ -адической эргодической теории, в особенности для случая  $p=2$  как наиболее важного для приложений к алгоритмам шифрования, реализуемым на современной компьютерной технике. Курс нацелен в первую очередь на приложения к анализу и синтезу потоковых шифров, хотя блочные шифры затрагиваются тоже.

2. Уровень высшего образования – аспирантура

3. Научная специальность 1.2.1., 1.2.2., 1.2.3., 1.1.2., 1.1.4., 1.1.5., 1.1.6., 2.3.5., 2.3.6.,  
отрасль науки: Физико-математические науки,

Научная специальность 1.2.2., отрасль науки: Технические наук

4. Место дисциплины (модуля) в структуре программы аспирантуры- элективный курс.

Объем дисциплины составляет 2 зачетные единицы, всего 72 часа. Из них 40 часов составляет контактная работа с преподавателем – 32 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 4 часа мероприятий текущего контроля успеваемости, 2 часа групповых консультаций, 2 часа мероприятий промежуточной аттестации, 32 часа составляет самостоятельная работа аспиранта.

6. Входные требования для освоения дисциплины (модуля), предварительные условия.

На предыдущих уровнях высшего образования должны быть освоены общие курсы:

1. Математический анализ

2. Функциональный анализ

3. Дискретная математика

4. Алгебра

7. Содержание дисциплины (модуля), структурированное по темам

Наименование и краткое содержание разделов и тем дисциплины (модуля),  форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы						Самостоятельная работа обучающегося, часы		
		из них						из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости (коллоквиумы, практические контрольные занятия и др)*	Всего	Выполнение домашних заданий	Подготовка рефератов и т.п..	Всего
<b>Тема 1. Основные понятия теории симметричных криптосистем</b> Шифры замены и перестановки. Блочные и потоковые шифры. Понятие о стойкости и методах дешифрования симметричных шифров. Принцип Керкгоффса. Совершенные по Шеннону шифры. Шифры гаммирования и колонной замены. Совершенные шифры, не размножающие ошибку: теорема Котельникова. Эндоморфные шифры. Таблица зашифрования эндоморфного шифра как латинский квадрат. Имитостойкость, вероятность навязывания. Применение ортогональных латинских квадратов для	13	7	-	-	-		7	6	-	6

уменьшения вероятности навязывания.										
<p><b>Тема 2. Криптопримитивы программно-реализуемых потоковых шифров.</b></p> <p>Основные узлы и блоки современных программно-реализуемых потоковых шифров. Генераторы исходных последовательностей, функции усложнения, фильтры, мультиперестановки. Основные требования к узлам и блокам потоковых шифров. Равновероятность, биективность, транзитивность. Т-функции как структурные элементы криптопримитивов.</p>	10	2	-	-	-	-	2	2	6	8
<p><b>Тема 3. Математическая теория Т-функций.</b></p> <p>Т-функции как детерминированные функции на бесконечных бинарных словах. Бесконечные бинарные слова как 2-адические целые числа. Т-функции как 1-липшицевы функции на кольце целых 2-адических чисел. Элементы 2-адического анализа и 2-адической эргодической теории. Равновероятность, биективность, транзитивность Т-функций как сохранение меры и эргодичность.</p>	15	8	-	-	-	1	9	6	-	6
<p><b>Тема 4. Криптографические свойства Т-функций.</b></p> <p>Критерии и достаточные условия равновероятности/транзитивности (сохранения меры/эргодичности) для Т-функций. Координатные последовательности, линейная сложность, 2-адическая сложность, периоды, зависимости. Статистические свойства Т-функций. Закон 0 или 1 для Т-функций.</p>	9	4	-	-	-	1	5	4	-	4

<b>Тема 5. Методы построения алгоритмов потокового шифрования на основе T-функций.</b>  Построение латинских квадратов и пар ортогональных латинских квадратов на основе T-функций. Сплетения детерминированных функций и генераторы с динамически изменяющимся законом рекурсии. Построение потоковых шифров как сплетений T-функций.	23	12	-	2	-	1	15	8	-	8	
<b>6. Промежуточная аттестация – устный экзамен</b>	2	2									
<b>Итого</b>	72	40					32				

#### 8. Образовательные технологии.

При проведении лекционных занятий предусматривается использование информационных технологий, включающих пакеты математических программ MATLAB, MATHEMATICA, Grapher, а также специализированной программы Vorg и др. Использование информационных технологий осуществляется, в частности, в процессе реализации активных и интерактивных форм проведения занятий. При чтении лекций в качестве материала, иллюстрирующего возможности математического моделирования в различных ситуациях, активно используются примеры из практики в процессе исследований в предметной области. Информационные и интерактивные технологии используются при обсуждении проблемных и неоднозначных вопросов, требующих выработки решения в ситуации неопределенности.

#### 9. Учебно-методические материалы для самостоятельной работы по дисциплине (модулю):

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации.

Литература для самостоятельной работы студентов в соответствии с тематическим планом .

### **Тема 1 «Основные понятия теории симметричных криптосистем»**

- ✓ Зубов А.Ю. Совершенные шифры. – М.: Гелиос АРВ, 2003
- ✓ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
- ✓ Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Р, 2002

### **Тема 2 «Криптопримитивы программно-реализуемых потоковых шифров»**

- ✓ Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003
- ✓ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
- ✓ Анашин В.С. Неархимедов анализ, Т-функции и криптография.- М.: 2007 (электронная версия <http://istina.msu.ru/courses/7102110/>).

### **Тема 3 «Элементы математической теории Т-функций»**

- ✓ Анашин В.С. Неархимедов анализ, Т-функции и криптография.- М.: 2007 (электронная версия <http://istina.msu.ru/courses/7102110/>).
- ✓ Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011 (электронная версия доступна на сайте <http://istina.msu.ru/courses/7102110/>).
- ✓ Анашин В.С. Введение в прикладной p-адический анализ. - М.: 2008 (электронная версия <http://istina.msu.ru/courses/7102110/>).
- ✓ Коблиц Н. p-адические числа, p-адический анализ и дзета-функции. - М.: Мир, 1982
- ✓ Хренников А.Ю. Неархимедов анализ и его приложения. – М.: Физматлит, 2003
- ✓ Каток С.Б. p-адический анализ в сравнении с вещественным. –М.: МЦНМО, 2004
- ✓ Кнут Д. Искусство программирования для ЭВМ. т. 2. Получисленные алгоритмы. - Москва–СПб–Киев: Вильямс, 2000
- ✓ Anashin V., Khrennikov A. Applied Algebraic Dynamics, volume 49 of deGruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y., 2009.
- ✓ Anashin V. The p-adic ergodic theory and applications (электронная версия [https://www.researchgate.net/publication/269571423\\_The\\_p-adic\\_ergodic\\_theory\\_and\\_applications](https://www.researchgate.net/publication/269571423_The_p-adic_ergodic_theory_and_applications))

### **Тема 4 «Криптографические свойства Т-функций»**

- ✓ Анашин В.С. Неархимедов анализ, Т-функции и криптография.- М.: 2007 (электронная версия <http://istina.msu.ru/courses/7102110/>).
- ✓ Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011 (электронная версия доступна на сайте <http://istina.msu.ru/courses/7102110/>).

- ✓ Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003
- ✓ Anashin V., Khrennikov A. Applied Algebraic Dynamics, volume 49 of deGruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y., 2009.
- ✓ Anashin V. The p-adic ergodic theory and applications (электронная версия [https://www.researchgate.net/publication/269571423\\_The\\_p-adic\\_ergodic\\_theory\\_and\\_applications](https://www.researchgate.net/publication/269571423_The_p-adic_ergodic_theory_and_applications))

#### **Тема 5 «Методы построения алгоритмов потокового шифрования на основе T-функций»**

- ✓ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
- ✓ Анашин В.С. Неархимедов анализ, T-функции и криптография.- М.: 2007 (электронная версия <http://istina.msu.ru/courses/7102110/>).
- ✓ Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011 (электронная версия доступна на сайте <http://istina.msu.ru/courses/7102110/>).
- ✓ Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003
- ✓ Anashin V., Khrennikov A. Applied Algebraic Dynamics, volume 49 of deGruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y., 2009.

#### 10. Ресурсное обеспечение:

- Перечень основной и вспомогательной учебной литературы ко всему курсу

#### **Основная литература:**

1. Зубов А.Ю. Совершенные шифры. – М.: Гелиос АРВ, 2003
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
3. Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Р, 2002
4. Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003
5. Анашин В.С. Неархимедов анализ, T-функции и криптография.- М.: 2007 (электронная версия <http://istina.msu.ru/courses/7102110/>).
6. Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011 (электронная версия доступна на сайте <http://istina.msu.ru/courses/7102110/>).
7. Анашин В.С. Введение в прикладной p-адический анализ. - М.: 2008 (электронная версия <http://istina.msu.ru/courses/7102110/>).

#### **Дополнительная литература:**



1. Коблиц Н.  $p$ -адические числа,  $p$ -адический анализ и дзета-функции. - М.: Мир, 1982.
2. Хренников А.Ю.Неархимедов анализ и его приложения. – М.: Физматлит, 2003
3. Каток С.Б.  $p$ -адический анализ в сравнении с вещественным. –М.: МЦНМО, 2004
4. Кнут Д. Искусство программирования для ЭВМ. т. 2. Получисленные алгоритмы. - Москва–СПб–Киев: Вильямс, 2000
5. Anashin V., Khrennikov A. Applied Algebraic Dynamics, volume 49 of deGruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y.,2009.

- Перечень используемых информационных технологий, используемых при осуществлении образовательного процесса, включая программное обеспечение, информационные справочные системы (при необходимости):

<http://elibrary.ru>

[www.scopus.com](http://www.scopus.com)

<http://istina.msu.ru/courses/7102110/>

[https://www.researchgate.net/profile/Vladimir\\_Anashin](https://www.researchgate.net/profile/Vladimir_Anashin)

- Описание материально-технической базы.  
Занятия проводятся в аудитории, оснащенной мультимедийным экраном, доской, проектором

11. Язык преподавания – русский

12. Преподаватели:

Степень, должность ФИО., e-mail, тел.: д.ф.-м.н., профессор, Анашин Владимир Сергеевич, [Vladimir.anashin@cs.msu.ru](mailto:Vladimir.anashin@cs.msu.ru),  
+7(495)930-43-86

**Фонды оценочных средств, необходимые для оценки результатов обучения**

**Образцы домашних заданий:**

1. Решение конкретных задач на вычисления в кольце  $p$ -адических чисел. Например, построение обратного, нахождение производной детерминированной функции и т.п.
2. Решение конкретных примеров на проверку условий сохранения меры детерминированной функцией и построение фильтрующих преобразований, латинских квадратов и мультиперестановок на основе таких функций.
3. Решение конкретных примеров на проверку эргодичности детерминированной функции и построения псевдослучайных генераторов максимального периода с помощью таких функций.
4. Кроме того, в качестве домашнего задания подразумевается изучение рекомендуемой литературы.

Вопросы для промежуточной аттестации – зачета (экзамена):

1. Общее определение шифра, симметричного шифра и асимметричного шифра. Типы симметричных шифров. Блочные и потоковые шифры. Шифры гаммирования и колонной замены. Совершенные шифры. Примеры совершенных шифров.
2. Совершенные шифры, не размножающие ошибку. Эндоморфные шифры. Таблица зашифрования эндоморфного шифра. Имитостойкость эндоморфного шифра и методы ее обеспечения.
3. Основные узлы и блоки современных программно-реализуемых потоковых шифров. Генераторы исходных последовательностей, функции усложнения, фильтры, мультиперестановки. Основные требования к узлам и блокам потоковых шифров. Генератор гаммы наложения как автомат. Периодичность гаммы. Равновероятность, биективность, транзитивность детерминированных функций.
4. Детерминированные функции бинарных автоматов как 1-липпшицевы функции пространства целых 2-адических чисел. Необходимое и достаточное условие детерминированности 2-адической функции.
5. Определение Т-функции. Базисные команды процессора, являющиеся Т-функциями. Тождества.
6. Кольцо целых 2-адических чисел. Каноническая форма представления целого 2-адического числа. 2-адическая метрика и ее свойства. Шары и треугольники в пространстве целых 2-адических чисел.
7. Арифметика кольца целых 2-адических чисел. Обратимые элементы. Рациональные числа в кольце целых 2-адических чисел.
8. Предел и сходимость в кольце целых 2-адических чисел. Критерий сходимости рядов в этом кольце.
9. Непрерывные функции на кольце целых 2-адических чисел. Непрерывность Т-функций.
10. Представление Т-функций в координатной форме, в виде ряда Малера, в виде ряда ван дер Пута.
11. Дифференцируемые функции на кольце целых 2-адических чисел. Производные команд процессора.
12. Вероятностная мера на кольце целых 2-адических чисел. Функции, сохраняющие меру и эргодические функции. Изометричность сохраняющих меру Т-функций.
13. Основная эргодическая теорема для Т-функций. Сохранение меры и биективность (равновероятность), эргодичность и транзитивность.
14. Критерий сохранения меры/эргодичности для Т-функции в терминах координатных функций.
15. Критерий сохранения меры/эргодичности для Т-функции в терминах рядов Малера и представление сохраняющих меру/эргодических Т-функций.
16. Критерий сохранения меры/эргодичности для Т-функции в терминах рядов ван дер Пута.

17. Критерий и достаточные условия сохранения меры для T-функции нескольких переменных.
18. Построение латинских квадратов и пар взаимно-ортогональных латинских квадратов с помощью как сохраняющих меру T-функций.
19. Сохранение меры/эргодичность дифференцируемых T-функций.
20. Строение координатных последовательностей эргодических T-функций. Линейная сложность (над полем из 2-х элементов) координатной последовательности эргодической T-функции.
21. Линейная сложность последовательности, порожденной эргодической T-функцией, над кольцом целых 2-адических чисел.
22. Графики T-функций на действительной плоскости. Закон 0 или 1 для T-функций.
23. Сплетения детерминированных функций. Теорема о строении последовательности, порожденной сплетением детерминированной функции и эргодической T-функции.
24. Сплетения детерминированных функций. Теорема о распределении n-грамм в последовательности, порожденной сплетением детерминированной функции и эргодической T-функции.
25. Построение генераторов с динамически изменяющимся законом рекурсии, имеющих максимально возможный период по каждой координатной последовательности, с помощью сплетений.
26. Линейная сложность координатных последовательностей генераторов с изменяющимся законом рекурсии, построенных с помощью сплетений.

### **Методические материалы для проведения процедур оценивания результатов обучения**

Зачет (экзамен) проходит по билетам, включающем 2 вопроса (первый вопрос теоретический, второй вопрос – задача). Уровень знаний аспиранта по каждому вопросу на «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». В случае если на все вопросы был дан ответ, оцененный не ниже чем «удовлетворительно», аспирант получает общую оценку «зачтено».