

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины
Теория псевдослучайных генераторов

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

1. Цели освоения дисциплины

Целью освоения дисциплины «Теория псевдослучайных генераторов» является приобретение обучающимися теоретических знаний в области сложностной криптографии и практических навыков анализа криптографических примитивов с помощью математического аппарата сложностной криптографии.

Дисциплина обеспечивает приобретение передовых знаний в одной из наиболее динамично развивающихся областей современной криптографии.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к базовой части образовательной программы и является дисциплиной специализации.

Для освоения данной дисциплины обучающиеся должны владеть основными понятиями теории алгоритмов, математическим аппаратом теории вероятностей и математической статистики, знать основные методы криптографической защиты информации.

Для успешного освоения дисциплины «Теория псевдослучайных генераторов» ей должны предшествовать следующие дисциплины:

- «Математическая логика и теория алгоритмов»;
- «Теория алгоритмов»;
- «Теория вероятностей и математическая статистика»;
- «Методы и средства криптографической защиты информации»;
- «Криптографические протоколы».

Полученные в курсе «Теория псевдослучайных генераторов» знания необходимы для изучения дисциплин «Математические методы защиты банковской информации» и «Информационная безопасность электронного бизнеса», «Защита программ и данных».

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
Профессионально-специализированные компетенции	
ПСК-2.4 Обладает способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знать: - основные методы анализа криптографических примитивов с использованием математического аппарата сложностной криптографии. Владеть навыками: - корректного применения математического аппарата сложностной криптографии для анализа криптографических примитивов.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Односторонние функции	8	4	2				4	Задания для самостоятельной работы
2	Семейство односторонних функций. Трудный бит	8	2	2		1		4	Задания для самостоятельной работы
3	Генераторы псевдослучайных чисел	8	4	4				4	Задания для самостоятельной работы
4	Псевдослучайные функции	8	4	4		1		5	Задания для самостоятельной работы
5	Привязка к биту	8	2	4				4	Задания для самостоятельной работы
6	Шифрование с открытым ключом	8	2	2		2		4	Задания для самостоятельной работы
							0,3	6,7	Зачет
	ИТОГО		18	18		4	0,3	31,7	

Содержание разделов дисциплины:

Тема 1. Односторонние функции:

Односторонние в наихудших случаях функции. Сильные и слабые односторонние функции. Вопросы длин входов. Эквивалентность существования сильной и слабой односторонних функций

Тема 2. Семейство односторонних функций. Трудный бит:

Семейство односторонних функций. Универсальная односторонняя функция. Трудный бит

Тема 3. Генераторы псевдослучайных чисел:

Вычислительная неразличимость.

Генераторы псевдослучайных чисел.

Протоколы с секретным ключом

Тема 4. Псевдослучайные функции:

Вычислительная неразличимость полиномиального числа образцов.

Ансамбли функций.

Конструкция ансамбля псевдослучайных функций

Тема 5. Привязка к биту:

Неинтерактивные протоколы.

Интерактивные протоколы

Тема 6. Шифрование с открытым ключом:

Семейство односторонних перестановок с секретом.
Шифрование с открытым ключом

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:
для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.

при проведении практических занятий используется программное обеспечение

- Microsoft Visual Studio.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

- Электронная библиотечная система «Консультант студента»

<https://www.studentlibrary.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511700>
2. Агibalов Г. П. Теория псевдослучайных генераторов: учеб. пособие - Томск: Издательский Дом Томского государственного университета, 2019. <https://www.studentlibrary.ru/ru/book/ISBN9785946218016.html>

б) дополнительная литература

1. Goldreich O. Foundations of Cryptography Basic Tools – Cambridge University Press, Oded Goldreich 2004. https://doc.lagout.org/security/Oded_Goldreich-Foundations_of_Cryptography_Volume_2%2C_Basic_Applications%282009%29.pdf

в) ресурсы сети «Интернет» (при необходимости)

1. Мультимедийные материалы Computer Science клуба (Санкт-Петербург). Курс «Сложностная криптография», 2008, читает доктор физико-математических наук, ведущий научный сотрудник лаборатории математической логики ПОМИ РАН, заместитель заведующего кафедрой МиИТ СПбАУ РАН, Э. А. Гирш: <http://compsciclub.ru/courses/complexitycrypto/2008-spring/?tab=classes>.
2. Мультимедийные материалы Computer Science клуба (Санкт-Петербург). Курс «Сложность вычислений и основы криптографии», 2012, читает доктор физико-математических наук, ведущий научный сотрудник лаборатории математической логики ПОМИ РАН, заместитель заведующего кафедрой МиИТ СПбАУ РАН, Э. А. Гирш: <http://compsciclub.ru/courses/cryptography/2012-spring/?tab=classes>.
3. Мультимедийные материалы Computer Science клуба (Санкт-Петербург). Курс «Сложность вычислений и основы криптографии», 2013, читает кандидат физико-математических наук, старший научный сотрудник лаборатории математической логики ПОМИ РАН, Д. М. Ицыксон: <http://compsciclub.ru/courses/cryptography/2013-spring/?tab=classes>.
4. Мультимедийные материалы Computer Science клуба (Санкт-Петербург). Курс «Теоретико-сложностные основы криптографии», 2016, читает кандидат физико-математических наук, старший научный сотрудник лаборатории математической логики ПОМИ РАН, Д. М. Ицыксон: <http://compsciclub.ru/courses/cryptography-foundations/2016-spring/?tab=classes>.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий, оснащенные средствами вычислительной техники, с установленным программным обеспечением Microsoft Visual Studio;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля;
- помещения для самостоятельной работы;

- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры КБиММОИ, канд. физ.-мат. наук

Д.М. Мурин

**Приложение № 1 к рабочей программе дисциплины
«Теория псевдослучайных генераторов»**

**Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания и иные материалы,
используемые в процессе текущего контроля успеваемости**

Задания для самостоятельной работы

Варианты заданий по теме № 1: «Односторонние функции».

Упражнение 1. Функция называется регулярной, если она принимает значения одинаковой длины на входах одинаковой длины. Докажите, что если существует односторонняя функция, то существует и регулярная односторонняя функция.

Упражнение 2. Функция называется сохраняющей длину, если она принимает значения, длина которых совпадает с длиной входов. Докажите, что если существует односторонняя функция, то существует и односторонняя функция, сохраняющая длину.

Упражнение 3. Постройте функцию, сохраняющую длину на всех длинах входов.

Упражнение 4. Изменится ли понятие «односторонняя функция», если в определении наделить нарушителя возможностью использовать детерминированную полиномиальную машину Тьюринга вместо вероятностной полиномиальной машины Тьюринга?

Упражнение 5. Изменится ли понятие «односторонняя функция», если предположить, что она (функция) является вычислимой за полиномиальное время на вероятностной машине Тьюринга, а не на детерминированной машине Тьюринга?

Упражнение 6. К каким последствиям может привести неравномерное распределение входных строк x на множестве $\{0, 1\}^n$?

Задания по теме № 2: «Семейство односторонних функций. Трудный бит».

Упражнение 1. Докажите, что односторонние функции существуют тогда и только тогда, когда существуют семейства односторонних функций.

Упражнение 2. Сгенерируем k случайных равномерно распределенных битовых строк длины n : s_1, s_2, \dots, s_k . Для каждого $J \subset \{1, 2, \dots, k\}, J \neq \emptyset$ определим строку $r_J = \bigoplus_{i \in J} s_i$. Покажите, что все r_J одинаково распределены и попарно независимы.

Упражнение 4. Изменится ли понятие «семейство односторонних функций», если в определении наделить нарушителя возможностью использовать детерминированную полиномиальную машину Тьюринга вместо вероятностной полиномиальной машины Тьюринга?

Упражнение 5. Изменится ли понятие «семейство односторонних функций», если предположить, что оно (семейство) является вычислимым за полиномиальное время на вероятностной машине Тьюрина, а не на детерминированной машине Тьюринга?

Упражнение 6. Доказать, что если существует односторонняя функция, то существует и неуниверсальная односторонняя функция.

Задания по теме № 3: «Генераторы псевдослучайных чисел».

1. Докажите, что отношение «быть вычислительно неразличимым» рефлексивно, симметрично и транзитивно.

2. Пусть α_n и β_n вычислительно неразличимы, $q(n)$ – полином, $U_{q(n)}$ – случайная величина, определенная и равномерно распределенная на битовых строках длины $q(n)$. Докажите, что $\alpha_n U_{q(n)}$ и $\beta_n U_{q(n)}$ вычислительно неразличимы.
3. Пусть α_n и β_n вычислительно неразличимы, f – полиномиально вычислимая функция. Докажите, что $f(\alpha_n)$ и $f(\beta_n)$ вычислительно неразличимы.

Задания по теме № 4: «Псевдослучайные функции».

1. Существует ли какой-нибудь конкретный тест, из которого следует случайность по всем остальным?
2. Постройте из псевдослучайного генератора $G: B^n \rightarrow B^N$ псевдослучайную функцию $F: n \times \log N \rightarrow \{0,1\}$.

Задания по теме № 5: «Привязка к биту».

1. Зафиксирует простое число p и первообразный корень $g \in Z_p^*$. Рассмотрим следующий протокол привязки к биту b :

Алиса выбирает случайное натуральное число $q \in \{2, \dots, p-2\}$ и вычисляет $y = g^q \bmod p$.

Алиса посылает Бобу y .

Боб выбирает случайное натуральное число $r \in \{2, \dots, p-2\}$ и вычисляет $C(b, r) = y^b g^r$.

Обладает ли данный протокол свойствами вычислительной связанности, безусловной связанности и безусловной секретности?

2. Могут ли одновременно достигаться и безусловная связанность и безусловная секретность?

Задания по теме № 6: «Шифрование с открытым ключом».

1. Доказать, что из существования надежной системы шифрования с открытым ключом следует существование семейства односторонних функций с секретом.
2. Предположим, что противник может использовать только детерминированные машины Тьюринга. Постройте криптосистему, полную в классе криптосистем с таким противником.
3. Будет ли существование семейства односторонних перестановок эквивалентно существованию одной односторонней перестановки?
4. Докажите, что если существует протокол с открытым ключом для сообщений из 1 бита, то существует протокол с открытым ключом для сообщений произвольной полиномиальной длины.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету

1. «Честные» функции, односторонние в наихудших случаях функций, теорема о существовании односторонних в наихудших случаях функции при $P \neq NP$. Сильные и слабые односторонние функции.
2. Эквивалентность существования сильной и слабой односторонних функций.
3. Семейство односторонних функций. Универсальная односторонняя функция. Теорема об универсальной функции Левина. Трудный бит (определение).
4. Теорема Голдрейха-Левина.
5. Генераторы псевдослучайных чисел. Вычислительная неразличимость. Теорема Голдрейха-Импальяцио-Луби-Хастада.

6. Теорема о $p(n)$ -генераторе. Протоколы с секретным ключом.
7. Неразличимость с полиномиальным количеством образцов. Полиномиально моделируемые распределения. Теорема о неразличимости полиномиального числа образцов.
8. Ансамбли функций. Псевдослучайные ансамбли функций. Эффективно вычислимые ансамбли функций. Конструкция псевдослучайного ансамбля функций.
9. Теорема об эффективно вычислимом ансамбле псевдослучайных функций (описание алгоритма « D »).
10. Теорема об эффективно вычислимом ансамбле псевдослучайных функций (полагаем алгоритм « D » заданным).
11. Протоколы привязки к биту. Неинтерактивные протоколы. Теорема об условном существовании неинтерактивных протоколов привязки к биту.
12. Протоколы привязки к биту. Интерактивные протоколы. Теорема об условном существовании интерактивных протоколов привязки к биту.
13. Статистическая неразличимость. Односторонние перестановки. Теоремы о вычислительной неотличимости распределений случайных величин.
14. Семейства односторонних перестановок с секретом.
15. Шифрование с открытым ключом.

3. Правила выставления оценки на зачете.

В процессе зачета требуется ответить на один из приведенных выше вопросов. На подготовку к ответу дается не менее 1 академического часа.

По итогам зачета выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «Зачтено» выставляется студенту, который демонстрирует владение содержанием материала и понятийным аппаратом теории псевдослучайных генераторов; умеет связывать теорию с практикой. В ответе могут допускаться отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора. На часть дополнительных вопросов студент может не дать ответ или дать неверный ответ.

Оценка «Не зачтено» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение № 2 к рабочей программе дисциплины «Теория псевдослучайных генераторов»

Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Теория псевдослучайных генераторов» отводится один семестр. В конце семестра в качестве итогового контроля предусмотрен зачет. В процессе изучения дисциплины выполняются восемь домашних заданий.

При изучении учебного материала по дисциплине «Теория псевдослучайных генераторов» соблюдается баланс между лекционными и практическими занятиями. Это связано с тем, что с одной стороны в рамках дисциплины излагается большое количество нетривиального учебного материала, в том числе результаты научных исследований последнего десятилетия, а, с другой стороны, для полноценного освоения данного материала обучающемуся необходимо получить самостоятельный опыт по применению изучаемого в рамках дисциплины математического аппарата.

Основную роль для анализа и контроля качества усвоения материала играют домашние работы. В качестве заданий для самостоятельной работы дома обучающимся предлагаются математические задачи, которые должны позволить студенту переосмыслить изученные на лекциях понятия и методы, применить их для решения типовых задач из соответствующих разделов дисциплины. Решения задач должны быть подготовлены, оформлены в письменном виде и представлены в установленные сроки.

Для повышения качества усвоения теоретического материала, приобретенных практических навыков работы с изучаемым в рамках дисциплины математическим аппаратом проводятся консультации по разбору заданий для самостоятельной работы. Также на консультациях, возможно повторно, разъясняются вопросы, вызвавшие затруднения у обучающихся.

По окончании семестра изучения дисциплины, обучающиеся сдают зачет. Зачет принимается по билетам, каждый из которых включает в себя один теоретический вопрос. На самостоятельную подготовку к зачету выделяется 2 дня.

Опыт преподавания дисциплины «Теория псевдослучайных генераторов» говорит о высокой сложности ее самостоятельного изучения для обучающегося в первую очередь ввиду достаточно узкого выбора учебной литературы на русском языке, а также ввиду необходимости обладания достаточно глубокими знаниями теории алгоритмов и теории вероятностей и математической статистики. Излагаемый на лекциях материал часто является нетривиальным и отражает результаты научных исследований последнего десятилетия. Поэтому посещение всех аудиторных занятий является обязательным.