
ПЕРВОЕ ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

SIBECRYPT — одна из ведущих конференций по криптографии и компьютерной безопасности в России, ежегодно проходящая в разных городах Сибири. Её цель — обсуждение фундаментальных математических проблем криптографии и защиты информации в компьютерных системах и сетях, обмен научными результатами по развитию теоретических основ и созданию программно-аппаратных средств компьютерной безопасности.

**Сроки проведения:** 6-11 сентября 2021 г.

**Место проведения:** г. Новосибирск, Новосибирский государственный университет и Институт математики им. С.Л.Соболева

**Сайт конференции:** www.sibecrypt.ru

**Организаторы:**

Новосибирский государственный университет
Международный математический центр в Академгородке
Томский государственный университет
Институт криптографии, связи и информатики Академии ФСБ
Академия криптографии Российской Федерации
Московский государственный университет им. М.В. Ломоносова

**Расписание** (предварительное):
Понедельник, 6 сентября – День заезда в Новосибирск. После обеда — пленарное заседание в Новосибирском государственном университете.
7 — 9 сентября – *Пленарные лекции, секционные доклады,*
*Концерт художественной самодеятельности силами участников,*
*Вечер воспоминаний о Геннадии Петровиче Агибалове*
Пятница, 10 сентября – Экскурсионная программа
Суббота, 11 сентября – День отъезда из Новосибирска

**Тематика школы-семинара** имеет математическую направленность, и её научную основу образует прикладная дискретная математика. В соответствии с этим проблематику исследований по тематике школы-семинара составляют проблемы дискретной математики, возникающие в компьютерной безопасности и криптографии. Они распределяются по следующим основным направлениям:

1) *теоретические основы прикладной дискретной математики* – алгебраические структуры, дискретные функции, комбинаторный анализ, теория чисел, математическая логика, теория информации, системы уравнений над конечными полями и кольцами;

2) *математические методы криптографии* – синтез криптосистем, методы криптоанализа, генераторы псевдослучайных последовательностей, оценка стойкости криптосистем, криптографические протоколы, математические методы квантовой криптографии;
3) *математические методы стеганографии* – синтез стеганосистем, методы стеганоанализа, оценка стойкости стеганосистем;
4) *математические основы компьютерной безоп*асности – математические модели безопасности компьютерных систем (КС), математические методы анализа безопасности КС, математические методы синтеза защищенных КС;
5) *математические основы надежности вычислительных и управляющих систем* (*ВиУС*) – математические модели функциональной устойчивости ВиУС (к отказам, неисправностям, сбоям, состязаниям, исследованию), математические методы анализа функциональной устойчивости ВиУС, математические методы синтеза функционально устойчивых ВиУС, математические методы верификации логических схем и программ, математические методы синтеза самопроверяемых и контролепригодных схем;
6) *прикладная теория кодирования* – коды для сжатия данных и защиты информации, коды для обнаружения и исправления ошибок, построение оптимальных кодов, анализ свойств кодов;
7) *прикладная теория автоматов* – автоматные модели сетевых протоколов, криптосистем и управляющих систем, автоматы без потери информации, эксперименты с автоматами, декомпозиция автоматов, автоматные уравнения, клеточные автоматы;
8) *логическое проектирование дискретных автоматов* – математические модели и методы анализа, синтеза, оптимизации и оценки сложности дискретных автоматов, аппаратная реализация криптоалгоритмов;
9) *математические основы информатики и программирования* – формальные языки и грамматики, алгоритмические системы, языки программирования, структуры и алгоритмы обработки данных, теория вычислительной сложности;
10) *вычислительные методы в дискретной математике* – теоретико-числовые методы в криптографии, вычислительные методы в теории чисел и общей алгебре, комбинаторные алгоритмы, параллельные вычисления, методы дискретной оптимизации, дискретно-событийное и клеточно-автоматное моделирование;
11) *математические основы интеллектуальных систем* – базы данных, базы знаний, логический вывод, экспертные системы, математическая лингвистика;
12) *прикладная теория графов* – графовые модели в информатике и программировании, в компьютерной безопасности, вычислительных и управляющих системах, в интеллектуальных системах;
13) *исторические очерки по дискретной математике и её приложениям* – в криптографии, компьютерной безопасности, кибернетике, информатике.

**Программный комитет:**

Черемушкин А.В., чл.-корр. АК России, Москва, председатель
Алексеев В.Б., профессор, МГУ, Москва
Девянин П.Н., чл.-корр. АК России, РусБИТех, Москва
Романьков В.А., профессор, ОмГУ, Омск
Панкратова И.А., зав. лабораторией, ТГУ, Томск
Сафонов К.В., профессор, СибГУ, Красноярск
Токарева Н.Н., зав. лабораторией, НГУ, ИМ СО РАН, Новосибирск,
Фомичёв В.М., профессор, Финансовый университет при Правительстве РФ, Москва

**Организационный комитет:**

Токарева Н.Н., зав. лабораторией, НГУ, ИМ СО РАН, Новосибирск, председатель
Панкратова И.А., зав. лабораторией, ТГУ, Томск, зам. председателя
Городилова А.А., научный сотрудник, ИМ СО РАН, Новосибирск
Идрисова В.А., научный сотрудник, ИМ СО РАН, Новосибирск
Коломеец Н.А., научный сотрудник, ИМ СО РАН, Новосибирск
Кондырев Д.О., преподаватель, НГУ, Новосибирск
Куценко А.В., научный сотрудник, ИМ СО РАН, Новосибирск

**Рабочие языки:** русский и английский.

**Формы докладов:** цикл лекций (одна или более; 1,5 ч. на лекцию), пленарный доклад (до 45 мин.) и секционный доклад (до 15 мин.).

**Представление докладов.** К представлению и публикации в материалах конференции принимаются тезисы докладов на русском или английском языках. Тезисы должны включать содержательные аннотации на русском и английском языке. Объём аннотации на английском языке — от одной четверти до половины страницы. Тезисы должны быть подготовлены в формате LaTeX с использованием стилевого файла sibecrypt.sty. Стилевой файл и шаблон для подготовки тезисов доступны на сайте www.sibecrypt.ru.

**Требования к содержанию тезисов.** Тезисы должны обязательно содержать конкретный новый результат по тематике школы-семинара. Это может быть модель, метод, алгоритм, теорема, доказательство, оценки (теоретические или экспериментальные) и т.п. Допускаются также тезисы обзорного доклада как заявка на лекцию для участников школы-семинара. Несодержательность или безграмотность английской аннотации является основанием для отклонения тезисов!

**Издание трудов конференции**. Тезисы докладов и аннотации к ним, удовлетворяющие требованиям к содержанию и оформлению, будут изданы в журнале «Прикладная дискретная математика. Приложение» (РИНЦ) к открытию конференции.

**Сроки**
- Тезисы докладов и заявки на лекции принимаются **до 30 апреля 2021 г.**
- Информация о принятии доклада будет отправлена **до 30 июня 2021 г.**

**Оргвзнос**
Примерно 2000 руб. Сроки и порядок оплаты будут оговорены во Втором информационном сообщении.

**Тезисы доклада с аннотацией следует посылать** по электронной почте в tex-файле и в pdf-файле. Каждый файл именовать фамилией первого автора (образец: Ivanov.tex, Ivanov.pdf). К TeX'овскому исходнику не забудьте приложить графические файлы, если они есть! Графики, диаграммы и т.п. рисунки должны быть созданы и присланы в векторном формате (.eps, .svg, .pdf и т.п.) без использования растровых вставок, в оттенках серого цвета. Имена графических файлов рекомендуется начинать с фамилии первого автора, так же, как и имя основного файла.

**Сайт школы-семинара:** www.sibecrypt.ru

**Электронный адрес** для представления заявок и тезисов: sibecrypt@mail.ru

**Ответственный секретарь оргкомитета конференции**
Ирина Анатольевна Панкратова,
ТГУ, лаборатория компьютерной криптографии
634050, Томск, пр. Ленина 36
E-mail: sibecrypt@mail.ru
Телефон для срочной оперативной связи: 8-913-845-24-30.