**Программа** (предварительная)

**23 МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ**
**«СИБИРСКАЯ НАУЧНАЯ ШКОЛА-СЕМИНАР**
**“КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ И КРИПТОГРАФИЯ”**
**имени Г.П. Агибалова» – SIBECRYPT'24**

**Вторник, 3 сентября**

**9:00 — 10:30** Регистрация участников — холл БТИ, здание Б (ул. Трофимова, 27).

**10:30** Открытие конференции. Приветственное слово директора БТИ М.А. Ленского

***Пленарные лекции***

**10:50 — 11:40**

1. *Денисов О.В., Рамоданов С.М.* (Москва). Разностно-линейные атаки различения на блочные шифры

***Кофе-брейк***

**12:00 — 12:50**

2. *Камловский О.В.* (Москва). Частотные характеристики элементов в линейных рекуррентных последовательностях и их усложнениях

**12:50 — 14:00** ***Обед***

**14:00 — 14:45**

3. *Антонов К.В., Семёнов А.А., Отпущенников И.В., Павленко А.Л.* (Москва, Иркутск, Санкт-Петербург). Алгебраические атаки на некоторые низкоресурсные шифры на основе функций с малым числом выходных бит

***Секционные доклады***

**14:50 — 15:50 Теоретические основы прикладной дискретной математики**

*Председатель — Панасенко С.П.*

1. *Комягин М.М.* (Москва). Изоморфизмы 5-конфигураций, получаемых по орграфам
2. *Новоселов С.А.* (Калининград). Характеристические многочлены геометрически приводимых обычных абелевых многообразий размерности 3
3. *Погорелов Б.А., Пудовкина М.А.* (Москва). О подстановках, совершенно рассеивающих классы разбиений векторного пространства $V_n^l(2^m)$
4. *Черемушкин А.В.* (Москва). Медиальные и парамедиальные алгебры сильно зависимых операций

***Кофе-брейк***

**16:10 — 17:40 Математические методы криптографии — I**

*Председатель — Пудовкина М.А.*

1. *Алексеев Е.К., Кяжин С.Н.* (Москва). Атаки на протоколы аутентифицированной выработки общего ключа, использующие схемы подписи, при связанных ключах участников
2. *Бахарев А.О., Царегородцев К.Д.* (Новосибирск, Москва). О стойкости некоторых алгоритмов над группой точек эллиптических кривых
3. *Бобровский Д.А., Шиликов Д.А.* (Москва). Исследование конструкций преобразования сигнала с ФДСЧ, основанного на кольцевых осцилляторах
4. *Бугров А.Д., Камловский О.В., Мизеров В.В.* (Москва). Свойства последовательностей, вырабатываемых алгоритмом поточного шифрования GEA-1
5. *Глухов М.М., Денисов О.В.* (Москва). Матрица переходных вероятностей разностей 8-раундовой схемы Луби — Ракофф
6. *Заикин О.С.* (Иркутск). Нахождения прообраза 44-шаговой функции сжатия MD4 при ослабленном последнем шаге (*докладчик — А.А. Семенов*)

**Среда, 4 сентября**

***Пленарные лекции***

**10:00 — 11:00**

1. *Панасенко С.П.* (Москва). Низкоресурсное аутентифицированное шифрование: обзор подходов

***Кофе-брейк***

**11:20 — 12:50**

2. *Черемушкин А.В.* Современные угрозы компьютерной безопасности (*для студентов БТИ*)

**12:50 — 14:00** ***Обед***

***Секционные доклады***

**14:00 — 15:30** **Дискретные функции**

*Председатель — Токарева Н.Н.*

1. *Быков Д.А., Коломеец Н.А.* (Новосибирск). О числе ближайших бент-функций к некоторым бент-функцям Мэйорана — МакФарланда
2. *Коломеец Н.А.* (Новосибирск). О числе функций, разрушающих структуру подпространств размерности 3 и выше
3. *Куценко А.В.* (Новосибирск). Характеризация обобщённых бент-функций алгебраической степени 1
4. *Панкратова И.А., Гарчукова П.Р.* (Томск). Об одной конструкции обратимых векторных булевых функций
5. *Панкратова И.А., Сорокоумова А.Д.* (Томск). Криптоаналитическая обратимость функций трёх аргументов
6. *Хильчук И.С.* (Новосибирск). О возможности построения S-блока, устойчивого к алгебраическому криптоанализу, с помощью выбора координатных булевых функций

***Кофе-брейк***

**15:50 — 17:20** **Математические методы криптографии — II**

*Председатель — Черемушкин А.В.*

1. *Казанцев С.Ю., Панков К.Н.* (Москва). Алгоритм быстрой выработки ключевой последовательности с использованием квантового канала связи
2. *Коренева А.М., Фирсов Г.В.* (Москва). Атака различения на один режим работы блочных шифров при наличии у нарушителя доступа к квантовому оракулу
3. *Поляков М.В., Коренева А.М.* (Москва). О стойкости алгоритма блочного шифрования КБ-256 к атакам с использованием квантовых алгоритмов
4. *Пудовкина М.А., Смирнов А.М.* (Москва). 6-раундовая атака на класс XSL-алгоритмов блочного шифрования
5. *Токарева Н.Н.* (Новосибирск). Десять лет международной олимпиаде по криптографии NSUCRYPTO
6. *Чежегова П.А., Коренева А.М., Поляков М.В., Фирсов Г.В.* (Москва). О перемешивающих свойствах регистровых преобразований алгоритмов шифрования TEA1 и TEA2

**19:00 Концерт силами участников школы-семинара**

Пожалуйста, будьте готовы!

**Четверг, 5 сентября**

***Пленарные лекции***

**10:00 – 11:00**

1. *Малыгина Е.С.* (Москва). Обзор постквантовых цифровых подписей дополнительного раунда NIST

***Кофе-брейк***

**11:20 — 12:20**

2. *Токарева Н.Н.* (Новосибирск). Об олимпиаде NSUCRYPTO и Летней школе по криптографии (*для студентов БТИ*)

**12:20 — 13:00**

3. *Кяжин С.Н.* (Москва). Развитие архитектур систем электронной подписи в условиях массового применения

**13:00 — 14:00** ***Обед***

**14:00 — 14:50**

4. *Беззатеев С.В.* (Санкт-Петербург). Обобщённые ($L$,$G$)-коды во взвешенной метрике Хэмминга для защиты информации

***Секционные доклады***

**15:00 — 15:45 Математические основы информатики и компьютерной безопасности**

*Председатель — Семенов А.А.*

1. *Егорушкин О.И., Колбасина И.В., Сафонов К.В.* (Красноярск). О решении линейных однородных грамматик, порождающих линейные языки
2. *Кондырев Д.О.* (Новосибирск). Система замера эффективности внутреннего представления схем zk-SNARK
3. *Лебедев Р.К., Ситнов В.Е.* (Новосибирск). Использование перемещений ELF для шифрования исполняемых файлов

***Кофе-брейк***

**16:00 — 17:15 Прикладная теория кодирования и автоматов**
**Вычислительные методы в дискретной математике**

*Председатель — Денисов О.В.*

1. *Болотникова А.Д., Колесников С.Г., Леонтьев В.М., Семенов А.И.* (Красноярск). Свойства поляризационной матрицы полярного кода и вычисление параметра Бхаттачарьи
2. *Кунинец А.А.* (Калининград). Обзор квазициклических альтернантных кодов и анализ их безопасности в криптографических приложениях
3. *Прудников Е.С.* (Томск). Конечно-автоматные генераторы максимального периода
4. *Бахарев А.О.* (Новосибирск). Исследование алгоритма $k$-просеивания для решения задачи нахождения кратчайшего вектора в решётке
5. *Утехина М.П., Божко А.А., Алексеев Е.К.* (Москва). О построении вспомогательных кривых алгоритма Маурера для стандартизированных в России «коротких» эллиптических кривых

**Закрытие школы-семинара**

**Обсуждение планов на будущее**

**Пятница, 6 сентября**

**Экскурсионная программа** (1600 руб — **оплачивается наличными** при регистрации)

Выезд на турбазу Усадьба "Сокол", расположенную в туркомплексе "Бирюзовая Катунь" на берегу Катуни, отправление автобуса в 8:00 от гостиницы «Центральная», возвращение в Бийск примерно в 21:30.