Международная научная конференция

# ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ КРИПТОГРАФИЯ

# ПРОГРАММА


БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

НИИ прикладных проблем математики и информатики


**19–20 октября 2023 года**
**Минск, БЕЛАРУСЬ**

**Информация**: http://conf.bsu.by/theoreticalandappliedcrypto
**Обратная связь**: apmi@bsu.by
**Офлайн**: главный корпус, а. 521
**Онлайн** (Skype): https://meet.bsu.by/bsu_sfb/T5K8KLSF

## 19 октября (четверг)

### ОТКРЫТИЕ КОНФЕРЕНЦИИ

**10:00**
**10:20** **А.В. Блохин** (проректор по научной работе, доктор химических наук, профессор);
**Ю.С. Харин** (директор НИИ прикладных проблем математики и информатики, академик НАН Беларуси)

### Заседание 1. ВЕРОЯТНОСТНО-СТАТИСТИЧЕСКИЕ МЕТОДЫ КРИПТОЛОГИИ
### Председатель: Ю.С. Харин (БГУ, Минск)

**10:20**
**10:40** Итерации случайных отображений конечных множеств
**А.М. Зубков** (Математический институт им. В.А. Стеклова РАН, Москва)

**10:40**
**11:00** Статистическая проверка сложных гипотез об *s*-мерном равномерном распределении вероятностей двоичных последовательностей
**Ю.С. Харин** (БГУ, Минск)

**11:00**
**11:20** Оценки для распределений рангов случайных двоичных матриц, состоящих из строк с заданными весами
**В.И. Круглов** (Математический институт им. В.А. Стеклова РАН, Москва)

**11:20**
**11:40** Об асимптотических свойствах семейства $\chi^2$-тестов чистой случайной двоичной последовательности
**В.А. Волошко** (БГУ, Минск)

**11:40**
**12:00** **Кофе-пауза**

### Заседание 2. ГЕНЕРАТОРЫ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ
### Председатель: В.А. Волошко (БГУ, Минск)

**12:00**
**12:20** Предельные совместные распределения статистик критериев пакета NIST
**М.П. Савелов** (МГУ им. М.В. Ломоносова, Москва)

**12:20**
**12:40** Статистическое тестирование криптографических генераторов на основе сложной нулевой гипотезы
**В.Ю. Палуха, Ю.С. Харин** (БГУ, Минск)

**12:40**
**13:00** О статистическом оценивании многомерной энтропии для проверки качества криптографических генераторов
**М.В. Мальцев, Ю.С. Харин** (БГУ, Минск)

### Заседание 3. ОЦЕНКА НАДЕЖНОСТИ
### Председатель: С.В. Агиевич (БГУ, Минск)

**14:00**
**14:20** Анализ полнораундового алгоритма шифрования LILLIPUT-TBC-II-256
**А.М. Смирнов, М.А. Пудовкина** (МИФИ, Москва)

**14:20**
**14:40** Линейный криптоанализ алгоритма шифрования ISL_LWC
**Д.С. Дюсенбаев, С.Е. Нысанбаева, К.С. Сакан, А. Хомпыш** (ИИВТ, Алматы)

**14:40**
**15:00** О стойкости семейства алгоритмов NEA/NIA
**К.Д. Царегородцев, С.А. Давыдов, А.А. Чичаева** (АО «Криптонит», Москва)

**15:00**
**15:20** Дифференциальный криптоанализ легковесного алгоритма LBC
**Н.А. Капалова, К.Т. Алгазы, А. Хаумен** (ИИВТ, Алматы)

**15:20**
**15:40** Анализ криптосистемы на булевых функциях
**А.В. Кандинский, И.А. Панкратова** (ТГУ, Томск)

## 20 октября (пятница)

### Заседание 4. ДЕЦЕНТРАЛИЗОВАННЫЕ СИСТЕМЫ
### Председатель: М.В. Мальцев (БГУ, Минск)

| | |
|---|---|
| **10:00**<br>**10:20** | Вариант реализации низкоресурсного блокчейна для индустриального интернета вещей<br>**С.Л. Панасенко** (АО «Актив-софт», Москва) |
| **10:20**<br>**10:40** | Extending the functionality of blind accumulators: contexts<br>**S. Agievich, M. Kazlouski** (БГУ, Минск) |
| **10:40**<br>**11:00** | Обеспечение конфиденциальности в приватных блокчейн-системах<br>**М.Н. Мицкевич** (БГУ, Минск) |
| **11:00**<br>**11:20** | **Кофе-пауза** |

### Заседание 5. СИММЕТРИЧНЫЕ ПРИМИТИВЫ
### Председатель: С.В. Агиевич (БГУ, Минск)

| | |
|---|---|
| **11:20**<br>**11:40** | Рассеивающие свойства преобразований, заданных комбинацией циклических сдвигов, в различных алгебраических структурах<br>**Д.М. Крапивенцев, М.А. Пудовкина** (МИФИ, Москва) |
| **11:40**<br>**12:00** | О разностном анализе модулярного сложения с помощью ЦЛП<br>**Д.В. Коледа** (ИМ НАН Беларуси, Минск) |
| **12:00**<br>**12:20** | Комбинаторный подход к исследованию APN-подстановок<br>**А.Р. Белов** (ЯГУ им. П.Г. Демидова, Ярославль) |
| **12:20**<br>**12:40** | О компактном линеаризуемом алгебраическом описании криптографических преобразований<br>**Ф.Б. Дасько** (БГУ, Минск) |

### Заседание 6. АУТЕНТИФИКАЦИЯ, ОБЛАЧНЫЕ СЕРВИСЫ, СТЕГАНОГРАФИЯ
### Председатель: В.А. Волошко (БГУ, Минск)

| | |
|---|---|
| **14:00**<br>**14:20** | Использование пороговой криптосхемы разделения секрета для биометрической аутентификации<br>**С.Е.Нысанбаева, Н.А.Капалова, С.Б.Бейсенова** (ИИВТ, КНУ им. Аль-Фараби, Алматы) |
| **14:20**<br>**14:40** | Облачная электронная цифровая подпись: протокол активации подписи<br>**О.В. Соловей** (БГУ, Минск) |
| **14:40**<br>**15:00** | Стеганографическая стойкость растрированных изображений с осаждением тайной информации в полутоновых оттенках<br>**М.Г. Савельева, П.П. Урбанович** (БГТУ, Минск) |

### Заседание 7. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ
### Председатель: Ю.С. Харин (БГУ, Минск)

| | |
|---|---|
| **15:00**<br>**15:20** | Оптимизация программного кода разработанного легковесного алгоритма шифрования ISL_LWC<br>**О.А. Лизунов, А. Хомпыш** (ИИВТ, Алматы) |
| **15:20**<br>**15:40** | Методы выявления и анализа уязвимостей в распределенных компьютерных системах<br>**И.К. Пирштук, Н.А. Возовиков** (БГУ, Минск) |
| **15:40**<br>**16:00** | К вопросу использования опенсорсных средств шифрования при защите каналов связи<br>**А.М. Сапрыкин** (ООО «С-Терра Бел», Минск) |
| **16:00** | **ЗАКРЫТИЕ КОНФЕРЕНЦИИ** |