Настоящие и перспективные задачи стандартизации в области криптографии и безопасности информационных технологий

Бондаренко А.И.
Академия криптографии
Российской Федерации
bondarenko_ai@tc26.ru

Регулирование национального информационного пространства

- **«Доктрина информационной безопасности Российской Федерации»**, утвержденная Президентом Российской Федерации от 9 сентября 2000 года № Пр-1895

Документ утратил силу

- Федеральный закон **«Об электронной цифровой подписи»** от 10 января 2002 года № 1-ФЗ

Документ утратил силу

- Федеральный закон **«Об информации, информационных технологиях и защите информации»** от 27 июля 2006 года № 149-ФЗ

- **«Стратегия развития информационного общества в Российской Федерации»**, утвержденная Президентом Российской Федерации от 7 февраля 2008 года № Пр-212

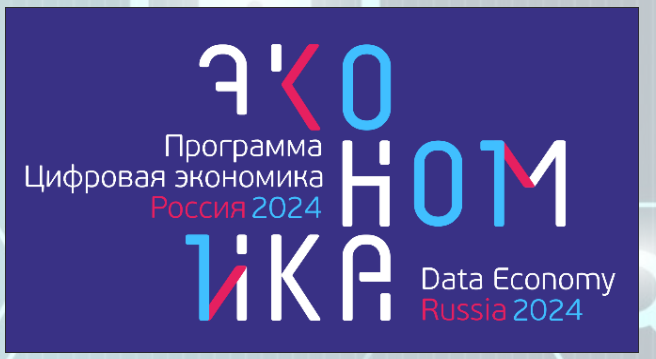
Документ утратил силу

Риски отсутствия коммуникаций с профильными специалистами

- Риск интеграции решений, содержащих уязвимости, являющиеся «сырыми» или непроверенными.
- Сложность организации и планирования фундаментальных научных исследований по актуальным направлениям защиты информации.
- Отсутствие возможности привлечения специалистов по узкоспециализированным вопросам.
- Многократный анализ одних и тех же стандартизируемых решений специалистами на различных площадках.

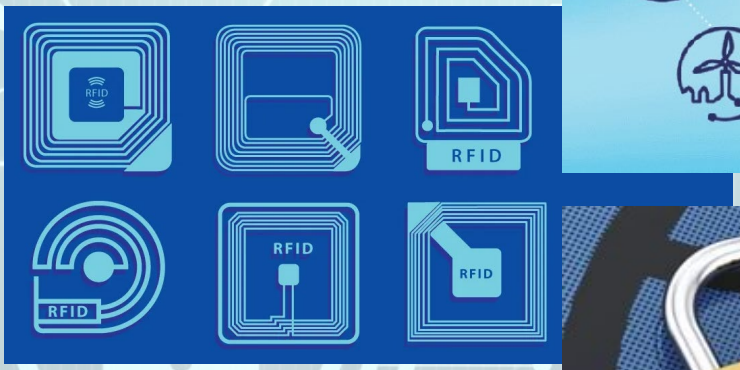
Федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»

- осуществление **информационно-аналитическое обеспечение и координацию** участия российских экспертов в деятельности международных организаций, осуществляющих разработку международных документов по стандартизации в области криптографии и безопасности информационных технологий



Научные исследования в интересах стандартизации

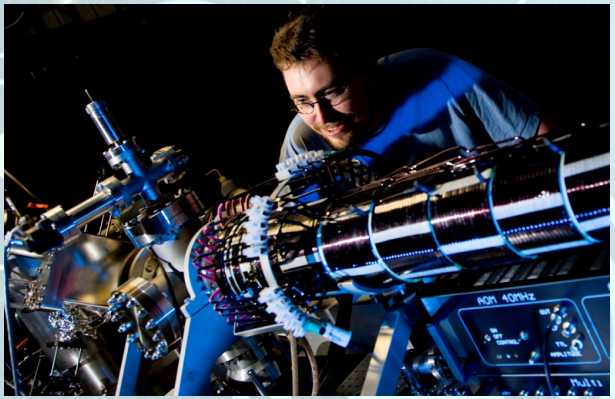
- Криптографические механизмы средств радиочастотного обмена



- Криптографические механизмы значимых платежных систем

Научные исследования в интересах стандартизации

- Криптографические механизмы в средствах беспроводной связи



- Постквантовые криптографические алгоритмы

•изогении суперсингулярных эллиптических кривых
•деревьев хэшей
•задача обучения с ошибками
•типа NTRU
•многочлены от многих переменных
•теория корректирующих кодов
•некоммутативные и неассоциативные структуры

Научные исследования в интересах стандартизации

- Аспекты информационной безопасности новых технологий

- Технологии защиты информации облачных платформ

Форум по информационной безопасности в цифровой экономике

- г. Москва
  Академия криптографии Российской Федерации

- 7 октября 2020 года
  10.00 – 14.00

- Текущие результаты и научная дискуссия

Спасибо за внимание