ВИЗУАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

А.Л.ТРУХАНОВИЧ, Н.А.РАЩЕНЯ, М.В.ЛОСЬ
Белорусский государственный университет,
Научно-исследовательское учреждение
«ИНСТИТУТ ПРИКЛАДНЫХ ФИЗИЧЕСКИХ ПРОБЛЕМ ИМЕНИ А.Н. СЕВЧЕНКО»
Белорусского государственного университета

Специфика подготовки специалистов в области защиты информации и кибербезопасности

Базовые предметы

- Математический аппарат
- Общая физика
- Правовые аспекты

Компьютерные технологии

- Программирование
- Архитектура компьютера
- Микроконтроллеры
- Операционные системы
- Компьютерные сети

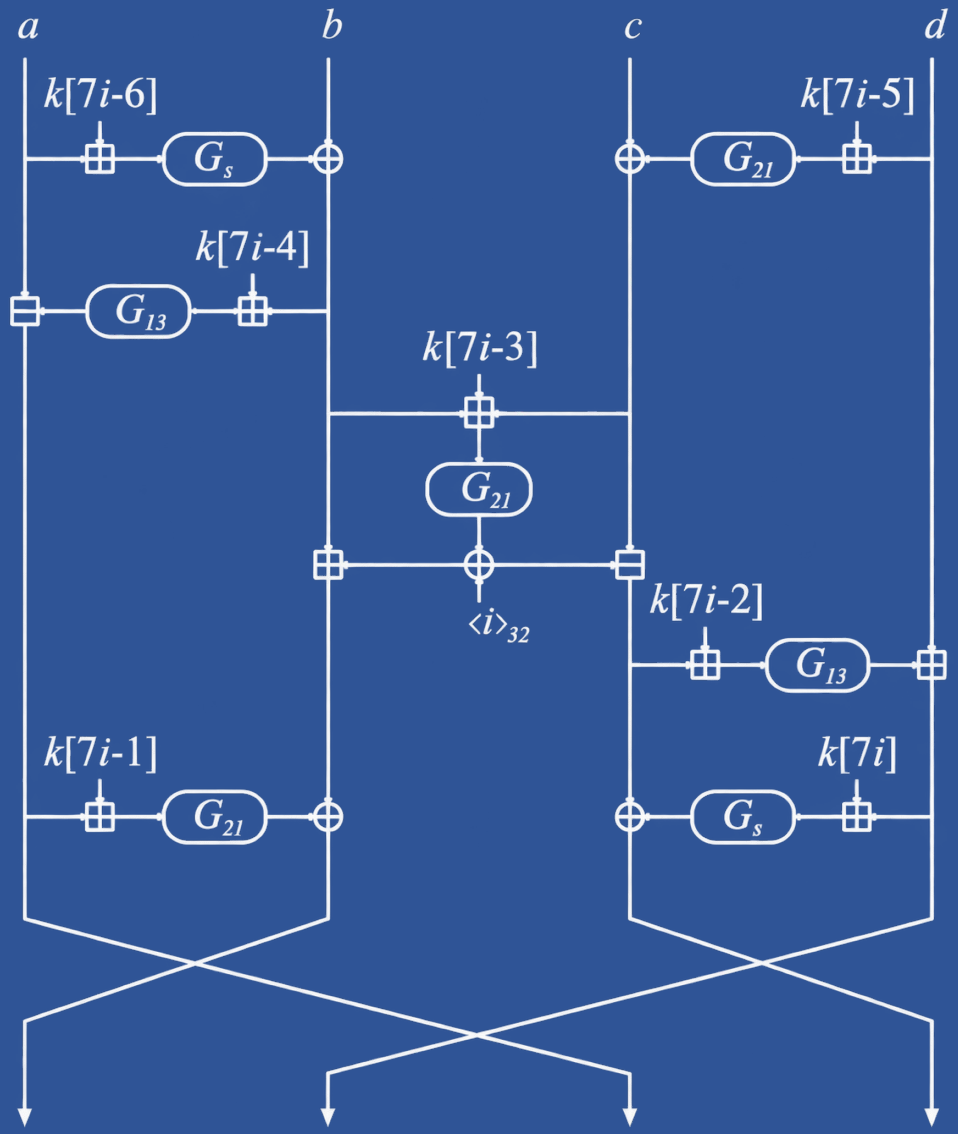
Защита информации

- Основы информационной безопасности
- Программно-аппаратные средства обеспечения информационной безопасности
- Криптография

Сложность изучения внутренней логики работы криптографических преобразований

Криптографические алгоритмы являются сложной многошаговой структурой:

- множество однотипных раундов обработки данных,
- применение различных видов операций (перестановки, подстановки, модульная арифметика),
- нелинейные зависимости между входными и выходными данными.



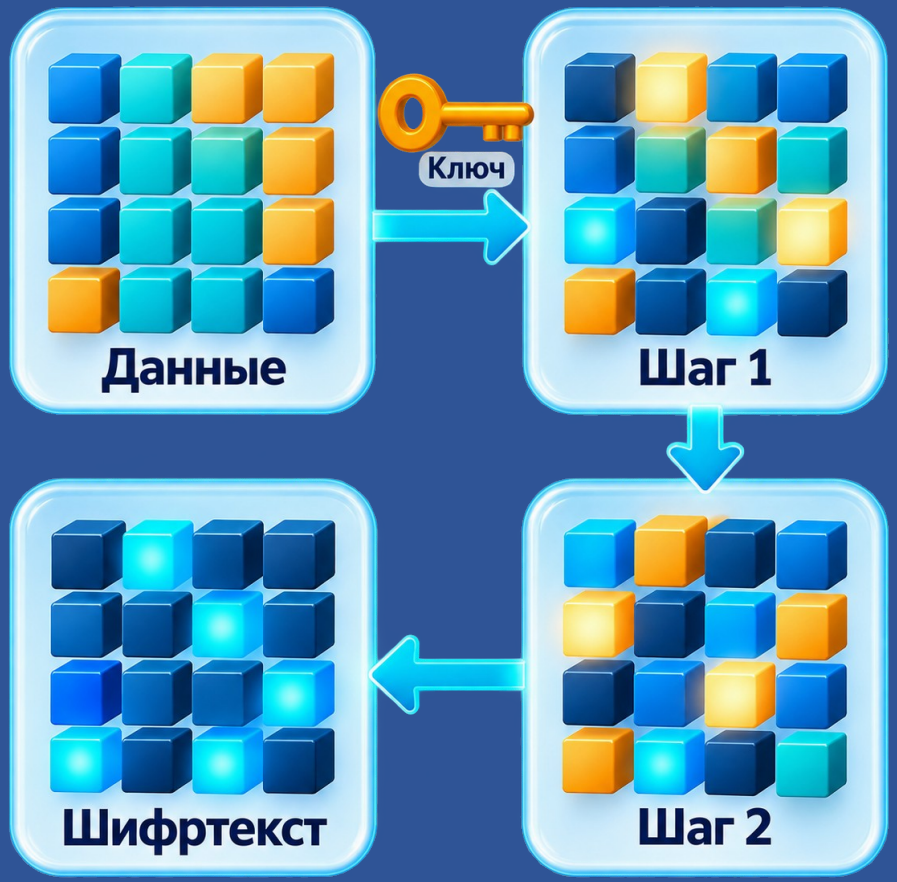
Классические подходы к изучению криптографических механизмов

- Теоретический подход.
- Текстовое представление криптографических алгоритмов, основанное на изучении официальной нормативной документации.
- Алгоритмический метод основан на построении классических блок-схем.
- Графический подход.

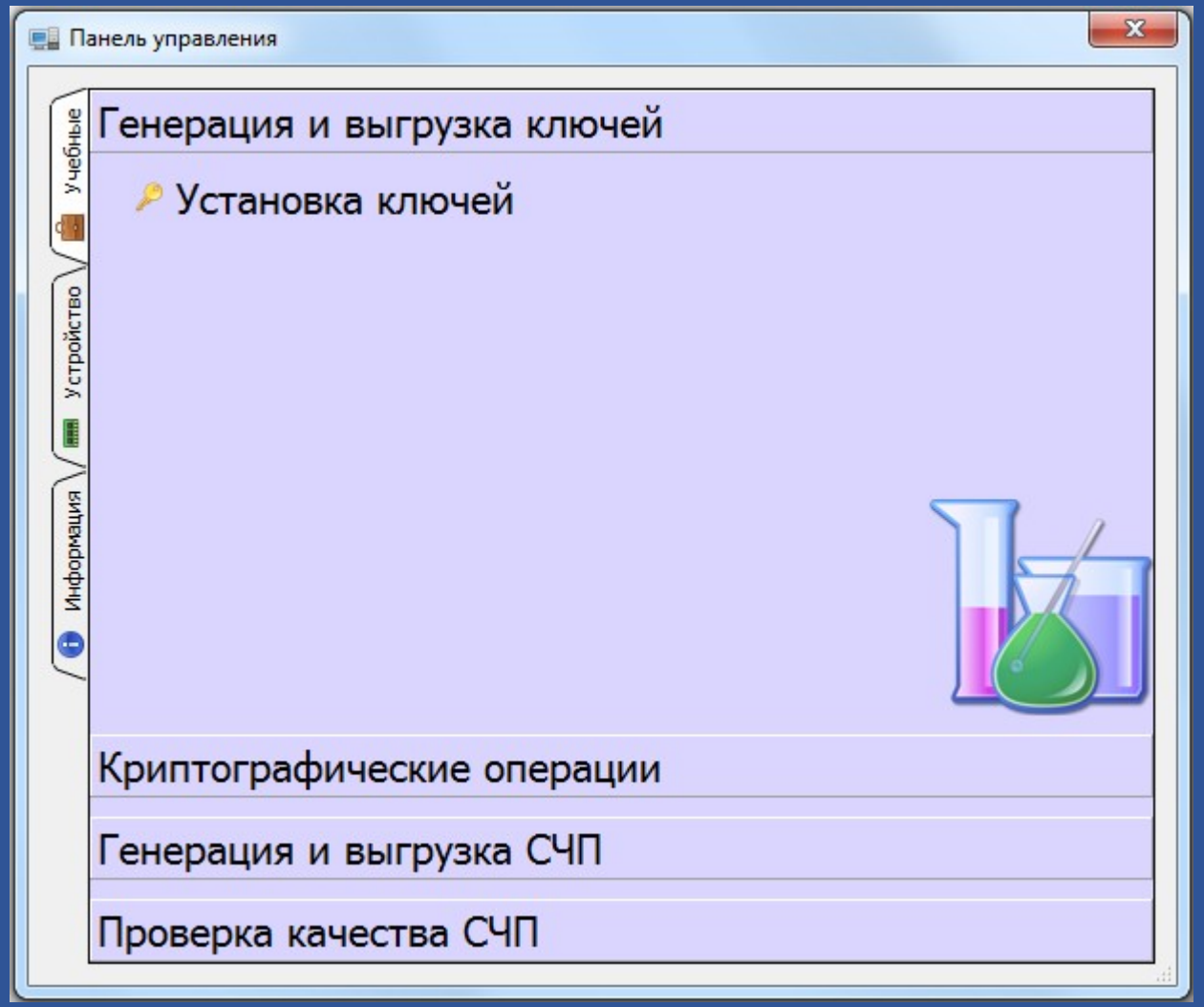
Визуализация алгоритмов

Визуализация криптографических алгоритмов выступает связующим элементом между теоретическими знаниями и практическим применением.

Она позволяет продемонстрировать не только итоговый результат, но и пошаговую трансформацию данных внутри каждого этапа алгоритма.



Аппаратно-программный комплекс «Крипто-Лаб»

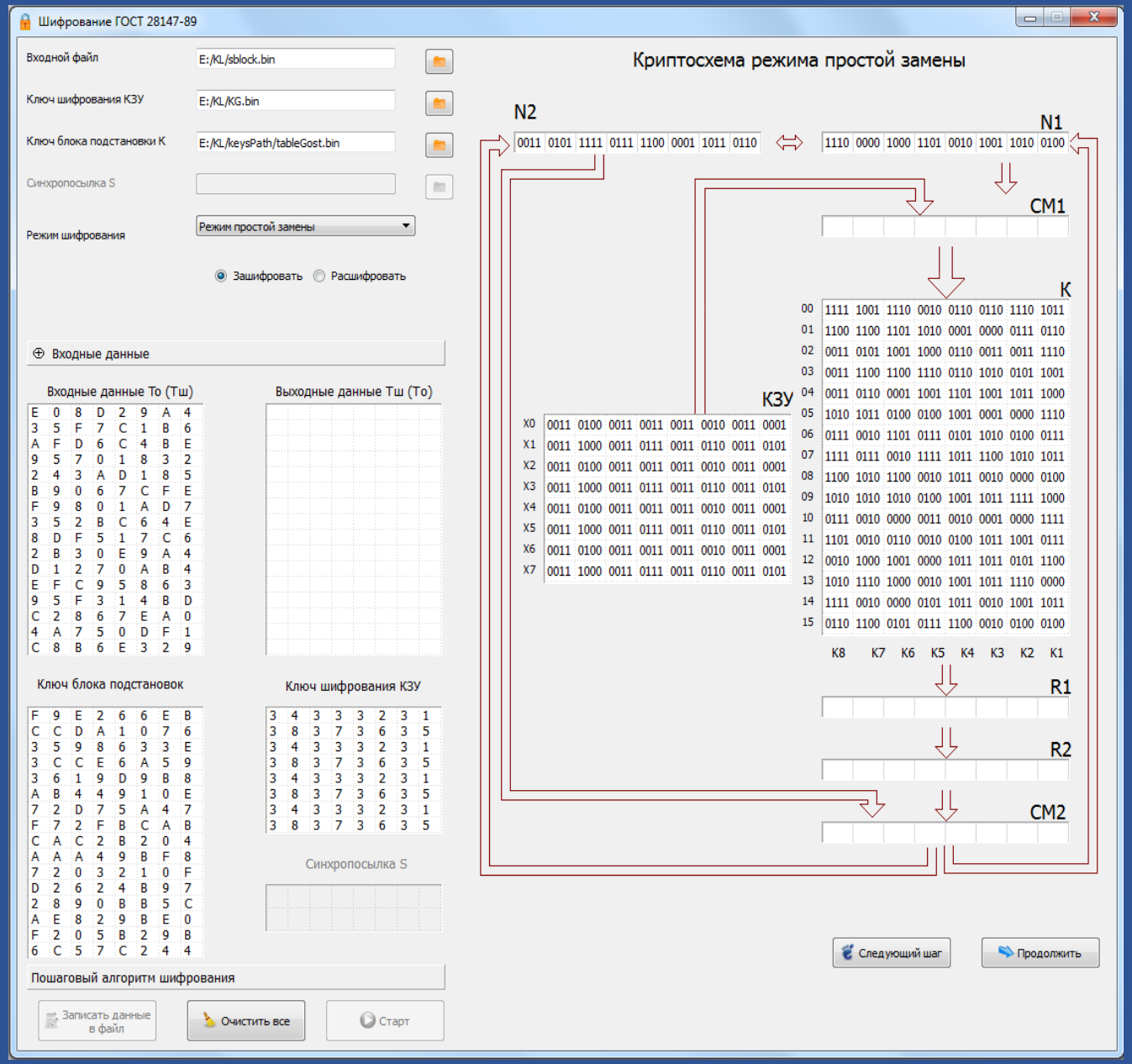


Визуализация работы криптографического алгоритма

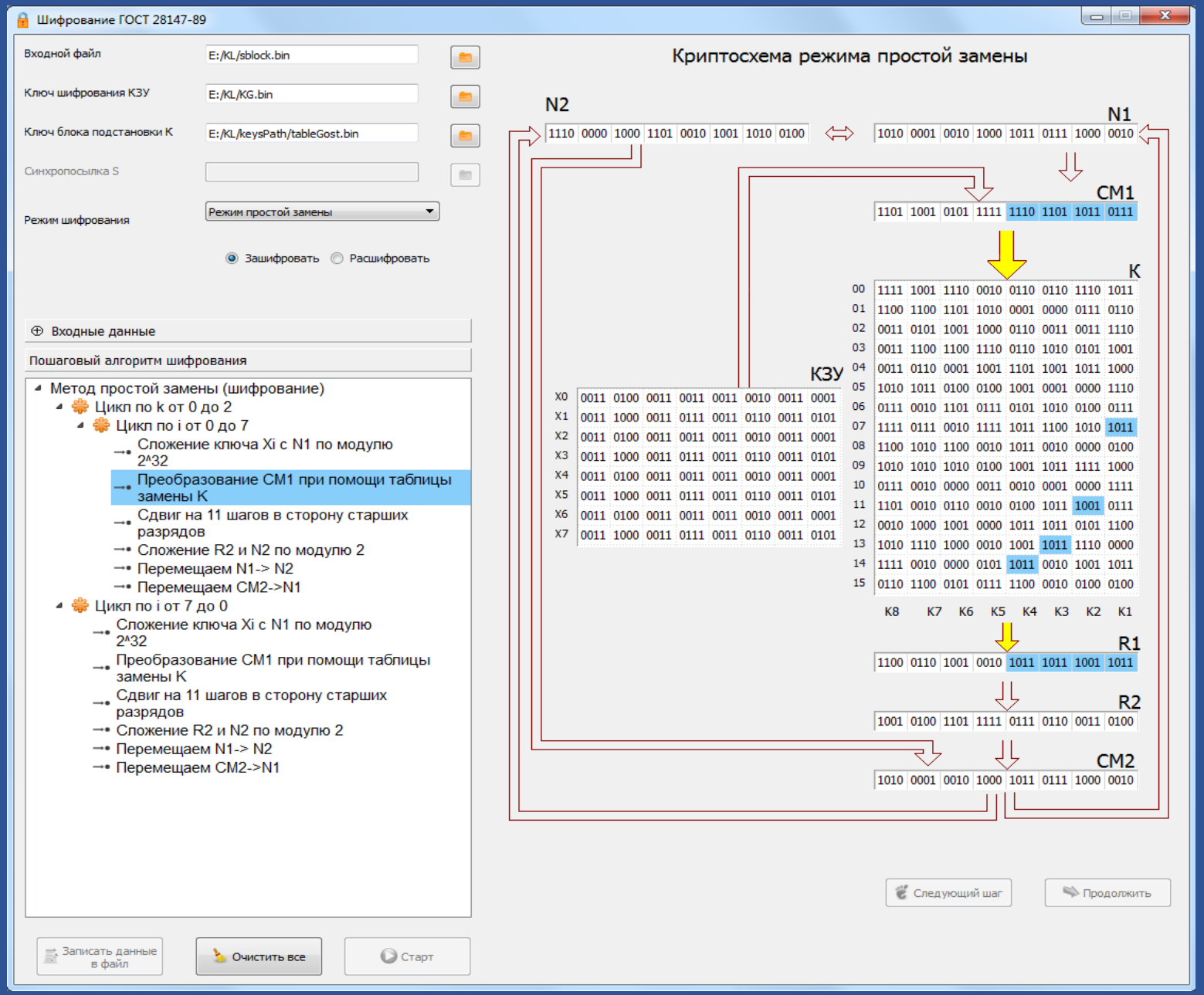
Программный интерфейс визуализации алгоритма разделен на две рабочие зоны:

панель управления параметрами (слева) и

визуализацию криптосхемы (справа).



Пошаговое выполнение алгоритма



Возможность исследовать и производить анализ алгоритмов

- Возможность видеть структуры данных и перемещение информации в них
- Возможность производить анализ данных на каждой операции алгоритма
- Измерять временные параметры работы отдельных блоков алгоритма

Криптографические алгоритмы для визуализации

Назначение	Алгоритмы и стандарты
Учебные шифры	Цезаря, Виженера, Плейфера, Хилла
Симметричные шифры	DES, AES, ГОСТ 28147-89, ГОСТ 34.12-2018
Шифрование и целостность	СТБ 34.101.31
Асимметричные алгоритмы	RSA, ECDSA, ECDH
Подпись и транспорт ключа	СТБ 34.101.45
Хеширование	СТБ 1176.1-99, SHA-256, MD5
Электронная подпись	СТБ 1176.2-99, ГОСТ 34.10-2018

Визуализация криптографических алгоритмов для обучающихся

Визуализация позволяет следующее:

- перейти от статического заучивания стандартов к динамическому пошаговому наблюдению выполнения криптографических процессов
- детально понимать принципы криптографических преобразований
- связать абстрактные операции с изменяющимися данными
- ускорить восприятие и понимание алгоритмов
- снизить нагрузки на рабочую память у обучаемого
- исследовать алгоритмы
- производить анализ алгоритмов

Спасибо за внимание

Докладчик: Труханович Алексей Леонидович
старший преподаватель
кафедры телекоммуникаций и информационных технологий
факультета радиофизики и компьютерных технологий
Белорусского государственного университета