МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

# «Асимметричное шифрование данных»

**Студент:** Яковлев Роман Денисович

**Группа:** ИУ7-54Б

**Руководитель:** Кострицкий Александр Сергеевич

# Цели и задачи

**Цель работы** – проанализировать существующие методы асимметричного шифрования данных.

**Задачи работы**

1. Ознакомиться с существующими алгоритмами асимметричного шифрования данных.
2. Выделить их сходства и различия.
3. Сформулировать критерии для сравнения алгоритмов
4. Провести сравнительный анализ алгоритмов по сформулированным критериям

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ

| Критерий | RSA | DSA | ECDSA |
|---|---|---|---|
| Безопасность (Сложность криптоанализа) | 1 | 2 | 3 |
| Безопасность (Размер ключа) | 2 | 1 | 3 |
| Производительность (Скорость шифрования/дешифрования) | 2 | 3 | 1 |
| Производительность (Эффективность вычислений) | 1 | 3 | 2 |