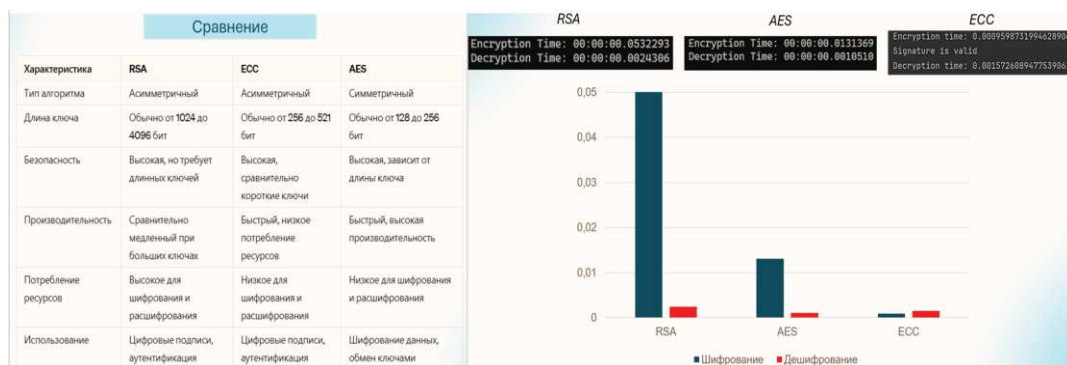


методов шифрования на мобильных устройствах становится необходимостью для обеспечения безопасности и конфиденциальности данных пользователей.

В рамках доклада была проделана работа по анализу и сравнению современных методов шифрования; были затронуты как программные способы, так и аппаратные. На рисунке приводится результат проделанной работы: сравнительные оценки известных шифров.



Как итог, следует отметить, что важна не только программная часть шифрования данных, но и аппаратная, в связи со стоимостью реализаций для тех или иных задач.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 218 с.
2. Урбанович, П. П., Шутько, Н. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 2. Криптографические и стеганографические методы защиты информации: учеб.-метод. пособие для студ. вузов. – Минск: БГТУ, 2020. – 226 с.

УДК 004.5

Студ. П.А. Арцыхович
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ ЭФФЕКТИВНОСТИ КОДОВ ХЭМИНГА

В работе проведена оценка производительности кодов Хэмминга в условиях переменной зашумленности канала связи с применением генетических алгоритмов. Цель исследования – определить,

насколько эффективно использование генетических алгоритмов может улучшить производительность кодов Хэмминга по сравнению с традиционными методами.

Для наглядного представления использована библиотека для работы с генетическими алгоритмами: DEAP (Distributed Evolutionary Algorithms in Python), а также библиотека для работы с кодами Хэмминга – `bitarray`.

Анализ результатов экспериментов показал, что применение генетических алгоритмов значительно улучшает производительность кодов Хэмминга в условиях переменной зашумленности канала связи. Коды Хэмминга, оптимизированные с помощью генетических алгоритмов, демонстрировали более высокую вероятность успешной коррекции ошибок и более низкую вероятность обнаружения ошибок по сравнению с кодами, оптимизированными традиционными методами.

Анализ эффективности кода был выявлен в ходе выполнения генетического алгоритма, производя, оценку производительности каждой особи (индивидуума) популяции.

В данном случае функция *evaluate* вычисляет производительность кода Хэмминга, используя заданные критерии оценки (например, вероятности обнаружения и успешной коррекции ошибок).

Функция *evaluate* представленная ниже, позволяет оценить производительность каждой конфигурации кода Хэмминга в популяции генетического алгоритма:

```
def evaluate(individual):  
    hamming_code = create_hamming_code(individual)  
    P_detect, P_correct = test_hamming_code(hamming_code)  
    return (P_detect, P_correct)
```

ЛИТЕРАТУРА

1. Защита информации и надежность информационных систем: методические указания и контрольные задания для студентов специальности 1-40 01 02 (1-40 01 02-03) "Информационные системы и технологии (издательско-полиграфический комплекс)" заочной формы обучения / [сост.: П.П. Урбанович, Д.В. Шиман]. – Минск: БГТУ, 2012. – 42 с.