ключей и контроль целостности сообщений. С появлением протокола WPA2, внедренного в стандарте IEEE 802.11i, алгоритм RC4 был заменен на более безопасный и криптостойкий алгоритм шифрования AES [1, 2]. Беспроводные сети подвержены различным угрозам извне, самыми распространёнными из которых являются такие как «Человек посередине», или Man-in-the-middle, DDOS-атаки, ложные точки доступа и другие. Усилить защиту можно при помощи программных, аппаратных и аппаратно-программных средств (WIPS-системы, Fortinet, Sophos Wireless).

В области криптографической защиты беспроводных сетей проводится множество исследований, направленных на разработку новых методов и улучшение существующих технологий – квантовая криптография, методы машинного обучения для обнаружения атак, развитие протоколов аутентификации и шифрования, защита от атак со стороны искусственного интеллекта, управление уязвимостями и стандартизация [2, 3].

ЛИТЕРАТУРА

1 Урбанович, П. П. Компьютерные сети и сетевые технологии: учеб. пособие для студ. технических спец. / П.П. Урбанович, Д.М. Романенко. – Минск: БГТУ, 2022. – 608 с.

2. Анализ безопасности Wi-Fi [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/bastion/articles/777182/ – Дата доступа: 29.03.2024.

3. Ласык, Я. Использование сетевых протоколов и стеганографии для тайной передачи информации / Я. Ласык, Д.М. Романенко, П.П. Урбанович // Информационные технологии: материалы 86-й НТК профессорско-преподавательского состава, научных сотрудников и аспирантов, Минск, 31 января – 12 февраля 2022 г. – Минск: БГТУ, 2022. – С. 158–163.

УДК 003.26

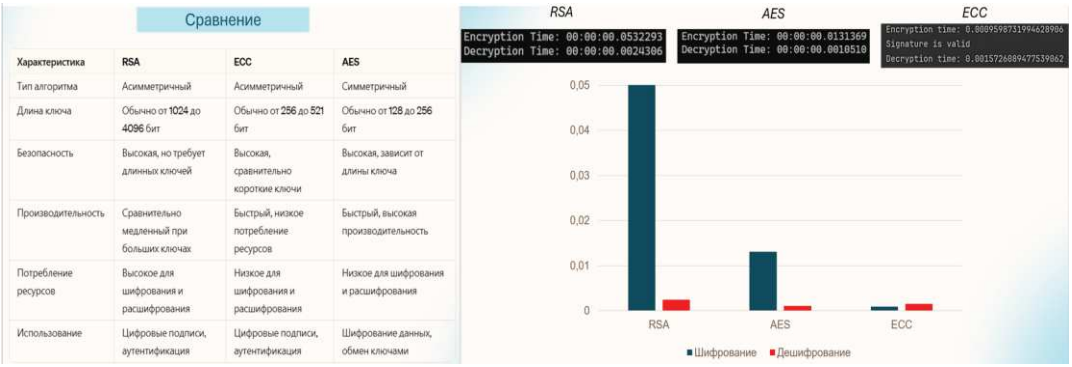
Студ. А. Н. Халалеенко, Т.С. Шишова
Науч. рук. проф., д-р техн. наук П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

МЕТОДЫ ШИФРОВАНИЯ В МОБИЛЬНЫХ УСТРОЙСТВАХ

С каждым днем все больше людей используют мобильные устройства для проведения финансовых транзакций, обмена конфиденциальной информацией и доступа к личным данным. Вместе с этим увеличивается и риск кибератак, направленных на кражу чувствительных данных, в том числе банковских реквизитов, личных сообщений и фотографий. Поэтому, разработка и применение надежных

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.



Сравнение

Характеристика	RSA	ECC	AES
Тип алгоритма	Асимметричный	Асимметричный	Симметричный
Длина ключа	Обычно от 1024 до 4096 бит	Обычно от 256 до 521 бит	Обычно от 128 до 256 бит
Безопасность	Высокая, но требует длинных ключей	Высокая, сравнительно короткие ключи	Высокая, зависит от длины ключа
Производительность	Сравнительно медленный при больших ключах	Быстрый, низкое потребление ресурсов	Быстрый, высокая производительность
Потребление ресурсов	Высокое для шифрования и расшифрования	Низкое для шифрования и расшифрования	Низкое для шифрования и расшифрования
Использование	Цифровые подписи, аутентификация	Цифровые подписи, аутентификация	Шифрование данных, обмен ключами

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 ХЭММИНГА

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