УДК 004.4

Студ. К.В. Граховская
Науч. рук. доц., канд. техн. наук Н.И. Белодед
(кафедра программной инженерии, БГТУ)

ПРИМЕНЕНИЕ ШИФРОВАНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

ИТ играют ключевую роль в развитии общества, проникнув во все сферы жизни. В военном деле ИТ способствуют повышению безопасности. Одной из главных задач стало обеспечение защиты информации от несанкционированного доступа.

Каждый день разрабатываются новые протоколы шифрования, системы обнаружения вторжений и методы защиты периметра, чтобы предотвратить утечки данных, кибератаки и другие угрозы.

Таким образом, развитие информационных технологий и обеспечение их безопасности становятся факторами стратегического значения для любого государства в эпоху цифровой трансформации.

Цель доклада – изучить реализацию методов шифрования на C++ и продемонстрировать их эффективность для защиты информации в различных сферах, включая военную отрасль и образование

Шифрование в контексте программирования на языке C++ – это процесс преобразования информации (текста, данных) в форму, которая не может быть легко прочитана или понята без специального ключа.

В C++ можно реализовать множество методов шифрования, от простых до сложных.

Шифр Цезаря. Это метод шифрования, где каждая буква в тексте заменяется другой буквой, сдвинутой на определенное количество позиций в алфавите.

RSA – это асимметричный метод шифрования, использующий пару ключей: открытый и закрытый.

Книжный шифр – это метод шифрования, где каждая буква исходного текста заменяется её координатами (строка и столбец) в тексте-ключе.

Одной из самых проблемных задач в реализации алгоритма шифрования на C++ является обеспечение защиты от атак посторонних каналов, таких как атаки по времени или анализ энергопотребления.

Таким образом, шифрование на C++ остается мощным и актуальным инструментом, адаптируясь к современным требованиям. Его эффективность и гибкость делают его ключевым элементом в разработке безопасных систем.