УДК 004.4

Студ. К.В. Граховская

Науч. рук. к.т.н., доцент Н.И. Белодед, кафедра программной инженерии, БГТУ

**ПРИМЕНЕНИЕ ШИФРОВАНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

1. **Актуальность**

IT прочно вошли во все сферы жизни, определяя развитие современного общества. В химической промышленности они ускоряют исследования и способствует созданию новых материалов с помощью ИИ. В военном секторе IT-технологии обеспечивают разработку высокоточных систем и повышают безопасность операций. Закрытие информации от несанкционированного доступа стало одной из основных задач использования информационных технологий.

1. **Цель**

Цель доклада — рассмотреть реализацию методов шифрования на C++ и показать их эффективность для защиты информации в различных сферах, таких как военная отрасль, образование и другие области. Планируется продемонстрировать практические примеры применения алгоритмов шифрования, их надежность и применимость для решения задач информационной безопасности.

1. **Шифрование. Современные задачи шифрования**

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. Это важная часть кибербезопасности, которая используется для защиты данных от несанкционированного доступа.

В C++ можно реализовать множество методов шифрования, от простых до сложных. Каждый метод имеет свои особенности и применяется в зависимости от задачи. Рассматривается несколько популярных методов шифрования и их реализация на C++.

Шифр Цезаря. Это один из самых простых методов шифрования, где каждая буква в тексте заменяется другой буквой, сдвинутой на определенное количество позиций в алфавите. Изучение шифра Цезаря позволяет освоить такие концепции, как ключ, алгоритм шифрования и частотный анализ.

RSA — это асимметричный метод шифрования, использующий пару ключей: открытый и закрытый. В C++ для работы с RSA также используются библиотеки, такие как OpenSSL. В некоторых случаях книжный шифр применяется в играх или интерактивных квестах, где участники должны найти скрытое сообщение, используя подсказки.

Книжный шифр – метод шифровки текста, в котором имеется текст ключ. Смысл шифрования заключается в том, чтобы находить каждую букву шифруемого слова в тексте-ключе и вывод поочерёдно строки и столбца. Это и будет шифр.

Разработка алгоритмов шифрования — это сложный процесс, требующий глубоких знаний в области математики, криптографии и программирования.

К основным принципам разработки алгоритмов шифрования относится криптостойкость, эффективность, управление ключами, совместимость.

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. Эти атаки используют неочевидные уязвимости, связанные с временем выполнения операций или физическими характеристиками системы, что делает их сложными для обнаружения и предотвращения.

Кроме того, важно избегать утечек данных через управление памятью, например, не очищая вовремя чувствительные данные, что может привести к их компрометации.

1. **Вывод**

Шифрование на C++ решает задачи в банковской сфере, защите данных и борьбе с киберугрозами, обеспечивая конфиденциальность, целостность и аутентификацию. Гибкость языка позволяет использовать как классические алгоритмы (AES, RSA), так и создавать новые методы для современных вызовов безопасности.

Таким образом, шифрование на C++ остается актуальным и мощным инструментом, способным адаптироваться к быстро меняющимся требованиям цифровой эпохи. Его широкие возможности и высокая эффективность делают его важным элементом в создании безопасных и надежных систем, что подчеркивает его значимость в наши дни.

Авторами разработаны алгоритмы программ, созданы программные средства, выполнено тестирование кода и получены практические результаты, которые будут использоваться в информационной системе управления учебным процессом на кафедре программной инженерии Белорусского государственного технологического университета.