ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В КОНТЕКСТЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Н.А. Урбан

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Криптография является одной из основ информационной безопасности. Выработка хэш-значения используется для проверки целостности и подлинности информации, а также в других криптографических алгоритмах [1]. Шифрование позволяет передавать данные в безопасном виде. В симметричных криптосистемах для зашифрования и расшифрования используется один и тот же секретный ключ. Без доступа к ключу невозможно расшифровать данные [2]. В асимметричных криптосистемах для зашифрования используется открытый ключ, а для расшифрования – закрытый. По сравнению с симметричным шифрованием такой алгоритм является более медленным, однако он лишен необходимости передавать секретный ключ. Для выработки электронной цифровой подписи (ЭЦП) используется секретный ключ, а для ее проверки – открытый. ЭЦП позволяет обеспечить контроль целостности и подлинности передаваемых данных [3].

В рамках дипломного проектирования была разработана программа, позволяющая вычислять хэш-значения от файла, вырабатывать и проверять значения ЭЦП файла. Программа обладает возможностью формирования и проверки файла контроля целостности, который можно использоваться для реализации требований к защите объектов (ЗО), самотестированию (СТ), обновлению программ (ОП) СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности». Она может быть использована в системах электронного документооборота для проверки целостности и подлинности передаваемых файлов различными организациями как при внешнем, так и при внутреннем обмене информацией, а также в обучающих целях для понимания работы криптографических алгоритмов.

При разработке программы использовалась библиотека Bee2 [4]. Bee2 – это криптографическая библиотека, распространяющаяся бесплатно под лицензией Apache 2.0 [5]. С помощью этой библиотеки в программе были реализованы функции выработки хэш-значения, формирование и проверка файла контроля целостности информации в соответствии с СТБ 34.101.31-2020, выработки значения электронной цифровой подписи в соответствии с СТБ 34.101.45-2013.

Разработанная программа позволяет реализовать требования безопасности к средствам криптографической защиты информации, в соответствие с СТБ 34.101.27-2022 и впоследствии может быть сертифицирована как средство криптографической защиты информации.

Список литературы

1. Что такое криптография? [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cryptography/. – Дата доступа: 17.04.2024

2. СТБ 34.101.27-2022 Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности.

3. Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи», 07.05.2021, № 113-З // Национальный правовой Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/. – Дата доступа: 17.04.2024

4. Библиотека Bee2 [Электронный ресурс]. – Режим доступа: https://apmi.bsu.by/blog/cryptology/bee2.html. – Дата доступа: 17.04.2024

5. Agievich/bee2: A cryptographic library [Электронный ресурс]. – Режим доступа: https://github.com/agievich/bee2/. – Дата доступа: 17.04.2024