УДК 681.06

КОЖЕМЯКИН Д.С., ЗЫКОВ И.С., канд. техн. наук

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ АЛГОРИТМА ЦИФРОВОЙ ПОДПИСИ

В многопользовательских компьютерных системах возникает проблема идентификации пользователей. Для идентификации пользователя, как правило, используются цифровые подписи на основе закрытого и открытого ключей.

По причине того, что использование асимметричных алгоритмов связано с большими затратами времени и вычислительных мощностей, алгоритмом цифровой подписи обрабатывается не исходный текст сообщения, а лишь его цифровой дайджест, также называемый хэшем.

Основным уязвимым местом алгоритма хэш-функции является возможность появления коллизий – ситуации, когда два разных сообщения имеют один и тот же хэш. Надежность используемой хэш-функции определяется вероятностью возникновения коллизии. Чем выше стойкость – тем меньше вероятность.

Коллизии могут быть использованы для подмены подписанных сообщений и лицо, подписавшее хэш, не сможет отрицать факт подписи.

Предлагается реализация алгоритма обнаружения коллизий хэш-функции md5.

Список литературы: 1. *Брюс Шнайер.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. Второе издание. М.:ТРИУМФ, 2002. **2.** wikipedia.org «Digital Signature Algorithm» http://en.wikipedia.org/wiki/Digital_Signature_Algorithm. **3.** Сетевые решения: поиск коллизий. http://www.nestor.minsk.by. 4. PGP. https://www.pgpru.com