УДК 004.054.53

Студ. Д.А. Черноус, А.Н. Самсончик
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

ИСПОЛЬЗОВАНИЕ СРЕДСТВ БИБЛИОТЕКИ OPENSSL ДЛЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ

OpenSSL – это полнофункциональный набор инструментов с открытым исходным кодом для протокола Transport Layer Security (TLS), ранее известного как протокол Secure Sockets Layer (SSL). Реализация протокола основана на полнофункциональной криптографической библиотеке общего назначения, которую также можно использовать автономно [1, 2]. В докладе анализируются некоторые особенности практического использования OpenSSL.

Протокол SSL (слой защищенных сокетов) – это криптографический протокол, который может располагаться поверх HTTP, тем самым добавляя в конец букву *S* (HTTPS), которая означает *secure*. Библиотека содержит набор функций, с помощью которых пользователь может разрабатывать собственные программы для криптографической защиты данных или создавать расширения, не входящие в стандартный набор. Протокол предоставляет различные меры обеспечения безопасности, две из которых являются основополагающими в HTTPS:

- взаимная аутентификация (peerauthentication, также известная как mutualchallenge): каждая сторона соединения аутентифицирует идентификационные данные другой стороны;
- конфиденциальность: отправитель шифрует сообщения перед их отправкой по каналу связи.

Функции OpenSSL часто содержат SSL в имени, даже если используется TLS, а не SSL. Вызов утилит командной строки OpenSSL начинается со строки ***openssl.***

ЛИТЕРАТУРА

1. Открытый SSL. Криптография и набор инструментов SSL/TSL. – URL: http://www.openssl.org – Дата доступа: 10.04.2023.

2. Урбанович, П. 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 / П. П. Урбанович, Н. П. Шутько. – Минск: БГТУ, 2020. – 226 с.