ПРОГРАММНЫЙ КОМПЛЕКС РЕГИСТРАЦИОННОГО ЦЕНТРА ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ С МЕХАНИЗМОМ ВЫРАБОТКИ ОБЛАЧНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В.А. Герасимов

Государственное предприятие «НИИ ТЗИ», Минск, Беларусь

В настоящее время одним из наиболее востребованных облачных сервисов является сервис облачной электронной цифровой подписи. Это обусловлено широким применением облачной (т. е. виртуальной) инфраструктуры в деятельности компаний [1]. С помощью указанного сервиса обеспечивается возможность удаленной выработки значения электронной цифровой подписи. Используемый при этом личный ключ хранится и управляется удаленным сервером от имени подписанта, являющего владельцем этого ключа [2]. Чтобы обеспечить безопасность среды создания электронной цифровой подписи и гарантировать использование личного ключа только под контролем подписанта, поставщик сервиса облачной электронной цифровой подписи должен применять специальные процедуры безопасности и использовать надежные аппаратные средства и программное обеспечение, в том числе для защиты канала связи с подписантом [3].

В связи с вышеизложенным, в Республике Беларусь в рамках опытно-конструкторской работы «Совершенствование инфраструктуры открытых ключей на основе современных web-технологий» по мероприятию 2 программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» («Паритет»), утвержденной постановлением Совета Министров Союзного государства от 11 июня 2018 г № 5 был разработан программный комплекс, реализующий возможности выработки облачной электронной цифровой подписи.

Для безопасного функционирования комплекса используются следующие криптографические стандарты:

– СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности»;

– СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности».

– СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».

Программные компоненты комплекса характеризуются одними из следующих функций:

– формирование общего секретного ключа в соответствии с СТБ 34.101.66-2014, с помощью которого стороны могут выполнять аутентификацию по протоколу защиты транспортного уровня (СТБ 34.101.65-2014);

– идентификация пользователей, в том числе их регистрация и проверка их идентичности в соответствии с СТБ 34.101.87-2022.

Внедрение программного комплекса позволит повысить эффективность функционирования информационных систем инфраструктуры открытых ключей Республики Беларусь. Для организаций переход на «облачные» сервисы позволит повысить гибкость, создавать более рациональную организацию работы сотрудников и сократить расходы на поддержание собственных серверов.

Список литературы

1. Защищенная виртуальная инфраструктура [Электронный ресурс]. – Режим доступа: https://becloud.by/services/uslugi-rtsod/infrastruktura-kak-usluga-iaas/zashchishchennaya-virtualnaya-infrastruktura/. – Дата доступа: 03.04.2023

2. СТБ 34.101.78-2019. Профиль инфраструктуры открытых ключей.

3. СТБ 34.101.bclo. Требования безопасности к системам облачной подписи.