УДК 004.056

ИТОГИ ПРОЕКТА «СИСТЕМА ОБЛАЧНОЙ ПОДПИСИ» В РЕСПУБЛИКЕ БЕЛАРУСЬ

Д. Н. АРЕСТОВИЧ, В. А. ГЕРАСИМОВ

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»г. Минск, Республика Беларусь

Система облачной подписи (СОП) в Республике Беларусь является одним из важных достижений в сфере цифровой трансформации общества. Этот проект представляет собой передовое решение, которое обеспечивает безопасность, надежность и эффективность в процессе создания электронный документов с электронной цифровой подписью (ЭЦП), созданной по средством облачных технологий.

Разработанная система является результатом опытно-конструкторской работы под названием «Совершенствование инфраструктуры открытых ключей на основе современных web-технологий», которая проводилась в рамках программы «Совершенствование системы защиты информационных ресурсов Союзного государства и государств-участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» (программа «Паритет»).

Для обеспечения высокого уровня безопасности работы СОП используются следующие криптографические стандарты [1]:

— СТБ 34.101.17–2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»;

— СТБ 34.101.19–2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;

— СТБ 34.101.23–2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»;

— 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»;

— СТБ 34.101.47–2017 «Информационные технологии и безопасность. Алгоритмы генерации псевдослучайных чисел»;

— СТБ 34.101.65–2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)»;

— СТБ 34.101.66–2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых»;

— СТБ 34.101.78–2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»;

— СТБ 34.101.87–2022 «Информационные технологии и безопасность. Инфраструктуры аутентификации».

В рамках разработанной системы используются разработанные или же модифицированные механизмы защиты информации [2] для обеспечения безопасности и подлинности электронных документов. Вот некоторые из них:

«Использование JWT при аутентификации пользователей».

Для аутентификации пользователей, СОП применяет JSON Web Token (JWT), который представляет собой компактный и самодостаточный метод передачи информации о пользователе. JWT содержит цифровую подпись, которая обеспечивает аутентичность и неподдельность данных, предоставляемых пользователем.

«Использование сетевого токена для аутентификации пользователей»

Этот механизм позволяет осуществлять аутентификацию пользователей с помощью специального сетевого токена. Токен генерируется и передается пользователям для проверки их подлинности при доступе к системе облачной подписи.

«Использование PIN для аутентификации пользователей»

Для повышения безопасности при аутентификации, СОП включает механизм использования персонального идентификационного номера (PIN). Пользователи должны предоставить правильный PIN для подтверждения своей личности и получения доступа к личному ключу.

«Использование данных активации подписи для повышения уровня гарантий контроля над личным ключом».

СОП использует данные активации подписи (ДАП) для обеспечения дополнительного контроля над личным ключом пользователя. Эти данные помогают установить идентичность пользователя и подтвердить его право на использование личного ключа.

«Использование протокола активации подписи для повышения уровня гарантий».

Для обеспечения дополнительной гарантии подлинности и безопасности, СОП реализует протокол активации подписи (ПАП). Этот протокол позволяет проверить, что подписывающая сторона имеет право подписывать документы и что подписываемые данные являются действительными и не подвергались подмене. При работе ПАП проверка ДАП происходит в устройстве программно-аппаратном криптографическом «NT HSM» (собственная разработка предприятия), которое принимает ДАП из двух источников и самостоятельно принимает решение по выработке значения ЭЦП.

Кроме указанных механизмов защиты, СОП также реализует механизм, который обеспечивает защиту от подмены подписываемого документа. Это позволяет предотвратить возможность внесения несанкционированных изменений в документ перед его подписанием.

Апробации возможностей разработанной системы в соответствии с планом действий по оперативному решению проблемных вопросов, связанных с использованием биометрических документов, удостоверяющих личность, была проведена с помощью закрытого бета-тестирования в инфраструктуре единого портала электронных услуг «Е-Паслуга», функционирующего в Республике Беларусь.

Таким образом, проект «система облачной подписи» в Республике Беларусь является важным достижением в области цифровой трансформации, предоставляя безопасность и

эффективность при создании электронных документов. Ее использование способствует развитию электронного правительства и улучшению качества услуг для граждан и организаций.

Список литературы

1. Герасимов, В. А. Программный комплекс регистрационного центра инфраструктуры открытых ключей с механизмом выработки облачной электронной цифровой подписи / В. А. Герасимов // Технические средства защиты информации: тезисы докладов XXI Белорусско-российской научно-технической конференции, Минск, 6 июня 2023 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол.: Т. В. Борботько [и др.]. — Минск, 2023. — С. 27–28.
2. Герасимов, В. А. Механизмы защиты информации при выработке облачной электронной цифровой подписи / В. А. Герасимов // Комплексная защита информации: материалы XXVIII научно-практической конференции, г. Гомель, 23–25 мая 2023 г. / Белорусский государственный университет транспорта. — Гомель, 2023. — С. 257–261.